CORAL ARANGÜENA FANEGO
MONTSERRAT DE HOYOS SANCHO
ESTHER PILLADO GONZÁLEZ
Directoras

PEDRO MIGUEL FREITAS
Coordinador

EL PROCESO PENAL ANTE UNA NUEVA REALIDAD TECNOLÓGICA EUROPEA

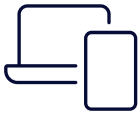
Prólogo

Francisco Jiménez-Villarejo Fernández

ARANZADI

EL PROCESO PENAL ANTE UNA NUEVA REALIDAD TECNOLÓGICA EUROPEA

Primera edición, 2023



Incluye versión en digital

Proyecto de investigación del Ministerio de Ciencia e Innovación: "*Proceso penal y Unión Europea. Análisis y propuestas*" –PID2020-116848GB-100.

Proyecto de investigación del Ministerio de Ciencia e Innovación: "Respuesta jurídica y socioeducativa a la violencia de género ejercida por menores. Protección de la víctima e intervención con el menor agresor. PID2019-106700RB-100.

Editorial Aranzadi, S.A.U.
Camino de Galar, 15
31190 Cizur Menor (Navarra)
ISBN: 978-84-1125-845-6
DL NA 82-2023
Printed in Spain. Impreso en España
Fotocomposición: Editorial Aranzadi, S.A.U.
Impresión: Rodona Industria Gráfica, SL
Polígono Agustinos, Calle A, Nave D-11
31013 – Pamplona

Índice General

Página

Página

Página

Página

II

INTELIGENCIA ARTIFICIAL Y JUSTICIA PENAL

Página

Página

Página

III

COOPERACIÓN JUDICIAL PENAL EN LA UNIÓN EUROPEA Y DIGITALIZACIÓN

Página

Página

Página

IV

CRIMINALIDAD ORGANIZADA, RESPONSABILIDAD DE LAS PERSONAS JURÍDICAS Y NUEVAS TECNOLOGÍAS

Página

Página

Página

Libro electrónico. Guía de uso

Prólogo

Agradezco a la Catedrática y querida amigo Coral Aranguena la amable invitación a prologar este libro colectivo sobre el proceso penal ante una nueva realidad tecnológica europea, que lo es también global. Reconozco que tras aceptar tuve una sensación de vértigo ya que no es un tema ante el que los prácticos del derecho de cierta edad nos sintamos especialmente cómodos. Una vez puestos manos a la obra, me di cuenta que, tal vez, quienes llevamos tiempo trabajando para la administración de justicia y en la construcción del espacio judicial europeo, con un recorrido, e mi caso, que puede compararse con una etapa de una vuelta ciclista, subiendo y bajando puertos de montaña, trabajando recientemente como fiscal de cooperación "a pie de obra" en la Fiscalía de Málaga y en lo que podemos considerar "atalayas de la cooperación judicial", como son Eurojust y la Unidad de Cooperación Internacional de la Fiscalía General del Estado, tal vez podamos alcanzar el equilibrio entre la realidad existente y la visión general necesaria con el enfoque correcto, de manera que permita analizar esta obra colectiva y valorarla en su justa medida. En primer lugar, destacaría que no hay arista que no haya sido tratada, siendo todos los aspectos que aborda tan actuales como relevantes, desde la doble perspectiva nacional y europea, que evidentemente aparece entreverada a causa del reconocimiento mutuo y la aproximación normativa. Por ello, quisiera destacar este acertado enfoque de este libro colectivo que pretende, no solo concienciar a los prácticos del derecho sobre la relevante transformación que estamos experimentando en los últimos años, introduciéndonos con interesantísimas reflexiones de su impacto y oportunidades que nos ofrece, de manera que nos sirva de acicate y ayuda en el esfuerzo de adaptación y capacitación que este desafío tecnológico y digital supone para la justicia penal europea.

El mayor acierto de la Directora de esta obra es haber sabido seleccionar materias y aspectos tan diversos del ámbito de la justicia penal dentro de la Unión Europea, unidos todos ellos por el sedal invisible de la singularidad y transformación tecnológica, estructurándolos de manera especialmente acertada en los cuatro ejes temáticos en los que se articulan los

24 capítulos del libro. En cada uno de estos pilares se repasa el impacto, los límites, las posibilidades y, como no, los retos de la digitalización en relación con cuestiones legales y prácticas de la utilización de datos personales, la inteligencia artificial, la cooperación internacional, la criminalidad organizada, la responsabilidad penal de las personas jurídicas y la protección de las víctimas y justicia juvenil. Si además, se cuenta con los mejores expertos en cada materia, esta acertada combinación es formula de éxito garantizado.

Hace cerca de quince años publiqué un artículo sobre delincuencia económica y nuevas tecnologías en el que destacaba como el espectacular desarrollo tecnológico de la informática y su aplicación en redes telemáticas en la segunda mitad del siglo XX, si bien ha facilitado el acceso masivo a las diversas fuentes de información, había traído aparejada como consecuencia perniciosa, el perfeccionamiento y aumento exponencial de las modalidades delictivas y de la eficacia lesiva de la delincuencia económica tradicional. Tras el impacto del ferrocarril, el barco de vapor y el telégrafo en la primera mitad del siglo XIX, la tecnología informática y su interconexión con los sistemas de telecomunicación, se ha calificado con acierto como la "segunda revolución industrial", caracterizada por la automatización, digitalización y globalización de redes informáticas (principalmente Internet) en la que el acceso masivo a la información, alcanza el más destacado protagonismo.

La realidad nos muestra como se ha producido una interconexidad entre los avances de las tecnologías de la información y de los sistemas informáticos y de telecomunicación, en lo que se denomina telemática, con la desaparición material no ya de las fronteras, sino de cualquier tipo de barreras espacio-temporales, permitiendo obtener, procesar y transmitir la información en tiempo real y a cualquier parte del planeta, lo que favorece la descentralización de la información y la interrelación, incluso simultánea de múltiples sujetos ubicados en distintos lugares lejanos geográficamente entre sí.

Los mecanismos de mera "automatización" o "digitalización" de la administración de justicia, mediante la generalización de los sistemas automáticos o telemáticos utilizados para facilitar y agilizar la tramitación de expedientes digitales que progresivamente van sustituyendo a los manuales en papel con documentos escaneados o en soporte electrónico o, para las notificaciones procesales, así como para la celebración de juicios online, está cambiando o entorno de trabajo. Si preguntas a cualquier autoridad judicial (concepto en el que incluyo a jueces y fiscales, de acuerdo con la jurisprudencia del Tribunal de Luxemburgo) sobre el cambio más relevante en su entorno laboral durante la última década, la

respuesta será el cambio de archivos manuales a archivos electrónicos, y el uso de intercambio de información estandarizada.

En cualquier caso, el reto de la digitalización, más que una opción es una obligación para las autoridades judiciales y, por extensión, para todos los operadores jurídicos. Sin perjuicio de que la digitalización no sea un fin, sino una herramienta para facilitar nuestro trabajo, es una herramienta irrenunciable. Tal vez el único efecto positivo de la dolorosa e incierta pandemia del COVID-19 que hemos sufrido en los últimos años haya sido el hacernos caer de bruces en la urgente necesidad de actualizar nuestros sistemas judiciales de acuerdo con las exigencias de la era digital. Esta situación excepcional ha puesto de manifiesto las vulnerabilidades de los sistemas judiciales europeos, pero también la resiliencia y adaptabilidad de los mismos para promover soluciones digitalizadas y el uso generalizado de comunicaciones por correo electrónico y reuniones por videoconferencia para dar una respuesta rápida y eficiente a cualquier necesidad de cooperación internacional. Un buen ejemplo de ello es la compilación del impacto del COVID-19 en la cooperación judicial internacional coordinada por Eurojust junto con la RJE, cuyas actualizaciones semanales tuve el honor de coordinar durante el año 2020. Sin duda, este incierto desafío ha dejado muchas cuestiones abiertas y mantiene retos para los profesionales de la justicia como la generalización del trabajo a distancia y los problemas de acceso a archivos confidenciales; la incompatibilidad de los sistemas de videoconferencia entre los diferentes Estados miembros y la necesidad de una mejor interconexión de estos sistemas para mejorar la calidad de las audiencias (¿tal vez a través de e-EDES cuando tienen finalidad probatoria?) y las reuniones virtuales en general; ante la generalización del uso del correo electrónico, la necesidad de una plataforma-portal de comunicación segura como puede ser el mencionado e-EDES; problemas relacionados con archivos de gran tamaño, más allá de la mera transmisión de formularios estandarizados inherente al régimen de reconocimiento mutuo; la integridad de los datos y la autenticación de los documentos electrónicos vinculada con la admisibilidad de la prueba; la necesidad de un mayor uso y reconocimiento de la firma electrónica a nivel transfronterizo; obstáculos y retrasos persistentes en relación con terceros países, ya que no todos aceptan transmisiones por correo electrónico y documentos escaneados o electrónicos…Las respuestas a algunos de estos retos las podemos encontrar en soluciones tecnológicas y en normas de *soft-law*, pero otras soluciones a las exigencias y el intercambio y comunicación de datos seguros y encriptados, requiere no solo de inversiones para su renovación tecnológica, sino también de reformas legales que proporcionen una base clara y revestida de seguridad jurídica. Además, en el ámbito de la cooperación con terceros países, los

acuerdos de cooperación internacional que celebrarán las instituciones de la UE nos permitirán abrirnos al resto del mundo.

En cualquier caso, la digitalización nos ofrece, principalmente, oportunidades para un mejor control y un uso más eficiente de los recursos en la justicia penal, haciendo posible la trazabilidad de las pruebas que se utilizarán ante los tribunales a través de todo el sistema de justicia penal (cadena de custodia); el formato electrónico facilita la revisión analítica y el cruce de datos en investigaciones financieras o la creación de datos procesables permitiría a los investigadores acelerar el tiempo de obtención de pruebas. Aquí entramos en el mundo de las posibilidades presentes y futuras que nos ofrecen los sistemas Inteligencia Artificial (AI) en el uso de algoritmos de ayuda a la valoración de la prueba y de los denominados "algoritmos predelictivos" que pueden auxiliar a las autoridades judiciales y policiales y que deber ser equilibrado con el respeto a los derechos y libertades fundamentales del ciudadano en relación con el debido proceso, en línea con el Libro Blanco sobre esta materia aprobado por la Comisión Europea. En cualquier caso, como recuerda dicho Libro Blanco, en materia de IA, el uso de algoritmos por las autoridades judiciales en la UE exige un ecosistema de confianza entre ellas con un enfoque antropocéntrico mediante una aproximación normativa que evite cualquier fragmentación, teniendo en cuenta que la cooperación judicial se basa en el principio de reconocimiento mutuo de resoluciones judiciales, cuya eficacia depende, como es bien sabido, del nivel de confianza mutua alcanzado entre las autoridades judiciales de la UE.

Como se destaca en la última Evaluación de la amenaza de la delincuencia grave y organizada de la Unión Europea (SOCTA 2021) y se hace eco la Comunicación de la Comisión Europea de 14 de abril sobre estrategia de la UE contra la Delincuencia Organizada 2021.2025 (SWD -2021- 74 final) La complejidad del modelo de negocio de los grupos de delincuencia organizada, con utilización de nuevas tecnologías y *modus operandi* cada vez más sofisticados, quedaron evidenciados en los ECIs que desmantelaron *EncroChat* y *Sky ECC*, redes de telefonía cifrada utilizadas por redes delictivas. En 2022 la Comisión ha propuesto el camino a seguir para abordar la cuestión del acceso legal y focalizado a información cifrada en el marco de investigaciones y acciones penales y con la necesaria supervisión jurisdiccional, partiendo del hecho de que el cifrado es esencial para el mundo digital, pues asegura los sistemas y las transacciones digitales y protege una serie de derechos fundamentales, tales como la libertad de expresión, la privacidad y la protección de datos, si bien se utiliza extensivamente con fines delictivos, ocultando la identidad de los delincuentes y el contenido de sus comunicaciones.

A nadie se le escapa la importancia de la conservación de los metadatos, a fin de permitir el acceso a pruebas y pistas de investigación digitales y la necesidad de que esta exigencia probatoria se compadezca con el secreto de las comunicaciones electrónicas y llegue a tiempo, teniendo en cuenta que los proveedores de servicios de comunicación borran periodica y sistemáticamente dichos metadatos de acuerdo con la ley impidiendo su utilización como prueba o/y la identifición de perpretadores y víctimas. Los metadatos de comunicaciones son especialmente importantes, para detectar y acreditar delitos ciberdelitos pero tambien para un espectro cada vez más amplio de delitos, desde la delincuencia organizada, al narcotráfico, la trata de seres humanos, el blanqueo de capitales,…se estima que el 80% de las investigaciones actuales involucran algún tipo de evidencia o dato digital (fotos, videos y mensajes de texto) almacenados y descargados masivamente de dispositivos incautados o recabados de redes sociales o proveedores de servicios en la nube (terabytes de datos cifrados…). Como quiera que de acuerdo con la jurirudencia del TJUE (*vid.* Sentencia de 2 de marzo de 2021 H.K./Prokuratuur, de 2 de marzo de 2021) no es posible la conservación generalizada e indiferenciada de los datos de tráfico no es posible y al estar en juego el derecho a la privacidad y a la protección de los datos personales y que, por ello, debe ser un juez o un tribunal quien autorice su conservación y uso para la investigación y la persecución de delitos. Desde 2028 en que la Comisión lanzó el paquete de pruebas electrónicas con miras a facilitar el acceso transfronterizo a ellas mediante las órdenes europeas de entrega y de conservación, estamos a la espera del resultado de las relaciones interinstitucionales entre el Parlamento Europeo y el Consejo, con el apoyo de la Comisión (los famosos trilogos), confiando que lleguen al consenso necesario que permita la pronta publicación del Reglamento y Directiva.

Uno de los principales retos a los que me enfrenté cuando fui Fiscal Anticorrupción en Málaga fue cómo digerir el enorme volumen de documentos antes de llevar los casos a juicio. Era el riesgo de sobreabundancia de pruebas, al que denominábamos como hiperoxia o "síndrome de exceso de oxígeno", por las dificultades para ordenar y racionalizar este inmenso material probatorio recabado durante la instrucción a fin de presentarlo adecuadamente, de manera estructurada y racional, ante un tribunal y con respeto a los derechos y garantías procesales y a la normativa de protección de datos requiere un ingente trabajo y de equipos bien dotados, lo que constituye uno de los grandes desafíos de la Fiscalía en la actualidad.

Hoy en día, los fiscales a nivel nacional no solo están sobrecargados de trabajo con la preparación esos complejos procedimientos de larga duración (que se prolongan en numerosas sesiones durante la fase de juicio

oral ante el tribunal de enjuiciamiento), además, el ingente volumen de datos que el formato digital permite recabar mediante el volcado de dispositivos de almacenamiento masivo o la interceptación de correos electrónicos, constituye un verdadero desafío que requiere de una estrategia investigadora eficaz y respetuosa, no solo del secreto de la comunicaciones y de la privacidad a la hora de su obtención, también con las exigencias de la legislación de protección de datos en su utilización en el procedimiento penal. La falta de la adecuada perspectiva y estrategia procesal podría generar efectos colaterales procesales (en relación con las garantías procesales de los sospechosos, derecho de defensa y derecho al debido proceso, divulgación y abuso de proceso, así como potenciales violaciones a la protección de datos) impidiendo que la prueba electrónica pueda ser finalmente utilizada y/o valorada como prueba de cargo principal.

Por lo tanto, el intercambio de grandes paquetes de prueba y de datos necesita un marco tecnológico y un tratamiento legal que proporcione a nuestras autoridades nacionales un enfoque de gestión de datos coherente y actualizado a nivel de la UE. Ello incluye una nueva plataforma ECI para el intercambio de información y pruebas (*JITS collaboration platform)*, cuya Propuesta de Reglamento fue lanzada por la Comisión en diciembre de 2021 con el fin de facilitar apoyo tecnológico mediante el establecimiento de una plataforma accesible por todos las autoridades judiciales y policiales involucradas en los procesos de constitución y funcionamiento de los ECIs, cuyo general approach se aprobó 9 de junio de 2022 por el Consejo y que se prevé iniciar a finales de 2022, durante la Presidencia Checa); una base de datos centralizada totalmente funcional con información sobre condenas de nacionales de terceros países y apátridas (ECRIS-TCN); así como a nivel de Eurojust, las mejoras técnicas en el funcionamiento del registro judicial de procedimientos en materia de terrorismo o, tras la reforma de su Reglamento, la recientemente creada base de datos de prueba en delitos de lesa humanidad [*Core International Crime Evidence Database* (CICED por sus siglas en inglés)]. Asimismo, debe destacarse el acceso efectivo entre los CMS de Eurojust y los de Europol, la Fiscalía Europea y los canales de intercambio de información con Frontex y OLAF, según lo previsto en las disposiciones espejo de los Reglamentos correspondientes y en los acuerdos de Colaboración firmados.

De cara al futuro, los retos de modernización del Espacio Judicial Europeo se reflejan en el informe final de la Comisión sobre la justicia penal digital transfronteriza publicado en septiembre de 2020. En concreto, las normas de cooperación judicial del siglo XXI requerirían canales de comunicación seguros entre las autoridades judiciales nacionales. La pregunta clave es como podemos intercambiar y analizar de manera automatizada

datos y material probatorio a nivel europeo entre autoridades judiciales. Hay dos proyectos que dan respuesta, tanto el Evidence2 como parte técnica de e-codex a fin de vincular grandes paquetes de prueba electrónica al portal e-codex a fin de permitir su transmisión segura, de manera que el paquete de prueba sea enviado como simple adjunto bajo el paraguas de transmisión de las OEIs entre los Estados miembros. Los esfuerzos realizados para acelerar la digitalización en la UE se reflejan en la Comunicación de la Comisión publicada en diciembre de 2020 con el título «La digitalización de la justicia en la UE: Un abanico de oportunidades». En ese sentido, los jueces y fiscales de la UE participamos en una fase piloto del sistema digital de intercambio de pruebas electrónicas (eEDES), finalmente basado en un portal que es una página web en superación del inicial proyecto e-Codex, con vistas a mejorar y acelerar el intercambio de prueba transfronterizo entre autoridades judiciales de diferentes Estados miembros. En este sistema e-EDES ya se están intercambiando OEIs (y comisiones rogatorias con IE y DK) entre las fiscalías y juzgados que participan en el proyecto piloto en esta plataforma digitalizada, si bien su conexión con los sistemas de gestión de casos nacionales todavía está pendiente de una solución técnica que pasaría por la robotización. Sin duda, la digitalización del área de la obtención de prueba transfronteriza, es la mejor manera de iniciar el impulso del reconocimiento mutuo como piedra angular de la cooperación judicial en el Espacio Judicial Europeo en esta nueva era digital. Recordemos que una de las principales características o el cambio de paradigma inherente a la libre circulación de decisiones judiciales es el uso de plantillas electrónicas estandarizadas, dado que se basa en una confianza mutua que hace innecesario que la autoridad judicial de ejecución revise los "méritos del caso". Por ello, como quiera que los instrumentos reducen el intercambio de datos a los verdaderamente necesarios y limitan drásticamente la posibilidad de adjuntar documentos o decisiones subyacentes, las plataformas digitales puestas en marcha aparecen como el contexto adecuado para sacar de este nuevo paradigma de la cooperación todo su potencial.

Francisco Jiménez-Villarejo Fernández
Fiscal de Sala de Cooperación Penal Internacional de la Fiscalía General del Estado.

Presentación

A ligação entre a tecnologia e o direito penal não é, por tradição, a mais óbvia.

Enquanto forma de reação do Estado a um ataque aos valores e às liberdades fundamentais da sociedade, o direito penal está profundamente enraizado na sua cultura social, reproduzindo o seu conjunto de valores comuns.

Assim, e porque as mudanças culturais são, geralmente, fenómenos de evolução lenta, também o direito penal tende a ser uma realidade pouco dada a mudanças bruscas, sendo-lhe, antes, atribuído um papel de consolidação de processos em conjuntos de regras que refletem o quadro de valores sociais comummente aceites e sedimentados.

Com efeito, a severidade da reação penal traz implícita a ideia de que a rejeição de uma certa conduta é partilhada por uma vasta maioria da comunidade, tal como a despenalização de uma determinada conduta tende a provocar, pelo menos no início, uma reação negativa. Se assim não for, o legislador estará a impor, à margem dos mais elementares princípios do Estado de direito democrático, valores e regras que não refletem os sentimentos e as opiniões gerais dessa comunidade.

Por outro lado, isso implica, também, que o cidadão compreenda, em cada caso, a interligação entre a conduta penalmente relevante e a respetiva estatuição normativa: não se pode legitimamente esperar que evite comportamentos criminosos se não conhece, plena e adequadamente, o que a lei considera ser uma conduta socialmente desvaliosa.

Assistimos, nas últimas décadas, ao desenvolvimento acelerado e exponencial de novas tecnologias de informação e de comunicação que atravessam todas as áreas da vida em sociedade. A expansão das redes e plataformas digitais e o recurso aos *big data* e à Inteligência Artificial tornam evidentes os desafios atuais que a tecnologia coloca à democracia e ao Estado de Direito.

O ritmo das nossas sociedades, da economia e da vida das pessoas, dominado pela utilização destas tecnologias, exige também respostas da Justiça que possam ir ao encontro das expetativas dos cidadãos e reforcem a transparência, assegurem a *accountability* e promovam a confiança nas Instituições e nos profissionais da Justiça.

A incorporação, crescente e consolidada, das novas tecnologias na Administração da Justiça, a digitalização dos processos e a utilização de ferramentas de Inteligência Artificial tornaram-se, por isso, incontornáveis, na perspetiva da efetivação do direito a uma justiça célere e independente e a um processo justo e equitativo, do aproximar da justiça dos cidadãos e no imperativo político de não deixar ninguém para trás, num ambiente de uma "justiça centrada nas pessoas".

Por todas estas razões, o tema da transformação digital constitui um eixo fundamental da estratégia de governação para fortalecer a União Europeia e continua a ser uma aposta firme do Ministério da Justiça de Portugal, num quadro e contexto mais globais e abrangentes de uma modernização da Justiça.

Afetando todos os domínios da justiça, as novas tecnologias conseguiram chegar, inclusivamente, até ao núcleo estável do direito penal.

A primeira manifestação no domínio do direito penal ter-se-á verificado ao nível do direito penal substantivo, onde, há pelo menos duas décadas, os legisladores europeus começaram a focar a sua atenção sobre novas formas emergentes de criminalidade, praticadas no mundo desmaterializado das tecnologias de informação, procurando estabelecer regras comuns para a incriminação de determinadas condutas e para questões processuais, regras de competência e de jurisdição e de cooperação internacional.

Recordo, aqui, a Convenção sobre Cibercriminalidade, aprovada pelo Conselho da Europa em novembro de 2001, da qual são também Parte Portugal e Espanha.

É inegável que a revolução digital, de dimensão global, está a ter repercussões em todos os aspetos da administração da justiça penal.

A transformação das nossas sociedades em sociedades digitais está a determinar mudanças substanciais não apenas no ambiente em que o crime pode ocorrer, mas também na forma como as investigações podem ser desenvolvidas, como a prova pode ser obtida e preservada, ou a que requisitos deve obedecer para ser admissível em tribunal, sobretudo quando estão em causa investigações transfronteiriças.

A revolução digital, além de disponibilizar ferramentas de Inteligência Artificial, permitiu disponibilizar uma enorme quantidade de dados, gratuitos e de fácil acesso, constantemente gerados por dispositivos digitais; introduziu recursos computacionais poderosos, com a capacidade de aceder e tratar quantidades imensuráveis de dados em poucos segundos e com custos de armazenamento muito baixos.

Estas condições estabeleceram as bases para oferecer soluções úteis aos sistemas de justiça criminal, embora nem sempre especificamente adaptadas para tais tarefas.

Disponibilizou também uma nova gama de dados em massa, que podem ser utilizados como prova em processos penais, entre os quais dados de natureza pessoal, merecedores de proteção e tutela penal, e que apenas podem ser utilizados, no âmbito da investigação e do processo penal, desde que verificadas determinadas condições.

Foi com essa filosofia que a União Europeia, a par do Regime Geral de Proteção de Dados, aprovou em 2016, uma Diretiva relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais.

A acrescer a estes progressos que permitiram a digitalização completa (ou, pelo menos, significativa) do acervo de decisões produzidas pelos tribunais, o acesso ilimitado a essas bases jurisprudenciais possibilitou, também, com a ajuda de poderosos softwares de análise, encontrar padrões de previsibilidade dentro das decisões judiciais.

Durante muito tempo todos estes progressos –e muitos outros que foram aqui tratados– foram desenvolvidos à margem de um diálogo entre a comunidade científica que lidera a transformação digital e os especialistas em direito penal, incluindo os profissionais do direito, mas também o legislador e a própria academia.

Tenho para mim que a comunidade jurídica deve ser o pilar principal da discussão relativa à introdução de Inteligência Artificial e de outras tecnologias inovadoras no processo penal, considerado na sua globalidade: desde os fenómenos criminosos emergentes à respetiva investigação e perseguição penal, incluindo a decisão e as consequências do crime, tanto para a vítima quanto para o agente, mas também para a sociedade em geral, cujos valores foram violados por aquelas condutas.

As realizações e os desenvolvimentos futuros das novas tecnologias na justiça penal devem ser enquadrados numa abordagem jurídica sólida, atualizada e multidisciplinar.

Para que as soluções de Inteligência Artificial e outras novas tecnologias possam ser aplicadas no âmbito do processo penal, devem ser pensadas, concebidas e aplicadas para servirem os objetivos específicos da justiça penal.

Neste campo, a validação de cada nova ferramenta a introduzir no terreno não pode assentar unicamente em parâmetros e normas científicas ou na mera consideração do seu potencial para acrescentar precisão, eficiência, economia de custos e rapidez a tarefas específicas a realizar neste âmbito.

Devem, por isso, ser tidos sempre em conta os valores e as garantias processuais estabelecidas tanto pelas constituições nacionais como pelos sistemas internacionais de proteção de direitos, tais como a proteção da vida privada e familiar ou a salvaguarda do direito a um processo justo e equitativo.

Assim, este esforço não pode deixar de assentar no estabelecimento de um equilíbrio entre a preservação das oportunidades associadas à implementação de cada sistema e a mitigação dos respetivos riscos, tendo sempre o respeito pelos direitos fundamentais como princípio orientador.

Concretamente, caberá garantir que as questões atinentes à responsabilização, transparência e responsabilidade são devidamente acauteladas, sem, contudo, ignorar a imprescindível necessidade de manter o ser humano no controlo dos processos e de prevenir eventuais discriminações ocultas.

Por isso, creio ser essencial, desde logo, assegurar que as decisões tomadas com recurso a estas tecnologias possam ser devidamente explicadas e justificadas aos respetivos utilizadores ou destinatários, cumprindo garantir que estes compreendem adequadamente todo o mecanismo de tomada de decisões para que possam, em cada caso, proceder ao seu escrutínio de forma justa e esclarecida.

No mesmo sentido, não podemos abstrair das preocupações de transparência, entendida enquanto capacidade para descrever, inspecionar e reproduzir os mecanismos e algoritmos através dos quais estes sistemas tomam decisões e aprendem a adaptar-se ao seu ambiente, bem como a proveniência e a dinâmica dos dados que por ele são utilizados e criados.

Além disso, ao nível da responsabilidade, não pode ignorar-se o papel das pessoas na sua relação com estas tecnologias, em particular com a Inteligência Artificial: à medida que a cadeia de responsabilidades cresce, há que assegurar meios idóneos para ligar cada decisão dos sistemas aos dados neles introduzidos e às ações das partes envolvidas em processo.

Tais elementos assumem importância capital no âmbito da justiça penal, porquanto a utilização destas tecnologias de Inteligência Artificial não deve permitir a utilização de "decisões automáticas", não pode substituir o papel do magistrado na formação da decisão judicial e não deve poder enviesar ou interferir negativamente na fundamentação dessa decisão.

As tecnologias de Inteligência Artificial devem ser um auxiliar do magistrado, respeitando a sua legitimidade exclusiva e o seu poder de decisão e a independência dos tribunais, mantendo-se, assim, a dimensão humana na administração da justiça, o respeito pelos direitos fundamentais e garantindo-se um processo justo e equitativo, transparente e público.

Sublinho, por isso, que a dinâmica resultante de um diálogo multidisciplinar abrangente e inclusivo –como aquele que aqui teve lugar– é essencial para assegurar a boa governação digital e fornecer ao legislador contributos decisivos na busca das soluções que hão de fornecer o enquadramento jurídico para a consideração das várias questões emergentes da utilização destas tecnologias e do seu impacto no âmbito da justiça em geral e da justiça penal em particular.

A evolução tecnológica destes sistemas é contínua. No plano da Justiça, estamos apenas no início de uma caminhada em que nos é dada uma oportunidade única para criarmos um quadro jurídico europeu exigente para a utilização da Inteligência Artificial na função de julgar, em particular nos processos de natureza penal, no que respeita à criação de salvaguardas e garantias de não discriminação, à proteção de dados pessoais e à anonimização das decisões para efeitos de publicação.

É essencial definir conjuntamente estas regras e impor as devidas limitações éticas à conceção e à utilização destas tecnologias, no estrito respeito pelos direitos fundamentais e pela dignidade da pessoa humana.

Impõe-se, por isso, uma abordagem sistemática de integração e interoperabilidade, baseada na identificação de necessidades e de recursos, em parceria com a indústria e com o setor privado, sempre orientada pelos objetivos do Direito Penal e das leis de processo e pelas finalidades que este visa prosseguir.

Não é, disso estou convicto, uma tarefa para apenas um sector da sociedade, antes requer uma cultura de abertura e de cooperação entre académicos, profissionais do Direito, investigadores criminais, criadores, decisores políticos e especialistas em ética e Inteligência Artificial, a fim de assegurar que a regulamentação cria os incentivos ao desenvolvimento que beneficiem tanto a evolução das tecnologias como a própria sociedade.

Todos temos responsabilidades diferentes, mas todos temos o direito e o dever de estar envolvidos na discussão do impacto que queremos que estas tecnologias assumam nas nossas sociedades, nas nossas vidas e nos nossos direitos.

Pela nossa parte, no Ministério da Justiça, estamos firmemente empenhados nesta caminhada de uma abrangente modernização da Justiça e, por isso, acompanhamos as discussões no Conselho da Europa, na União Europeia e de outras Organizações como a OCDE, em matéria de digitalização da Justiça, tendo sempre presente o Estudo sobre "Justiça Penal Digital" e o Estudo sobre a "Utilização de Tecnologias Inovadoras no domínio da Justiça" apresentados pela Comissão Europeia.

Os debates que aqui tiveram lugar foram, estou seguro, oportunos e esclarecedores sobre as várias dimensões a considerar na aplicação das novas tecnologias no âmbito da justiça penal.

Congratulo, por isso, a organização desta conferência e agradeço a todos os intervenientes pelos contributos e pelo valor acrescentado que trouxeram a estas discussões.

Aguardamos, com sincera expectativa, futuras iniciativas neste âmbito e deixo aqui a nossa abertura para a continuidade deste diálogo, lançando o desafio de, tão rápido quanto a evolução desta matéria assim o imponha, ser repetida a iniciativa em Espanha.

Muito obrigado.

Jorge Costa

Secretário de Estado Adjunto e da Justiça
Açores, 13 e 14 de junho de 2022

I

El uso de los datos personales y las nuevas tecnologías en el proceso penal

Capítulo 1

Limitaciones en el uso de la información y los datos personales en un proceso penal digital

Ignacio Colomer Hernández

Catedrático de Derecho Procesal
Universidad Pablo de Olavide de Sevilla

I. DELIMITACIÓN DEL OBJETO DE ESTUDIO[1]

El proceso penal es, sin duda, una de las instituciones jurídicas que más capacidad de afectación de los derechos fundamentales tiene, toda vez que la clásica tensión entre libertad y seguridad encuentra en él un campo abonado para su desarrollo. Las investigaciones penales requieren en muchas ocasiones la adopción de medidas que afectan y restringen los derechos de las personas para la obtención de información, datos y evidencias que luego puedan ser utilizados en el juicio oral como pruebas de cargo o de descargo.

En este sentido, es posible constatar que el proceso penal se encuentra actualmente en un período de transición y cambio en el que se van incorporando las nuevas tecnologías de la Sociedad de la Información, lo que está produciendo una transformación hacia un proceso penal digital, o más precisamente, un cambio hacia un proceso penal en el que las principales de fuentes de prueba son digitales, por extraerse de la actividad digital que desarrollan los sujetos.

En España la reforma operada por la LO 43/2015 de reforma de la LECrim ha servido para introducir cambios en la instrucción de los delitos al prever nuevas medidas de investigación tecnológicas, que, no debe

1. Trabajo realizado en el seno del Proyecto PGC2018-095735-B-I00, financiado por FEDER/Ministerio de Ciencia e Innovación – Agencia Estatal de Investigación sobre "*Límites a la utilización de datos, evidencias e información entre procesos y procedimientos diversos en España y la Unión Europea*" (LUDEI).

perderse de vista, tienen una importante capacidad de obtener información y datos de los ciudadanos objeto de la investigación[2]. De manera que en la actualidad el acceso a la información y los datos personales[3] que se encuentran en formato digital se ha convertido en una "autopista" hacia una posible afectación de derechos fundamentales de las personas (tales como, la intimidad, el derecho al entorno virtual, el secreto de las comunicaciones, la protección de datos personales, etc.) en el seno de los procesos penales, bien a través de diligencias de investigación tecnológicas, bien a través de la aportación de esa información y esos datos personales por parte de personas particulares o empresas que los tienen o los poseen de forma legítima, cuando los hayan obtenido con el consentimiento de sus titulares, o de forma ilegítima, cuando los hayan conseguido al margen del consentimiento de sus titulares.

Por ello, en el presente trabajo se va a analizar, en primer lugar, la relación existente entre las nuevas tecnologías, los datos personales y la prueba penal. Para en un segundo momento, abordar el régimen jurídico que presenta la obtención de datos e información personal por parte de los particulares y por parte de las autoridades competentes para su uso como prueba en el proceso penal. Y, finalmente, estudiar la posible exclusión probatoria de la información y los datos personales que se hayan obtenido sin cumplir con las exigencias establecidas en la normativa de protección de datos personales para su uso en los procesos penales.

II. NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN, DATOS PERSONALES Y PRUEBA PENAL

En la era digital en la que vivimos existe un cúmulo de información y datos que se encuentran, se almacenan y se transmiten a través

2. En la actualidad el trabajo más completo sobre datos personales y proceso penal es el de MONTORO SÁNCHEZ, J. A., *Uso y cesión de datos de carácter personal en el proceso penal*, Aranzadi Thomson-Reuters, Cizur Menor, 2022, 528 pp.

3. Sobre la estrecha relación entre los datos, algoritmos y las nuevas tecnologías se puede ver, BARONA VILAR, S., *Algoritmización del derecho y de la justicia: De la inteligencia artificial a la Smart Justice*, Tirant lo Blanch, 2021; MARTÍN DIZ, F., "Inteligencia artificial y derecho procesal: luces, sombras y cábalas en clave de derechos fundamentales", en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 969-1006; COLOMER HERNÁNDEZ, I., "Control y límites en el uso de la información y los datos personales por parte de la Inteligencia Artificial en los procesos penales" en *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, Barona Vilar, S. (edit.), Tirant lo Blanch, 2021, pp. 287-308; HUERGO LORA, A. "Una aproximación a los algoritmos desde el Derecho Administrativo" en *La regulación de los algoritmos*, Dir. Huergo Lora, A., Thomson-Reuters Aranzadi, Cizur Menor, 2020.

de dispositivos e instrumentos digitales. Esta digitalización de la vida corriente ha traído unas mayores posibilidades para el acceso a la información y a los datos personales que se recogen en formato digital[4]. De hecho, es usual y ordinario que la información personal se pueda encontrar tanto en redes sociales, como en otros canales abiertos o incluso en canales cerrados dependientes de la voluntad de sujetos, lo que ha provocado que la información personal haya pasado a constituir una mercancía más, que se transmite de forma onerosa o gratuita, y que con suma frecuencia cambie de manos entre las personas y las empresas[5]. No hay duda que, esta facilidad en el acceso a la información y a los datos en formato electrónico, ha determinado que en la ciudadanía se haya generado una cierta consciencia acerca de una inexistente libertad en relación con la obtención, uso y tratamiento de los datos personales.

Esta percepción, acerca de que la existencia de un cierto acceso libre a la información y a los datos permite su uso sin limitaciones, ha calado no solo en la ciudadanía en general, sino también en los abogados que introducen informaciones y datos personales en los procesos sin observar las exigencias que conlleva la protección de datos personales. Y es que, en efecto, la aparente libertad en el acceso a la gran mayoría de la información y de los datos no se corresponde con los límites que para la obtención, tratamiento y cesión de los datos personales se han introducido en el ordenamiento de la Unión Europea y por ende en nuestro Derecho. Estos límites en el tratamiento y cesión de los datos personales han venido impuestos desde el reconocimiento y cristalización de un derecho fundamental, el derecho a la protección de datos personales, que no se

4. Como señala VELASCO NÚÑEZ en relación con los datos personales que se obtienen e incorporan al proceso penal a través de las nuevas tecnologías, "*los atestados policiales, informes, periciales y resto de diligencias de investigación que el Juez instructor incorpora al proceso penal, pueden exhibir excesiva información afectante no ya sólo al derecho fundamental a la protección del dato en sus diversas facetas, sino igualmente a otros recogidos también en el Art. 18 CE (como el de a la intimidad, propia imagen, secreto telecomunicativo, …) que requieren un tratamiento específico, muy cuidadoso, no sólo cualitativo –por las garantías que exige– sino también cuantitativo –por el exceso de información–, a veces muy estigmatizante, que puede conllevar*" (*cfr*. "Investigación penal y protección de datos" en *El Cronista del Estado Social y Democrático de Derecho*, n.º 88-89, 2020, p. 139).

5. Como señala PÉREZ GIL "*son estos, los datos electrónicos, los que han de constituir una nueva categoría en las normas procesales (el género) mientras que los que se generen a partir de comunicaciones serán una especie dentro de ellos, ciertamente con particularidades determinantes, pero al fin y al cabo una entre muchas. Identificado el problema, habrá que dársele respuesta en futuras reformas procesales: la singularidad de la regulación de esta materia debe venir por la atención al formato en el que se encuentra la información electrónica en forma de datos y la especificidad que de ello se deriva*" *Cfr*. "Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal" en *Justicia: ¿garantías versus eficiencia?*, Jiménez Conde, F. y Bellido Penadés, R. (dir.), Llopis Nadal, P. y De Luis García, E. (coord.), Tirant lo Blanch, Valencia, 2019, p. 423.

encontraba en el catálogo clásico de derechos y garantías de los ciudadanos integrados en el bloque esencial de la constitucionalidad.

En este sentido, hay que recordar que la Carta de Derechos Fundamentales de la Unión Europea ha supuesto el reconocimiento del derecho a la protección de datos como un derecho autónomo e independiente respecto al derecho a la vida privada y familiar. Su reconocimiento se realizó en el artículo 8 CDFUE[6] bajo la rúbrica "Protección de datos de carácter personal"[7]. En este artículo, junto al general reconocimiento del derecho a la protección de datos, se establecen en su número 2, de un lado, los principios básicos que deben regir el tratamiento de los datos personales, lealtad y limitación de la finalidad; y de otro lado, las bases que legitiman el tratamiento, que se concretan en el consentimiento del interesado, dejando abierta la posibilidad de que el legislador establezca otros fundamentos.

En 2016 se aprobó un importante paquete normativo para la protección y desarrollo del derecho a la protección de datos. De una parte, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; y de otra parte, la Directiva (UE) 2016/680[8]

6. *"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*

   2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

   3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

7. Para un análisis del contenido del artículo 8 CDFUE ver, entre otros, ÁVILA RODRÍGUEZ, C. M., "Artículo 8. Protección de datos de carácter personal" en *La Europa de los derechos: estudio sistemático de la Carta de los derechos fundamentales de la Unión Europea*, MONEREO ATIENZA, C. y MONEREO PÉREZ, J. L. (coords.), Comares, Granada, 2012, pp. 157-180; ABERASTURI GORRIÑO, U., "El derecho a la protección de datos de carácter personal. La autodeterminación informativa como derecho autónomo en la Carta de derechos fundamentales de la Unión Europea" en *La Carta de los Derechos Fundamental de la Unión Europea y su reflejo en el ordenamiento jurídico español*, Aranzadi Thomson-Reuters, Cizur Menor, 2014, pp. 161-176.

8. Un análisis general sobre el contenido de la Directiva se puede encontrar en GONZÁLEZ CANO, I., "Cesión y tratamiento de datos personales, Principio de Disponibilidad y cooperación judicial penal en la Unión Europea", en *Cesión de datos personales y evidencias entre procesos penales y procedimientos sancionadores o tributarios*, Colomer Hernández, I. (dir.), Oubiña Barbolla, S. y Catalina Benavente, M. A. (coord.), Thomson-Reuters Aranzadi, Cizur Menor, 2017, pp. 59-79; "Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la directiva (UE) 2016/680" en *Revista Brasileira de Direito Processual Penal*, núm. 3, 2019, pp. 1331-1384; "Garantías del investigado y acusado en orden a la obtención, cesión y tratamiento de datos personales en el proceso penal. A propósito de la Directiva (UE) 2016/680 y su impacto en materia de prueba penal" en González Cano (coord.) *Orden Europea*

del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[9]; y la Directiva (UE) 2016/681 del Parlamento y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (Directiva PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave[10]. La Directiva (UE) 2016/680 ha sido traspuesta por la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

En el Derecho español el reconocimiento del derecho a la protección de datos personales como derecho fundamental apareció vinculado inicialmente a la previsión contenida en el artículo 18.4 de la Constitución, como derecho a la autodeterminación informativa[11]. Sin embargo, una

---

de Investigación y prueba transfronteriza en la Unión Europea, Tirant Lo Blanch, Valencia, 2019, pp. 98-154. También los trabajos de PILLADO GONZÁLEZ, E., "Principios generales de protección de datos en la cesión de información en la persecución criminal a la vista de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por la que se deroga la Decisión Marco 2008/977" en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 783-820; "Difícil equilibrio entre seguridad y salvaguarda del derecho a la protección de datos personales en la prevención, investigación y represión de delitos en la unión europea" en *Integración europea y justicia penal*, González Cano (dir.), Tirant Lo Blanch, Valencia, 2018, pp. 515-559. COLOMER HERNÁNDEZ, I., "Control y límites en el uso de los datos personales penales en la investigación y represión de los delitos a la luz de la Directiva 2016/680" en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 737-782.

9. Para un análisis de los antecedentes de la Directiva se puede ver PÉREZ-LUÑO ROBLEDO, E., "La garantía procesal de los datos personales en la Carta de Niza como fundamento de la Directiva 2016/680 UE", en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 957-968; FIODOROVA, A., "Directiva 2016/680: hacia mayor coherencia de protección de datos personales en la cooperación policial y judicial penal" en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 709-736.
10. Sobre el uso de los PNR en los procesos penales, ver CATALINA BENAVENTE, M. A., *El uso de los datos PNR en el proceso penal*, Aranzadi Thomson-Reuters, Cizur Menor, 2022, 230 pp.
11. En la STC 254/1993, de 20 de julio se reconoce la existencia de un derecho fundamental de la persona a la autodeterminación informativa que encuentra su anclaje en el artículo 18.4 Constitución. En concreto, el Tribunal señala que: "*en el presente*

evolución en la doctrina del Tribunal Constitucional, muy en particular a partir de la importante STC 292/2000, llevó al reconocimiento del derecho a la protección de datos como derecho autónomo y diferenciado del derecho a la intimidad[12]. En palabras, del Tribunal Constitucional *"el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información"*[13].

El derecho a la protección de datos *"atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer"*.

En consecuencia, la esencia de este derecho a la protección de datos, a juicio del interprete constitucional, se concreta en *"que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos"*[14]. Y esta necesidad o no del consentimiento es un elemento esencial, como se analizará más tarde, para valorar la admisibilidad del uso y tratamiento de los datos personales en el proceso penal, en particular para su empleo como prueba o evidencia de los hechos controvertidos.

Por último, es necesario también poner de relieve el carácter limitado del derecho a la protección de datos, puesto que, como ha señalado el Tribunal Constitucional, *"el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales,*

---

caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'" (FJ 6.º).

12. El derecho a la protección de datos "*atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer"* (STC 292/2000, de 30 noviembre. FJ 6.º).
13. STC 292/2000, de 30 noviembre. FJ 6.º.
14. En igual sentido, ya se había indicado en la STC 254/1993, identificándolo con el poder de disposición sobre los datos personales.

no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, FJ 7; 196/1987, de 11 de diciembre, FJ 6; y respecto del art. 18, la STC 110/1984, FJ 5)"[15].

El reconocimiento de la naturaleza limitada de este derecho, que por otra parte no constituye algo extraordinario en la configuración constitucional de los derechos fundamentales, ha sido, sin embargo, usado por el CGPJ, más concretamente por el órgano del mismo encargado de la protección de datos en el ámbito jurisdiccional[16], para precisamente adoptar resoluciones en las que el derecho a la protección de datos[17] se ha contrapuesto con el derecho a la tutela judicial efectiva, con la indeseable consecuencia de privar de eficacia en el ámbito jurisdiccional a la protección de datos[18]. Sin embargo, no se puede compartir la argumentación que se realiza en la Resolución, sobre la base del carácter limitado del derecho a la protección de datos, para confrontarlo con el derecho a la tutela judicial efectiva y extraer como consecuencia la consideración de que en el seno de los procesos la protección de datos deba ceder ante el derecho a la tutela judicial efectiva. Dicho, en otros términos, esta Resolución es una muestra clara de una confusión en cuanto a las dimensiones que concurren en esta cuestión. Pues, de lo que se trata, no es que el derecho a la tutela judicial efectiva sea un límite del derecho a la protección datos y éste deba ceder por ello, sino que la efectividad del derecho a la tutela judicial ha de contemplar necesariamente las consecuencias procesales del derecho a la protección de datos personales.

Esta posición es criticable[19] pues no se trata de contraponer protección de datos y derecho a la tutela judicial efectiva, sino que lo que debe

15. STC 292/2000, de 30 noviembre. FJ 11.º.

16. La Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial.

17. Ver, sobre la protección de datos en los tribunales, PÉREZ ESTRADA, M. J. "La protección de los datos personales en los órganos judiciales" en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 895-916.

18. En concreto, la Resolución de 13 de septiembre de 2021 de la Dirección de Supervisión y Control de Protección de Datos del CGPJ señala que "*no puede existir vulneración de la normativa de protección de datos cuando, como en este caso, los términos concretos en que pueda verse afectado el derecho a la protección de datos personales resultan de la ponderación de los derechos y bienes jurídicos constitucionalmente protegidos concurrentes, realizada en el seno de un procedimiento judicial, en la que, al cabo, se otorga prevalencia al otro derecho fundamental presente. En este caso, es el derecho de tutela judicial efectiva sin que pueda producirse indefensión (artículo 24.1 CE) el que, concurriendo con el de protección de datos personales (artículo 18.4 C.E.), actuaría precisamente como límite de este último*".

19. Sin perjuicio de que la Resolución acierta en cuanto a la falta de competencia de la Dirección de Supervisión y Control de Protección de Datos para conocer de cuestiones relativas a la valoración probatoria que el órgano jurisdiccional deba realizar, por

realizarse es una interpretación conjunta e integradora de ambos derechos. De manera que las posibles vulneraciones del derecho a la protección de datos que se cometan en la obtención y tratamiento de datos personales, que vayan a ser usados como fuentes de prueba en un proceso, tenga su plasmación y consecuencia en la actividad jurisdiccional desarrollada, y más concretamente en la valoración probatoria que puedan recibir esos datos personales como pruebas.

Por todo lo cual, es necesario tener presente que el derecho a la protección de datos personales no sólo se circunscribe a ese poder de disposición de las personas sobre sus datos, que el Tribunal Constitucional reconoce desde la STC 292/2000, sino que despliega también sus efectos en el ejercicio de la potestad jurisdiccional en la actividad de valoración de la prueba.

La trascendencia de esta contraposición entre una libertad absoluta de uso de los datos y la información y una libertad condicionada por las exigencias previstas para la licitud del tratamiento de los mismos, se manifiestan en el seno de los procesos desde el punto de vista de la prueba, o más específicamente, desde la óptica de la valoración de los materiales probatorios que tengan acceso al proceso. Y es que no se debe perder de vista que los datos personales son, desde el punto de vista del proceso, una fuente de prueba[20], por cuanto representan la realidad de unos hechos que habrán de tener acceso al proceso a través de distintos medios prueba (la documental, medios de archivo de la palabra o las imágenes, etc.).

Por tanto, se constata la relación existente entre el proceso y el derecho a la protección de datos, reconociendo que este último puede condicionar

---

ser una manifestación estricta de la potestad jurisdiccional, que en caso de ser desarrollada por terceros supondría una clara inmisión en la independencia del órgano jurisdiccional, ya que como indica la Resolución "*no resulta ocioso recordar que, por imperativo del principio de independencia en el ejercicio de potestad jurisdiccional consagrado en el artículo 117 CE, el Consejo General del Poder Judicial no puede pronunciarse en modo alguno respecto del contenido y alcance de las resoluciones adoptadas en un procedimiento judicial por el órgano competente en ejercicio de la función jurisdiccional. Cualquier posible intervención del Consejo General del Poder Judicial en tal ámbito supondría una intromisión en el ejercicio de dicha función que contravendría la prohibición expresamente contenida en el artículo 12.3 de la Ley Orgánica del Poder Judicial*".

20. MONTORO SÁNCHEZ distingue claramente la finalidad identificativa y la finalidad probatoria de los datos personales. Así respecto de la función identificativa señala que "*en primera instancia, los datos personales cumplen la labor de identificar de forma directa o indirecta a todo individuo vinculado o que deba vincularse o intervenir de algún modo en el proceso*"; y respecto de la función probatoria, que es la que a nosotros interesa en el presente trabajo, indica que "*los datos personales también pueden ser utilizados en el proceso con fines probatorios cuando se introduzcan en el proceso como fuente de prueba*" (*cfr. Uso y cesión de datos de carácter personal en el proceso penal*, Aranzadi Thomson-Reuters, Cizur Menor, 2022, p. 289).

la actividad judicial de valoración de prueba. De ahí que sea necesario para un análisis en profundidad de este condicionamiento que, como se verá a continuación, se desarrolla en el momento de la admisión y valoración de la prueba, proceder a realizar una serie de consideraciones en relación con las condiciones que deben cumplirse en la obtención y tratamiento de los datos personales para que puedan servir como fuente de prueba en el proceso penal.

III. TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL

El punto de partida, desde el que hay que iniciar el análisis del tratamiento de los datos personales como fuente de prueba en el proceso penal, pasa necesariamente por tener en cuenta el diverso régimen jurídico que tiene el tratamiento de los datos según que sea realizado por autoridades o por los particulares en relación con un concreto proceso o investigación penal. Y es que necesariamente hay que tener en cuenta que el tratamiento por parte de las autoridades competentes con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales se encuentra regulado en la Directiva (UE) 2016/680 y en la LO 7/2021. Mientras que, por el contrario, el tratamiento realizado por los particulares (el acusador particular, el investigado, la víctima, etc.) se encuentra sometido a las previsiones del Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Esta diversidad en el régimen jurídico aplicable al tratamiento de los datos personales que vayan a poder aportarse al proceso penal como fuentes de prueba[21] tiene evidentes consecuencias que afectan a su admisibilidad y a su posible exclusión al amparo de la previsión contenida en el artículo 11 LOPJ por haber sido obtenidos con vulneración de derecho fundamental a la protección de datos. Por ello, en las próximas páginas se van a delimitar las exigencias y requisitos que vienen impuestos por la normativa protectora del derecho a la protección de datos personales para su uso en el seno de los procesos penales.

21. "*Entendemos, además, que el dato personal, por su incorporación a un proceso de esa naturaleza, tan estigmatizante –protección por destino–, es de los calificados como de categoría, y, en consecuencia, protección 'especial' (Arts. 9 y 10 RGPD), lo que implica que sólo se puede recoger e incorporar (y valorar) para el fin del propio proceso penal (Art. 4.1 b) 2016/680 de Tratamiento con fines de investigación penal), debiendo asegurarse que su aportación garantiza que no se use para otro destino que el probatorio*" (*cfr*. VELASCO NÚÑEZ, *op. cit.*, p. 140).

1. TRATAMIENTO DE LOS DATOS PERSONALES CON FINES PENALES POR PARTE DE LAS AUTORIDADES COMPETENTES

La posibilidad de tratamiento de datos personales con fines penales por parte de las autoridades competentes se encuentra específicamente regulada en la Directiva (UE) 2016/680 y en la LO 7/2021 de trasposición de la norma europea. En concreto, en el artículo 1 de la Ley Orgánica expresamente se identifica como objeto de la norma la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública. De manera que en la Ley se regulan los requisitos, límites y condiciones existentes para que las autoridades competentes puedan proceder al tratamiento de los datos personales de personas, vinculadas o no con el proceso, con la finalidad de prevenir, detectar, investigar o enjuiciar delitos.

Lo primero que hay que tener claro es el concepto de autoridades competentes para el tratamiento de los datos personales con fines penales. Al respecto, la normativa vigente considera que tendrán la consideración de autoridades competentes a estos efectos toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con fin de prevenir, detectar, investigar o enjuiciar delitos (artículo 4.1 LO 7/2021)[22]. Mientras que en el artículo 4.2 se reconoce la habilitación como autoridades competentes para el tratamiento de datos personales con relevancia penal a las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal[23].

Este listado de autoridades competentes ha sido recientemente ampliado por la Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley Orgánica 8/1980, de 22

22. El propio apartado 1 del precepto detalla esa mención genérica a las autoridades públicas considerando que se incluyen dentro de ese concepto *"a) Las Fuerzas y Cuerpos de Seguridad. b) Las Administraciones Penitenciarias. c) La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria. d) El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. e) La Comisión de Vigilancia de Actividades de Financiación del Terrorismo"*.

23. Esta distinción entre los dos apartados del precepto tiene su relevancia, ya que se conecta, como luego se verá, con el distinto régimen jurídico que se aplica al tratamiento de datos por parte de jueces y fiscales (artículo 26 LO 7/2021), respecto del tratamiento de las demás autoridades competentes.

de septiembre, de Financiación de las Comunidades Autónomas y otras disposiciones conexas y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

En concreto, la LO 9/2022 ha introducido como autoridades competentes a la Fiscalía Europea en el ámbito de sus competencias; a las Policías Autonómicas con competencias estatutariamente asumidas en la investigación de delitos graves; y a la Oficina de Recuperación y Gestión de Activos del Ministerio de Justicia y las oficinas de recuperación de activos designadas por España de conformidad con la Decisión 2007/845/JAI, de 6 de diciembre de 2007[24].

En segundo lugar, hay que determinar qué significado tiene el concepto de tratamiento de datos personales en el seno de actuaciones o actividades de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales[25]. A estos efectos, la propia LO 7/2021 recoge el amplio concepto de tratamiento que se maneja en la Directiva (UE) 2016/680 cuando señala que ha de entenderse por tratamiento "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*" (artículo 5 b LO 7/2021). De manera que, por tanto, la recogida, obtención, uso o cesión de datos personales[26] en el seno de las investigaciones policiales y judiciales son

24. De manera que como autoridades competentes quedan habilitadas, de una parte, para acceder y consultar el Fichero de Titularidades Financieras, en el ejercicio de sus respectivas competencias para la prevención, detección, investigación o enjuiciamiento de infracciones penales graves delitos graves (artículo 3.1 LO 9/2022); y de otra parte, para solicitar y recibir información financiera o análisis financieros del Servicio Ejecutivo de la Comisión, en el ejercicio de sus respectivas competencias para la prevención, detección, investigación o enjuiciamiento de infracciones penales graves (artículo 3.2).

25. Una aproximación a esas finalidades del tratamiento de datos con relevancia penal se puede ver en VILLAR FUENTES, I., "Datos personales al servicio de la investigación y detección de infracciones penales" en *Revista General de Derecho Procesal*, n.º 48 (2019), 41 pp.

26. La LO 7/2021 define los datos personales como "*toda información sobre una persona física identificada o identificable ('el interesado'); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*" (artículo 5.a). De lo que se desprende que en la mayor parte de los casos el resultado de las diligencias de investigación de los procedimientos penales podrá tener la consideración

manifestaciones claras de un tratamiento de datos por parte de las autoridades competentes que deberá estar sometido a las exigencias y requisitos establecidos en la LO 7/2021 y en la Directiva (UE) 2016/680.

La tercera de las cuestiones que hay que abordar es identificar las exigencias necesarias para que las autoridades competentes puedan realizar un tratamiento lícito de los datos personales en el seno de las actuaciones de prevención, detección, investigación y enjuiciamiento de delitos. Al respecto, el artículo 11 LO 7/2021 establece de forma taxativa que sólo será lícito el tratamiento en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones. Lo que supone que la licitud del tratamiento de los datos personales con relevancia penal viene determinada, de una parte, por las finalidades que se persigan con su obtención y tratamiento (artículo 6.1 b LO 7/2021); y, de otra parte, por estar realizado por autoridades competentes.

Por lo que se refiere a la finalidad que habilita el tratamiento de datos personales con relevancia penal hay que tener presente que los fines previstos en la norma se concretan en la prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública. Esta identificación genérica contenida en el artículo 1 LO 7/2021 debe ser concretada con la referencia a los principios básicos que rigen el tratamiento de los datos personales[27] con relevancia penal. En particular, según lo dispuesto en el artículo 6 LO 7/2021, que concreta el alcance del principio de finalidad de los datos personales, se pueden distinguir dos dimensiones: (i) Finalidad en la recogida de los datos; (ii) Finalidad en el tratamiento.

En primer lugar, la recogida y obtención de los datos personales debe realizarse con "*fines determinados, explícitos y legítimos*" (artículo 6.1.b LO 7/2021). De manera que en el seno de las investigaciones criminales la recogida y obtención de los datos debe tener lugar para un fin determinado, que resulte claramente explicitado en la actuación que se lleve a cabo, en particular cuando la diligencia de investigación mediante la que se obtengan los datos personales afecte o limite derechos fundamentales,

---

de datos personales, lo que obliga a que en su obtención se hayan respetado las garantías de la protección de datos para su posterior uso en el proceso penal como prueba de cargo o de descargo.

27. En esta materia se puede ver RODRÍGUEZ AYUSO, J. F., "Principios rectores en materia de protección de datos personales" en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 945-956.

y que además resulte legítimo por servir a la finalidad de prevenir, investigar o enjuiciar conductas delictivas.

Con relación a la determinación del fin que motiva la obtención o la recogida de los datos personales es necesario establecer una correspondencia con los principios rectores que presiden la adopción de diligencias de investigación tecnológica mediante autorización jurisdiccional[28], tal como expresamente prevé el artículo 588 bis a) LECrim[29]. En concreto, la necesidad de determinación se encuentra directamente imbricada con el principio de especialidad que debe regir en la adopción de las diligencias de investigación tecnológica[30]. De manera que, si la especialidad exige que una medida de investigación tecnológica esté relacionada con la investigación de un delito concreto, la recogida y la obtención de los datos personales que se consigan en el desarrollo de esa medida de investigación habrá de haber sido realizado de conformidad con un fin determinado y explícito que se concretará en la investigación del delito concreto que esté siendo objeto de la diligencia de investigación. Y, por tanto, la alteración de los hechos que estén siendo objeto de investigación mediante la medida tecnológica supondrá un cambio en la concreta finalidad que habilita la obtención de los datos personales que consecuentemente podrá provocar la falta de licitud de esa recogida, y de su tratamiento ulterior, siempre que ese cambio en el concreto fin no se corresponda con algún caso de descubrimiento casual[31].

Dicho, en otros términos, el fin determinado que habilita la recogida de datos personales en el seno de una investigación tecnológica queda circunscrito a los hechos delictivos que sean objeto de la investigación, sin

28. Sobre el principio de proporcionalidad en relación con la obtención y cesión de datos personales en el proceso penal, ver LARO GONZÁLEZ, E., "Principio de proporcionalidad en la obtención, cesión y tratamiento de datos personales en materia penal" en *Exclusiones probatorias en el entorno de la investigación y prueba electrónica*, González Granda, P. (dir.), Ariza Colmenarejo, M. J. (coord.), Sanjurjo Ríos, E. (coord.), Reus, 2020, pp. 161-174.

29. "*Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida*".

30. Artículo 588 bis a) LECrim "*2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva*".

31. Artículo 588 bis i) LECrim. Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales. "*El uso de las informaciones obtenidas en un procedimiento distinto y los descubrimientos casuales se regularán con arreglo a lo dispuesto en el artículo 579 bis*".

perjuicio de la calificación jurídico penal que puedan revestir[32]. En consecuencia, la habilitación para la recogida de los datos no puede extenderse para hechos diversos de los contemplados en la autorización de la medida tecnológica sin que se produzca un supuesto de descubrimiento casual que, reunidas las exigencias previstas en el artículo 579 bis LECrim[33], podrá, en su caso, permitir que se habilite la recogida de datos mediante la continuación de la medida de investigación tecnológica en relación con los nuevos hechos descubiertos.

En segundo lugar, por lo que se refiere al principio de finalidad en relación con el tratamiento de los datos personales, esto es, para el tratamiento de los datos obtenidos en el desarrollo de una investigación a través de alguna medida tecnológica, se constata también que los fines que habilitan a las autoridades competentes para el tratamiento son los generales previstos en el artículo 1 LO 7/2021, es decir, aquellos incluidos en la finalidad de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales. De manera que, los datos personales obtenidos mediante medidas tecnológicas podrán ser usados para la investigación y el enjuiciamiento de los delitos por parte de las autoridades competentes constituyendo un tratamiento lícito que será acorde con la protección de los datos personales de las personas afectadas, sean partes en el proceso penal o terceros ajenos al mismo[34].

32. El fin que habilita la recogida u obtención de los datos personales por parte de la autoridad competente es la investigación de unos concretos hechos delictivos, con independencia de las posibles modificaciones en la calificación jurídico penal de los mismos que puedan sufrir a lo largo del procedimiento. De modo que, si la medida de investigación a través de la que se recabaron los datos personales estaba dirigida al esclarecimiento de una muerte, la obtención de los datos estará habilitada y será lícita con independencia de que en el curso de la instrucción los hechos delictivos pasen a ser calificados como asesinato cuando inicialmente lo hubieran sido como homicidio. De manera que lo esencial para la lícita obtención de los datos personales a través de cualquier diligencia de investigación, en particular en las que se producen a través de medidas tecnológicas, es que se produzcan en relación con unos concretos hechos delictivos y nunca en investigaciones prospectivas.

33. "*3. La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, éste comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo, se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce".*

34. Sobre el tratamiento de los datos personales de terceros en el proceso penal ver DE LEMUS VARA, F. J., "Límites para el tratamiento de los datos de los no investigados en el proceso penal" en *Uso de la información y de los datos personales en los procesos: los cambios en la Era Digital*, Colomer Hernández, I. (dir.), Catalina Benavente, M. A. y Oubiña Barbolla, S. (coord.), Aranzadi Thomson-Reuters, Cizur Menor, 2022, pp. 545-570.

Ahora bien, en relación con los fines que habilitan el tratamiento lícito de los datos personales, tanto la Directiva (EU) 2016/680 como la LO 7/2021, contemplan la posibilidad de que se produzca algún cambio o modificación en los fines para los que son tratados los datos y para ello establecen un régimen diferenciado según que la modificación de la finalidad sea respecto a fines de naturaleza penal o no. Es necesario distinguir, por tanto, dos posibilidades en relación con los eventuales cambios en la finalidad del tratamiento de datos personales: de un lado, los casos en los que la nueva finalidad resulte ajena a los fines penales previstos en el artículo 1 LO 7/2021; y de otro lado, los supuestos en los que se produzca un cambio en la concreta finalidad de naturaleza penal habitante del tratamiento, pero manteniéndose dentro de alguno de los fines previstos en el indicado precepto.

El primero de los supuestos, los cambios en la finalidad para la que habrán de ser tratados los datos personales que hayan sido recogidos u obtenidos por una autoridad competente bajo la habilitación de un fin penal, como por ejemplo la investigación de un delito, se encuentra regulado en el artículo 6.2 LO 7/2021. Al respecto, el precepto establece una clara proscripción para que los datos personales recogidos por las autoridades competentes no sean tratados para otros fines distintos de los establecidos en el artículo 1, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por la legislación española. Lo que supone que los datos personales que hayan sido recogidos al amparo de la habilitación penal, como esencialmente puede ser la investigación de un delito a través de una medida tecnológica, solo podrán ser tratados o usados para una finalidad ajena al fin penal cuando esté autorizado por una norma del Derecho de la Unión Europea o por la legislación europea. Es decir, los datos personales obtenidos al amparo de una finalidad penal solo podrán dedicarse a una finalidad no penal cuando exista habilitación expresa de una norma de la UE o española.

La trascendencia de este límite en relación con el tratamiento de datos personales obtenidos en la investigación de delitos es de suma relevancia, ya que los datos obtenidos en el desarrollo de una medida de investigación tecnológica no podrán ser tratados para fines no penales, como por ejemplo su uso en un proceso civil, sin que exista esa habilitación legal que lo autorice. Pero, aún más, el propio artículo 6.2 LO 7/2021 no solo requiere esa expresa autorización, sino que en los casos en que exista la habilitación legal para el tratamiento para fines no penales se aplicará el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre. De modo que el tratamiento para fines no penales de datos personales obtenidos bajo la habilitación de un fin penal estará sometido

a las exigencias generales de la protección de datos, lo que supone que, como regla general, la licitud del tratamiento vendrá condicionada al consentimiento del titular de los datos[35].

Un segundo grupo de casos está constituido por aquellos en los que el fin penal habilitante del tratamiento de los datos sea distinto de aquel que permitió su recopilación y obtención. Al respecto, el artículo 6.3 LO 7/2021 prevé que *"los datos personales podrán ser tratados por el mismo responsable o por otro, para fines establecidos en el artículo 1 distintos de aquel para el que hayan sido recogidos, en la medida en que concurran cumulativamente las dos circunstancias siguientes: a) Que el responsable del tratamiento sea competente para tratar los datos para ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española. b) Que el tratamiento sea necesario y proporcionado para la consecución de ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española"*.

Ambas exigencias deben concurrir simultáneamente, de manera que el fin penal distinto del que inicialmente permitió el tratamiento de los datos solo podrá ser desarrollado por alguna autoridad competente responsable del nuevo tratamiento cuando éste sea necesario y proporcionado para la consecución de ese nuevo fin.

En consecuencia, en la práctica esta posibilidad de cambio en el fin penal habilitante del tratamiento de los datos se produce en dos supuestos: de un lado, en los casos de hallazgos casuales en el curso de diligencias de investigación, en particular en las que se desarrollan a través de medidas tecnológicas (artículo 579 bis y 588 bis i LECrim); y de otro lado, los casos de uso en un procedimiento distinto de los datos personales obtenidos en el seno de una investigación criminal (artículo 588 bis i LECrim).

En los supuestos en que se produzca un hallazgo casual en el seno de la práctica de unas medidas tecnológicas de investigación las exigencias de necesidad y proporcionalidad, que impone el artículo 6.3 LO 7/2021 para un tratamiento de los datos con un fin penal distinto, se han de concretar en los requisitos que el artículo 579 bis LECrim establece. De manera

35. Imaginemos que en el curso de una investigación por un delito grave se procede al registro de un ordenador, obteniéndose datos de naturaleza financiera del investigado, que no olvidemos son datos personales recogidos con un fin penal de investigación de un delito, pero que posteriormente el acusador particular pretenda usarlos en un proceso civil ajeno a la responsabilidad civil *ex delicto*, lo que supondría un uso para fin no penal, que debería estar autorizado por una ley, y que en todo caso estaría sometida al Reglamento General de Protección de datos y a la LO 3/2018, lo que exigirá, para la licitud de ese tratamiento para fines no penales, que ese uso y tratamiento para un fin no penal sea consentido por el titular de los datos (artículo 6.1.1 RGDP).

que, para el tratamiento de los datos personales hallados casualmente se requiere que el juez de instrucción proceda a verificar la legitimidad de la injerencia[36] que ha permitido llevar a cabo la medida de investigación restrictiva de los derechos fundamentales en la que se ha obtenido casualmente la información personal que se va a tratar, esto es, que se va a usar en la investigación o enjuiciamiento de un delito distinto[37].

Para los casos en los que los datos personales obtenidos en una investigación de un concreto delito se vayan a usar/tratar en otro procedimiento distinto resulta claro que las dos exigencias de necesidad y proporcionalidad del nuevo tratamiento sólo podrán concurrir si el nuevo procedimiento es de naturaleza penal. Ello significa, por tanto, que el cambio de la concreta finalidad que permita el tratamiento lícito de esos datos solo podrá justificarse si su cesión se produce a otro proceso penal, y no en cambio si se usan en un proceso de otra naturaleza[38].

Por otra parte, buena prueba de la transcendencia que tiene el principio de limitación de la finalidad en el tratamiento de los datos personales en el seno de los proceso la podemos encontrar en el hecho de que el Reglamento (UE) 1783/2020 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020 relativo a la cooperación entre los órganos jurisdiccionales de los Estados miembros en el ámbito de la obtención de pruebas en materia civil o mercantil (obtención de pruebas), que ha entrado en vigor muy recientemente, recoja expresamente el principio de finalidad

36. Artículo 579 bis LECrim "*2. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen*".

37. Sobre el tratamiento de los hallazgos casuales resulta interesante la Sentencia del Tribunal Supremo (Sala Tercera) 3162/2022 de 26 de julio cuando indica que "*la Administración tributaria no puede realizar válidamente comprobaciones, determinar liquidación eso imponer sanciones a un obligado tributario tomando como fundamento fáctico de la obligación fiscal supuestamente incumplida los documentos o pruebas incautados como consecuencia de un registro practicado en el domicilio de terceros (aunque se haya autorizado la entrada y registro por el juez de esta jurisdicción), cuando tales documentos fueron considerados nulos en sentencia penal firme, por estar incursos en vulneración de derechos fundamentales en su obtención. Aun cuando tal declaración penal no se hubiera llevado a cabo formalmente, la nulidad procedería delo establecido en el art. 11 LOPJ, conforme al cual 'no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales'*".

38. Hay que tener en cuenta que esos datos personales obtenidos por una autoridad competente en el seno de una investigación penal, particularmente si se han obtenido a través de medidas que limiten derechos fundamentales, no pueden ser cedidos para ser usados en otros procedimientos de naturaleza no penal si no es de acuerdo a las exigencias que marca con carácter general el Reglamento (UE) 2016/679 y que se concretan en la necesidad de contar con el consentimiento del titular de los datos.

en cuanto a los datos y la información personal que se hayan podido recopilar en la actividad de obtención de pruebas en el seno de la cooperación entre órganos jurisdiccionales de los Estado miembros de la UE.

En el artículo 30 del Reglamento (UE) 1783/2020, con una rúbrica muy ilustrativa de su contenido "*Protección de la información transmitida*", expresamente se exige que todo tratamiento de datos personales realizado al amparo del Reglamento de obtención de pruebas en materia civil o mercantil, incluidos el intercambio o la transmisión de datos personales por las autoridades competentes, deberá ser conforme al Reglamento (UE) 679/2016. Lo que implica una clara declaración de principios conforme a la cuál la obtención de pruebas en el seno de la cooperación jurisdiccional entre Estados miembros de la UE tiene que respetar, en todo caso, las exigencias del derecho a la protección de datos, tal y como se prevé en el RGPD.

En concreto, en aplicación de la necesaria protección de datos en esta actividad de obtención de prueba expresamente se prevé que *"los datos personales que no sean pertinentes para la tramitación de un caso específico se eliminarán inmediatamente"* (artículo 30.1). De forma que, como regla general, no resulta aceptable la conservación de datos o informaciones personales que se hayan podido recopilar en una actividad de obtención de prueba transfronteriza que no sean pertinentes para el desarrollo del concreto y específico caso para el que se hayan obtenido, debiendo ser eliminados de inmediato. Esta clara e inequívoca prescripción que impone el legislador europeo resulta extremadamente importante, puesto que supone que la obtención de pruebas, en el caso de la norma cuando la obtención tenga lugar de forma transfronteriza, está limitada y condicionada por el concreto objeto, esto es por el caso, que se esté ventilando o se pueda tramitar ante los tribunales civiles o mercantiles.

Dicho de otro modo, los datos personales y la información personal que pueda obtenerse en la recopilación llevada a cabo en la obtención de la prueba transfronteriza sólo podrá ser usada en el concreto pleito y asunto para el que se haya recopilado, sin que pueda ser conservada o usada en casos diversos de aquel que sea objeto del procedimiento en el que se hayan obtenido. Hay que tener presente que se ordena la eliminación de todos aquellos datos personales obtenidos en la diligencia transfronteriza de cooperación jurisdiccional que no resulten pertinentes para la tramitación del caso específico, lo que significa que no estén vinculados con el concreto objeto de ese procedimiento.

Además de esa vinculación de la recopilación y tratamiento de los datos personales como fuentes de prueba con el específico caso para el que se obtengan, el propio Reglamento recoge expresamente la vigencia

del principio de limitación de la finalidad para esta clase de tratamientos. Puesto que en el número 3 del artículo 30 establece que *"la información transmitida en el marco del presente Reglamento será utilizada por el órgano jurisdiccional requerido solo para los fines para los que se transmitió"*. Lo que quiere decir que el órgano jurisdiccional requerido, esto es, el de Estado en el que se va a obtener la prueba, no podrá disponer del resultado de la misma, es decir, de los datos personales o la información personal obtenida para cualquier otra finalidad que no sea su transmisión al órgano jurisdiccional requirente, que lo usará, como se ha señalado anteriormente, exclusivamente en relación con el caso específico para el que se le haya transmitido.

Al tiempo, los órganos jurisdiccionales requeridos, de acuerdo con su derecho nacional, garantizarán la confidencialidad de la mencionada información. De modo que no solo habrán de limitar el tratamiento a la finalidad para la que se obtuvieron los datos, esto es, para su transmisión al órgano jurisdiccional requirente, sino que además deberán de garantizar la confidencialidad de esa información obtenida y transmitida a un tribunal de otro Estado miembro de la UE.

Por último, hay que destacar la consolidada doctrina del Tribunal de Justicia de la Unión Europea que en reiteradas ocasiones ha venido estableciendo límites al acceso por parte de las autoridades competentes a los datos de tráfico de las comunicaciones electrónicas de los ciudadanos. Así, por ejemplo, en la reciente Sentencia del Tribunal de Justicia (Gran Sala) de 20 de septiembre de 2022 (peticiones de decisión prejudicial planteadas por el Bundesverwaltungsgericht – Alemania) – Bundesrepublik Deutschland/SpaceNet AG (C-793/19), Telekom Deutschland GmbH (C-794/19), se ha establecido que *"el artículo 15, apartado 1, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, en relación con los artículos 7, 8, 11 y el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que se opone a medidas legislativas nacionales que establezcan, con carácter preventivo, a efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de los datos de tráfico y de localización"*.

De manera que el TJUE admite a efectos de la lucha contra la delincuencia grave[39] que en las legislaciones nacionales se puedan implementar

39. Nótese que la Sentencia acepta que se puedan adoptar esas medidas en la lucha contra la delincuencia grave, pero también prevé que en relación con la lucha contra la

medidas de: (i) conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse; (ii) conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario; (iii) requerimiento a efectuar a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan estos proveedores de servicios.

En todo caso, estas medidas legislativas que puedan adoptar los distintos Estados deberán garantizar siempre *"mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso"*[40].

2. TRATAMIENTO DE LOS DATOS PERSONALES CON FINES PENALES POR PARTE DE LOS PARTICULARES

Como se ha podido ver en el acápite anterior el régimen establecido en la Directiva (UE) 2016/680 y en la LO 7/2021 respecto del tratamiento de datos personales para fines penales queda reservado en su aplicación a las autoridades competentes. De ahí que la recogida y tratamiento de datos personales para su uso en el proceso penal por parte de los particulares queda claramente fuera de esa regulación y está sometida a la normativa general de protección de datos, en concreto a lo establecido en la Reglamento (UE) General de Protección de datos y en la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La circunstancia de que los particulares no estén sometidos a la normativa específica relativa al tratamiento de datos personales con fines penales supone que, en su actuación para la obtención de pruebas de cargo o de descargo que supongan afectación y manejo de datos personales,

---

delincuencia, no necesariamente grave, se puedan adoptar medidas "*que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia y de la protección de la seguridad pública, una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas*".

40. *Cfr*. STJUE (Gran Sala) de 20 de septiembre de 2022 Bundesrepublik Deutschland / SpaceNet AG (C-793/19), Telekom Deutschland GmbH (C-794/19).

estarán sometidos a las exigencias y condicionamientos del Reglamento General de Protección de datos. En este sentido, a los efectos del presente trabajo, lo que interesa analizar son los principios del tratamiento que se prevén en el artículo 5 del Reglamento (UE) 2016/679, y los efectos que su infracción tiene para el uso de los datos personales como fuente de prueba en los procesos.

En concreto, de acuerdo con la previsión de la norma europea, el tratamiento de datos personales debe respetar el principio de licitud, lealtad y transparencia[41]; el principio de limitación de la finalidad[42]; el principio de minimización de los datos; el principio de exactitud; el principio de limitación del plazo de conservación; y el principio de integridad y confidencialidad. De todos ellos, sin duda, los más relevantes, por su trascendencia en relación con el valor probatorio de los datos en el proceso, son: el principio de licitud y el principio de finalidad en el tratamiento de los datos. Puesto que, si la recopilación y su posterior tratamiento no se hace de forma lícita y para la finalidad para la que se recogieron, los datos personales no podrán ser considerados fuentes de prueba válidas para su uso en el seno de un proceso. Y por eso vamos a analizar a continuación la esencia de su contenido y las exigencias o requisitos que su vigencia impone a la recogida y tratamiento de los datos personales para un posterior uso en un proceso jurisdiccional.

2.1. Licitud del tratamiento de los datos personales por parte de los particulares

La principal exigencia del tratamiento de los datos personales es su licitud (artículo 5.1.a Reglamento UE 679/2016). De modo que el tratamiento de los datos, para respetar las exigencias y previsiones del Reglamento General de Protección de Datos, habrá de cumplir al menos una de las condiciones previstas en el artículo 6 para que pueda ser considerado lícito. De entre las distintas condiciones que se prevén en el artículo sobresale, sin la menor duda, como condición esencial para la licitud el consentimiento del interesado para el tratamiento de sus datos personales para

41. Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado (artículo 5.1 a).

42. Lo que supone que los datos serán "*recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales*" (artículo 5.1.b). Este principio es esencial para la determinación del valor que debe darse a los datos como fuente de prueba para los procesos.

uno o varios fines específicos (artículo 6.1.a). Las restantes condiciones para el tratamiento que se prevén en el precepto tienen en la práctica una menor incidencia[43], ya que la gran mayoría de los tratamientos de datos personales resultan lícitos por contar con el consentimiento del interesado titular de los datos.

En consecuencia, la condición por excelencia que debe cumplirse para el lícito tratamiento de los datos es el consentimiento del interesado. La importancia del consentimiento para el uso de los datos personales por parte de terceros, también en el desarrollo de los procesos, obliga a hacer unas consideraciones específicas sobre el alcance, la necesidad y los efectos que produce el consentimiento, o más correctamente la falta del mismo, en el uso de los datos en el seno de un proceso penal. Por ello, en este apartado se aborda un análisis del papel del consentimiento del titular de los datos en el proceso penal.

El consentimiento del titular de los datos se configura como la pieza clave para su recopilación, uso y tratamiento por terceros. Ahora bien, no debe perderse de vista que el consentimiento de los titulares de los datos no es una manifestación de una voluntad única y simple, sino que es un acto de voluntad complejo, cuyo objeto se extiende a varias actuaciones que pueden hacer los terceros respecto de los datos personales de alguien, que van desde la obtención y recogida de los mismos, hasta su posterior tratamiento.

De manera que es necesario distinguir claramente los diversos consentimientos que debe prestar la persona titular de los datos. Pues, de una parte, ha de consentir la recogida y recopilación de sus datos, y de otra parte, consentir el tratamiento posterior de los mismos para unas finalidades que debe conocer en el momento de aceptar el tratamiento. Esta distinción entre los consentimientos, que presta el titular de los datos, resulta fundamental a la hora de analizar el uso de los datos personales en los procesos, ya que, como veremos con detalle posteriormente, la normativa prevista en la Ley Orgánica del Poder Judicial para el tratamiento jurisdiccional de los datos personales (artículo 236 ter 3) no toma en consideración esos dos momentos del consentimiento, el de la recogida y el del posterior tratamiento, centrando su atención exclusivamente en

43. Algunas de las condiciones previstas en el artículo son: "*b)el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c)el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d)el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e)el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*".

el momento del tratamiento jurisdiccional de los mismos. De forma que se produce una confusión sobre el alcance que tiene la imprescindible exigencia de consentimiento del interesado para la recogida y tratamiento de sus datos, aun en los casos en que los mismos puedan acabar siendo tratados en un proceso.

El consentimiento del interesado para la recogida y tratamiento de sus datos personales presenta un elemento que lo caracteriza, y es el hecho de que la voluntad de consentir ha de estar dirigida teleológicamente a unos fines concretos y determinados. En este sentido, el artículo 6.1.a) del Reglamento (UE) 2016/679 expresamente prevé que una de las condiciones que pueden determinar la licitud del tratamiento es que *"el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos"*. De manera que, el consentimiento del titular de los datos para que puedan ser tratados lícitamente no se manifiesta en una aceptación incondicionada, sino que es una aceptación que se vincula y condiciona a las concretas finalidades que se puedan cumplir con los datos recopilados u obtenidos. Este elemento teleológico es fundamental en relación con el consentimiento que puedan prestar las personas, que deben comprender y aceptar las finalidades para las que se recopilan sus datos.

Hay, pues, una evidente transcendencia del principio de finalidad en el tratamiento de los datos (artículo 6.1.b Reglamento UE 2016/679), que se proyecta sobre la voluntad del interesado al aceptar la recogida y uso de sus datos personales. De manera que, en principio, un tratamiento de datos al margen de las finalidades para las que se consiente no constituirá un tratamiento lícito de los mismos.

El respeto del principio de finalidad en el tratamiento lícito de los datos personales resulta especialmente importante en aquellos casos en los que un particular proceda a tratar los datos personales para una finalidad, como es la prevención, investigación o enjuiciamiento de los delitos, claramente diversa de aquella que consintió el titular de los datos[44]. En este supuesto el uso que realice el particular aportando esos datos al proceso penal como prueba supondrá un tratamiento ilícito de los mismos que debe provocar su exclusión probatoria por haber sido utilizados con vulneración del derecho fundamental a la protección de datos.

44. Por ejemplo, que una compañía de telefonía móvil utilice los datos de alguno de sus clientes, que tiene recopilados con fines de facturación y gestión comercial de sus servicios, para aportarlos como prueba en un proceso penal concreto, supone, no debe perderse de vista, un uso o tratamiento de esos datos para un fin distinto del consentido por el titular de los mismos, y constituye un tratamiento ilícito.

Por otra parte, en el Reglamento (UE) 2016/679 se establece que el consentimiento debe ser libre, específico, informado e inequívoco[45].

En primer lugar, hay que tener presente que la libertad exigida en el momento de aceptar el tratamiento de los datos personales es un requisito axiomático del consentimiento[46]. De manera que es un requisito que necesariamente deberá concurrir en la voluntad expresada para consentir y que se concreta en que *"el consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno"*[47].

En segundo lugar, el consentimiento ha de ser específico, lo que implica que, cuando los datos proporcionados vayan a ser tratados para varias finalidades, el interesado deberá prestar su consentimiento para cada una de ellas. Esta exigencia está directamente conectada, de una parte, con la dimensión teleológica del consentimiento que se reconoce en el artículo 6.1.a del Reglamento (UE) 2016/679, y de otra parte, con el principio de finalidad en el tratamiento de los datos (artículo 6.1.b). De hecho, es un elemento esencial en relación con el uso de datos personales en el proceso, dado que se vincula con los dos consentimientos que concurren, el necesario para la recopilación y tratamiento de los datos por el responsable, y en un segundo momento, el eventual consentimiento para el tratamiento jurisdiccional de los mismos, que como ya se ha indicado no resulta necesario a tenor de lo dispuesto en el artículo 236.3 ter LOPJ a pesar de ser una finalidad que puede no haber estado presente cuando se consintió la recopilación e inicial tratamiento de los datos.

En definitiva, como indica el Reglamento (UE) 2016/679 *"el consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos"* (Cdo. 32). En igual sentido, el artículo 6.2. LO 3/2018 de Protección de Datos Personales y garantía de los derechos

45. En similares términos se contempla la necesidad de consentimiento prevista en artículo 6.1 de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

46. Así lo indica ARJONA GUAJARDO-FAJARDO cuando señala que "*un requisito que, dado su carácter axiomático, no necesita demostración ni justificación. Por ello, su análisis práctico debe realizarse adoptando una perspectiva negativa, esto es indagando cuándo puede entenderse que el consentimiento no ha sido prestado libremente*" (*cfr*. "El consentimiento para el tratamiento de datos personales: requisitos del mismo y capacidad para prestarlo a la luz del nuevo Reglamento europeo (Reglamento UE 2016/679)" en *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Oubiña Barbolla, S. y Catalina Benavente, M. A. (coord.), Colomer Hernández, I. (dir.), Aranzadi Thomson-Reuters, Cizur Menor, 2019, p. 707.

47. Cdo. 42 Reglamento (UE) 2016/679.

digitales prevé que *"cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas"*.

En tercer lugar, el consentimiento ha de ser informado, lo que supone que el interesado reciba una información clara y precisa sobre los datos que se le solicitan y sobre el tratamiento que se vaya a realizar con ellos.

Por último, el consentimiento debe ser inequívoco, lo que supone que no podrá ser presunto ni expresado en forma ambigua o genérica, sino que debe ser expreso, concreto y afirmativo.

2.2. Regulación de la LOPJ sobre el consentimiento para el tratamiento jurisdiccional de los datos

En un escenario como el que se ha ido describiendo en los anteriores apartados, y en el que la garantía del derecho a la protección de datos se materializa en la exigencia de licitud en el tratamiento de los datos personales, básicamente a través del consentimiento de los titulares de los datos que se extiende a la finalidad para la que son recogidos y tratados, nuestro legislador se ha visto impelido a introducir en la Ley Orgánica del Poder Judicial[48], una regulación específica en relación con el uso de los datos personales por parte de la Administración de Justicia con fines no jurisdiccionales y en relación con el uso de los datos por jueces y fiscales con finalidad jurisdiccional.

En particular hay que tener presente la previsión del artículo 236 ter 3 LOPJ cuando expresamente establece que *"no será necesario el consentimiento del interesado para que se proceda al tratamiento de los datos personales en el ejercicio de la actividad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba"*.

Esta norma merece una valoración crítica, dado que no distingue entre recopilación y posterior uso de los datos, limitándose a establecer una genérica habilitación para el tratamiento jurisdiccional de los datos sin que resulte necesario el consentimiento del titular, prescindiendo del origen y obtención de esos datos. El precepto no distingue entre el momento

48. El Capítulo I bis del Título III de la LOPJ, que lleva por rúbrica "*Protección de datos de carácter personal en el ámbito de la Administración de Justicia*" (artículos 236 bis a 236 decies), se introdujo por la Ley Orgánica 7/2015, de 21 de julio y ha sido objeto de modificación por la Ley Orgánica 7/2021, de 26 de mayo.

en que se recogen los datos y el tratamiento inicial de los mismos y el posterior momento en que son tratados en el seno de un proceso.

En este sentido, hay que hacer notar que la norma sólo exonera el consentimiento del interesado para el tratamiento que se realice con fines jurisdiccionales, pero no exime de la necesidad del consentimiento para la recopilación y recogida de los datos, así como para el tratamiento y la finalidad para la que inicialmente fueron recogidos. Por tanto, el no cumplimiento de las exigencias previstas para esa recogida y tratamiento previos al acceso de los datos al proceso (consentimiento, licitud, finalidad, etc.) ha de tener consecuencias en el valor probatorio de los datos en el proceso, sin perjuicio que para su incorporación al proceso y tratamiento por el órgano jurisdiccional no se requiera el consentimiento del interesado. De hecho, no debe perderse de vista, que el propio artículo 236 ter 3 LOPJ deja la puerta abierta a la existencia de estos efectos procesales en cuanto a la validez de los datos personales como prueba, al remitirse expresamente a lo dispuesto en las normas procesales para la validez de la prueba.

De ahí que, pudiera parecer que este artículo prescinde del origen lícito de los datos personales que se puedan usar en un proceso y que solo se preocupa de garantizar que el tratamiento que realice el juzgador, una vez que los datos hayan tenido acceso al proceso, pueda realizarse sin problemas a pesar de que la finalidad de uso jurisdiccional de los datos no haya sido expresamente consentida por el interesado. Y es que, en efecto, asegurar y exigir el carácter lícito de los datos personales desde su origen, sustancialmente que se hayan obtenido y recopilado cumpliendo al menos una de las condiciones previstas en el artículo 6 del Reglamento (UE) 2016/679, no parece ser una preocupación de esta norma. El precepto se limita a habilitar el tratamiento de los datos en el seno de un proceso, aunque esta finalidad no haya sido consentida por el interesado. Y lo único que contiene en relación con la eventual ilicitud de los datos en su origen es la remisión a *"sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba"*, lo que supone que todas las cuestiones relativas a la ilicitud de los datos desde su obtención y recogida deban ventilarse en el seno del momento de admisión de la prueba, conforme a lo dispuesto en las normas procesales. Al respecto, no debe perderse de vista que en la actualidad las normas procesales de los distintos órdenes jurisdiccionales carecen de normas específicas destinadas a regular la validez de los datos personales para su uso en los procesos en aquellos casos en los que los datos puedan tener vicios por no haberse cumplido las exigencias de la normativa de protección de datos en su recogida y posterior tratamiento[49].

49. No debe perderse de vista que el Anteproyecto de LECrim de 2020 recogiendo la necesidad de dar trascendencia procesal, desde el punto de vista la validez probatoria,

Por último, es necesario realizar alguna consideración en relación con la forma de incorporación de los datos personales a los procesos. En concreto, respecto a la distinción que se establece en el artículo 236 ter 3 LOPJ entre que los datos sean facilitados por las partes o recabados a solicitud de los órganos competentes para su incorporación al proceso. Hemos de tener en cuenta que, a pesar de lo que pudiera parecer del tenor del precepto, no resulta indiferente, según la clase de los datos, que sean aportados por las partes del proceso o requeridos por el juzgador.

Así, por ejemplo, la reciente STJUE (Gran Sala) de 5 de abril de 2022, en el asunto C 140/20 (Caso Commissioner of An Garda Síochána y otros) ha indicado que el acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas solamente puede realizarse con el control previo realizado por órgano independiente ("*bien por un órgano jurisdiccional, bien por un órgano administrativo independiente*")[50]. De manera que la aportación directa por las partes de esa clase de datos sin haber sido requeridos por el juez tras un previo control podría vulnerar el derecho a la protección de datos. Por ello, en los casos de aportación de los datos por las partes el juzgador deberá controlar y verificar que el litigante esté habilitado para, de conformidad con las exigencias de la normativa de protección de datos, para poder aportar esa información personal. Este concreto control debe extenderse a comprobar que los datos se han recopilado y tratado lícitamente, de acuerdo a las previsiones del artículo 6 Reglamento (UE) 2016/679.

En conclusión, por tanto, se constata que la habilitación del artículo 236 ter 3 de la LOPJ, para el tratamiento de los datos con fines jurisdiccionales, lo único que hace es exonerar la necesidad del consentimiento del interesado para el uso de los datos para una finalidad diversa de la que fueron obtenidos, pero no convalida, ni subsana los posibles defectos o vicios

---

al respeto y cumplimiento de las exigencias y requisitos derivados de la protección de datos personales, ha previsto en su artículo 520. 2 que "*Únicamente serán válidos aquellos datos relevantes para la investigación cuya obtención, tratamiento e incorporación se realice con sujeción a lo dispuesto en esta ley y en la normativa reguladora del tratamiento de datos personales para fines de prevención, investigación y enjuiciamiento de infracciones penales*". Es decir, no hay la menor duda que la necesidad de respetar las exigencias de la protección de datos en la obtención y tratamiento de las pruebas ha de ser un requisito imprescindible para la validez probatoria de las fuentes de prueba obtenidas, resultando su incumplimiento una causa de exclusión probatoria al amparo de la previsión contenida en el artículo 11.1 LOPJ.

50. Un análisis detallado de esta Sentencia en RODRÍGUEZ LAINZ "La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada de datos de comunicaciones electrónicas en la STJUE del Caso G. D. y Comissioner an Garda Síochána" en *Diario La Ley*, n.º 10058, 28 de abril de 2022, 22 pp.

de licitud que pudieran existir en la recogida e inicial tratamiento de los mismos. Es decir, la excepción que supone este precepto al principio de limitación de la finalidad en relación con el tratamiento jurisdiccional de los datos personales que se usen en un proceso como fuentes de prueba en modo alguno convalidará o subsanará los defectos de licitud que puedan gravar a los datos en su recogida y en su inicial tratamiento.

Por todo ello, la licitud del tratamiento de los datos personales de un interesado resulta una exigencia esencial para el respeto del derecho a la protección de datos de la persona titular de los mismos, de ahí que, si la recogida y uso de los datos no reúne los requisitos legalmente previstos, sustancialmente la necesidad de consentimiento del interesado, el resultado será que el tratamiento de los datos se realizará vulnerando el derecho fundamental a la protección de datos y en ciertos casos, que se concretaran más adelante en este trabajo, determinará la posibilidad de su exclusión como fuente de prueba en los procesos jurisdiccionales.

2.3. El problema de la finalidad del tratamiento de los datos personales por los particulares para su uso con fines penales

El segundo de los principios, previstos en el artículo 5 del Reglamento (UE) 679/2016, que han de presidir el tratamiento de los datos personales es el principio de limitación de la finalidad[51], según el cual: *"los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines"* (artículo 5.1.b). Este principio resulta de especial importancia en relación con el uso de datos personales en los procesos, ya que, en principio, la necesidad de una finalidad específica y concreta en el momento de la recogida y tratamiento de los datos obliga al responsable a comunicársela al interesado en el momento de obtener su consentimiento, como hemos podido ver en el anterior apartado. Por tanto, la vulneración del principio de limitación de la finalidad supone una infracción del derecho a la protección de datos por implicar la realización de algún tratamiento de los datos que no cumpla con este fundamental principio del artículo 5 del Reglamento (UE) 2016/679.

En un análisis del alcance del principio de limitación de finalidad se puede comprobar que, a efectos de la licitud de un tratamiento para un fin distinto de aquel para el que se recogieron los datos, en la regulación se

51. El artículo 4.1.3 del Reglamento (UE) 679/2016 define la limitación del tratamiento como "*el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro*".

prevén dos circunstancias que habilitan la posibilidad de un tratamiento para fines diversos: de un lado, aquellos casos en los que exista un consentimiento del interesado para unas finalidades distintas, y de otro lado, los casos en los que de acuerdo con el Derecho de la Unión o de los Estados miembros el tratamiento para finalidades distintas constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar alguno de los objetivos indicados en el artículo 23, apartado 1 del Reglamento (UE) 2016/679. De entre los objetivos que se recogen en el indicado precepto destacan, por su posible relación con el tratamiento de los datos personales para su uso en los procesos, los dos siguientes: (i) la protección de la independencia judicial y de los procedimientos judiciales; (ii) la protección del interesado o de los derechos y libertades de otros.

De modo que, fuera de estas dos habilitaciones para un tratamiento con finalidades distintas a aquellas para las que se recogieron los datos, el responsable del tratamiento deberá determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales (artículo 6.4).

La compatibilidad entre los fines deberá ser apreciada por el particular responsable del tratamiento atendiendo, entre otros, a los siguientes criterios: (i) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto; (ii) el contexto en que se hayan recogido los datos personales; (iii) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales; (iv) las posibles consecuencias para los interesados del tratamiento ulterior previsto; (v) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Sin embargo, en mi opinión este juicio de compatibilidad previsto en la norma no resultará efectivo en el supuesto que estamos analizando, pues no se debe de olvidar que nos encontramos antes un tratamiento para un fin penal, su uso como prueba en un proceso penal, de datos obtenidos y recopilados por el particular para fines diversos de los penales.

Por ello, dadas las dos posibilidades previstas en la norma para el tratamiento de datos con una finalidad distinta de aquella para la que fueron recopilados y conservados, resulta claro que el uso de los datos como fuente de prueba en un proceso solo podrá producirse siempre que el interesado lo haya consentido o una norma con rango de ley lo haya autorizado para la salvaguarda de alguno de los objetivos del artículo 23 del Reglamento (UE) 2016/679.

En definitiva, a modo de conclusión, debe destacarse que el principio de finalidad en el tratamiento condiciona las posibilidades de uso de

los datos personales, y que consecuentemente, salvo las dos excepciones previstas en el RGDP[52], el tratamiento para una finalidad distinta de que aquellas para las que se recogieron y se autorizó su tratamiento por el titular de los datos, supondrá que el uso no resultará lícito por adecuarse a las exigencias previstas en el artículo 6.4 Reglamento (UE) 2016/679.

3. EXCLUSIÓN PROBATORIA DE DATOS PERSONALES TRATADOS POR LOS PARTICULARES EN EL PROCESO PENAL

La última de las cuestiones que deben abordarse es la relativa al régimen jurídico procesal que se aplica a los datos de personales cuando son usados o se pretende su empleo como fuentes de prueba en el seno de un proceso penal por parte de los particulares sin haber realizado un tratamiento lícito de los mismos.

Como se ha indicado en el epígrafe anterior la actual regulación contenida en el artículo 236 ter 3 LOPJ recoge una general habilitación legal para el tratamiento de datos personales en el seno de los procesos dentro de la actividad jurisdiccional. En concreto, está previsto que no sea necesario el consentimiento del interesado para que sus datos personales puedan ser tratados con finalidad jurisdiccional en el seno de un proceso. Dicho, en otros términos, la norma excepciona la necesidad de consentimiento expreso para un tratamiento con una finalidad distinta de aquella para la que fueron recopilados, esto es, para su tratamiento con una finalidad jurisdiccional.

Esta previsión habilitante del cambio de finalidad en el tratamiento de los datos respecto a la que determinó su recogida y conservación no puede ocultar, ni convalidar, los vicios o defectos en los que se haya podido incurrir en el momento de la recogida de los datos. En efecto, si en la obtención y recogida de los datos, o incluso posteriormente en la cesión de los mismos a un tercero, no se han respetado las exigencias previstas en el artículo 6 del Reglamento (UE) 2016/679 para la licitud del tratamiento, los datos se habrán obtenido y usado con vulneración del derecho a la protección de datos personales del interesado. Y esta vulneración del derecho a la protección de datos en la obtención de la fuente de prueba, en este caso los datos, ha de tener necesariamente reflejo en el proceso,

52. Que expresamente se haya aceptado y consentido por el titular el cambio de finalidad en su tratamiento o que, de acuerdo con el Derecho de la Unión o de los Estados miembros el tratamiento para finalidades distintas constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar alguno de los objetivos indicados en el artículo 23, apartado 1 del Reglamento (UE) 679/2016.

en particular en el examen de la validez de la prueba que debe hacer el juzgador penal[53].

En el examen de la validez de los datos como fuente de prueba en los procesos penales el juez o el tribunal deben apreciar si concurre una causa de exclusión probatoria[54]. En concreto, deben apreciar si procede la exclusión probatoria de los datos obtenidos por particulares con vulneración del derecho fundamental a la protección de datos por aplicación de lo previsto en el artículo 11.1 LOPJ[55]. En este sentido, no hay duda de que los datos obtenidos y tratados sin las exigencias del artículo 6 del Reglamento (UE) 2016/679 no son objeto de un tratamiento lícito, y en consecuencia se vulnera el derecho fundamental a la protección de datos del artículo 18.4 CE. Por ello, los datos que se consigan como consecuencia de un tratamiento ilícito deben ser excluidos del proceso y no pueden constituir una fuente de prueba legítima por haber sido obtenidos con vulneración o violación de un derecho fundamental[56].

Esta consecuencia, la exclusión probatoria de los datos que sean el resultado de un tratamiento ilícito, si bien es clara, precisa y se adecua a la normativa de protección de datos y a la regulación procesal, sin embargo, en la práctica no se suele estimar por parte de los órganos jurisdiccionales penales.

---

53. Ver, sobre esta materia, el trabajo de PÉREZ GIL, J., "Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal" en *Justicia: ¿garantías versus eficiencia?*, Jiménez Conde, F. y Bellido Penadés, R. (dir.), Llopis Nadal, P. y De Luis García, E. (coord.), Tirant lo Blanch, Valencia, 2019, p. 399-441.

54. Hay que ser plenamente consciente que está actividad de valoración probatoria de los datos personales es una tarea compleja, pues no siempre la distinción entre datos personales y datos que no lo son resulta clara cuando se examinan en un concreto proceso. Pues, como señala PÉREZ GIL "*ha de contarse por ello con los llamados 'conjuntos de datos mixtos', en los que se entremezclan datos personales y datos no personales y que representan la mayoría de los conjuntos de datos utilizados en la llamada 'economía de datos'*" (*Cfr. op. cit.*, p. 416).

55. "*En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales*".

56. "*Si los datos se han obtenido ilícitamente, esto es, vulnerando directa o indirectamente derechos o libertades fundamentales, entre los que hay que entender se encuentra el protegido por el Art. 18.4 CE de que aquí tratamos, su cesión al Juez, lo que incluye también la hecha por un particular, en principio, debe obtener la sanción procesal de la nulidad probatoria (Art. 11.1 LOPJ) –no se puede obtener la verdad a cualquier precio, o al precio de vulnerar derechos fundamentales–, e igualmente podrá conllevar la sanción administrativa (LOPDGDD) o penal (Art. 197. 3 y 7 CP) que corresponda, con la única excepción de que la obtención se haya realizado –sin el consentimiento del titular del derecho afectado y sin orden judicial– en circunstancias de urgencia, esto es, en supuestos de imposibilidad para acudir a solicitar una orden judicial, con riesgo de pérdida de la información, mientras, además de su proporcionalidad, se mantenga la finalidad probatoria*" (*cfr*. VELASCO NÚÑEZ, *op. cit*., p. 140).

Las razones que explican que indebidamente no se excluyan los datos objeto de un tratamiento ilícito son esencialmente: de una parte, una interpretación extensiva y errónea del artículo 236 ter 3 LOPJ, según la cual la no necesidad de consentimiento del interesado para el tratamiento de los datos con finalidad jurisdiccional se interpreta como una habilitación para el uso de datos personales en los procesos sin atender a la licitud de su recopilación y del tratamiento inicial anterior a su entrada en el procedimiento jurisdiccional. Y, de otra parte, que no se distingue adecuadamente entre dos de los principios del artículo 5 del Reglamento (UE) 2016/679 que han de respetarse en el tratamiento de datos personales: el principio de licitud y el principio de limitación de la finalidad. Puesto que se olvida que la posible ilicitud del tratamiento por el que se obtienen los datos no queda subsanada, ni convalidada, por la previsión del artículo 236 ter 3 LOPJ, que lo único que hace es excepcionar la necesidad de consentimiento del interesado para el uso de los datos con una finalidad distinta de la que se recogieron.

Por tanto, aunque el precepto de la LOPJ permita el tratamiento jurisdiccional de los datos sin el consentimiento del interesado, ello no supone que el juzgador no tenga que apreciar la validez probatoria de los datos personales atendiendo a la licitud en el momento de su obtención y en los tratamientos anteriores a su aportación al proceso por parte de los particulares. Y en el caso de que los datos hayan sido obtenidos o tratados sin cumplir con las exigencias del artículo 6 del Reglamento (UE) deberá declarar su nulidad para ser usados como prueba[57].

Las concretas posibilidades de vulneración del derecho a la protección de datos personales en la obtención y tratamiento de los datos que posteriormente vayan a ser incorporados a un proceso penal por parte de los particulares son múltiples. A efectos de una posible clasificación de los casos de vulneración de este derecho fundamental hay que atender a un doble criterio: de un lado, a los vicios, esencialmente a la ilicitud, producidos en el momento de la recogida o recopilación de los datos personales; y de otro lado, a los vicios en los que se pueda haber incurrido en un tratamiento de los datos con anterioridad a su ingreso o aportación a un concreto proceso.

57. Como indica VELASCO NÚÑEZ las cesiones de datos hechas por un particular "*sólo tendrán validez probatoria –ya que no vulnerarán el derecho recogido en el Art. 18.4 CE, que es de protección legal, a través del Reglamento General y las Directivas específicas como la 2016/68013– cuando:*
– estén consentidas por el titular del derecho afectado,
– estén autorizadas por el Juez Instructor,
– o vengan justificadas por circunstancias de urgencia y obedezcan a un fin social o a un interés público" (*cfr. op. cit.*, p. 144).

Por ello, en aplicación de ambos criterios podemos identificar algunas de las vulneraciones de este derecho fundamental que más se dan en la práctica:

(i) Los datos son recopilados por los particulares sin el consentimiento del interesado y sin que concurra ninguna otra de las condiciones previstas en el artículo 6 del Reglamento (UE) 2016/679 para que el tratamiento sea lícito.

El caso más usual en el que se produce una vulneración del derecho a la protección de datos tiene lugar cuando los datos son recogidos, obtenidos o recopilados de forma ilícita por no cumplirse ninguna de las condiciones previstas en el RGPD. En estos supuestos la obtención de los datos, y su posterior tratamiento, no estaría habilitada de acuerdo con la normativa de protección de datos personales, y, en consecuencia, el uso y tratamiento de los mismos sería nulo y deberían ser excluidos como prueba en el proceso penal, por haber sido obtenidos con vulneración del derecho fundamental a la protección de datos.

En relación con estos supuestos se plantea el problema de cómo actuar en aquellos casos en los que los datos se recopilan de canales abiertos[58], es decir de fuentes de acceso libre, sin que la voluntad del titular de los datos haya establecido ninguna clase de exigencia para acceder a los mismos. En principio, cuando los datos se obtienen de canales abiertos puede

58. No debe perderse de vista que el anteproyecto de LECrim de 2020 prevé, de forma a mi juicio poco afortunada, en el artículo 514 ALECrim en relación con la búsqueda y obtención de datos a través de fuentes y canales abiertos por parte de las autoridades competentes que "1. *Para averiguar los delitos o descubrir a los responsables de su comisión, la Policía Judicial, por sí o por orden del Ministerio Fiscal, podrá recabar todas aquellas informaciones relevantes para la investigación que se encuentren disponibles en fuentes abiertas de información, así como los datos relativos al investigado que sean accesibles a través de canales abiertos de comunicación*". De manera que parece reconocer una libertad de obtención y uso de los datos personales que existan en canales abiertos sin necesidad de autorización jurisdiccional, salvo cuando esa recopilación de datos personales de fuentes abiertas "*se realice de forma sistemática y continuada con el objeto de crear un registro histórico de la actividad del investigado en el entorno digital, será necesaria autorización previa del Juez de Garantías*" (artículo 514.2 ALECrim). En todo caso, aunque eventualmente se pudiera aceptar esa libertad de búsqueda de datos por parte de las autoridades competentes en los canales abiertos, hipótesis que resulta más que dudosa desde el punto de la garantía de los derechos fundamentales, en concreto desde el de la protección de datos personales, no puede ocultarse que en la práctica se viene realizando (informes OSINT, etc.). Sin embargo, parece más adecuado sostener que los particulares no estarán habilitados para un tratamiento de datos personales de canales abiertos consistente en su aportación como fuente de prueba al proceso penal, siempre y cuando los datos se hayan recopilado sin el consentimiento del titular y sin que concurra ninguna otra de las condiciones del artículo 6 Reglamento (UE) 2016/679 que permita considerar que con esa actuación se produce un tratamiento lícito.

pensarse que la persona que los recopila y posteriormente los utiliza no está vulnerando el derecho a la protección de datos, pero ello es así solo en el caso que los datos hayan sido subidos o puestos por el titular en el canal abierto[59]. Por el contrario, si los datos no han sido subidos por su titular sino por un tercero, sin autorización o consentimiento del titular de los mismo, resulta evidente que cuando son tomados de la fuente de acceso libre se estará ante una recopilación y tratamiento ilícito, que en caso de resultar finalmente aportado a un proceso penal habrá de determinar la exclusión probatoria de dichos datos personales.

No es fácil mantener otra interpretación, pues hacerlo supondría reconocer que por el simple hecho de que un tercero suba a un canal de acceso libre una determinada información, obtenida sin el consentimiento de su titular, se estaría convalidando y subsanando esa obtención y tratamiento ilícito si se permitiese que tomada la información personal de la fuente de acceso libre ya no se considerase que se ha producido una vulneración del derecho a la protección de datos, que debiera llevar aparejada la exclusión probatoria de la información personal ilícitamente obtenida[60].

(ii) Los datos recopilados lícitamente son cedidos a un tercero sin el necesario consentimiento del interesado y el tercero destinatario los aporta al proceso penal.

Otro de los supuestos de vulneración del derecho a la protección de datos que, con cierta frecuencia, ocurre en la realidad es aquel en el que la recogida y tratamiento inicial de los datos en forma lícita, normalmente por haber sido consentida por el titular de los mismos, deviene en una situación de ilicitud en tratamientos posteriores, toda vez que estos no

59. La Agencia Española de Protección de datos expresamente ha señalado en una reciente resolución de septiembre de 2022 que "*no pueden ser objeto de tratamiento los datos personales obtenidos de una red social o de internet, sin que concurra alguna de las bases de legitimación previstas en el art. 6 del RGPD. Por lo tanto, se considera que estamos ante un tratamiento ilícito de datos personales, ya que en este caso la parte reclamada ni siquiera intentó obtener el consentimiento de los reclamantes para el uso de su imagen, dado que consideró que tenía interés legítimo para su tratamiento*" (Resolución sancionadora en Expediente N.º: EXP202104917).

60. A modo de ejemplo, imaginemos que un dato personal de una persona es subido sin su consentimiento a una página web de una empresa a una sección que es de acceso libre, y de ahí es tomada por un tercero que la aporta a un proceso penal como prueba. La aportación al proceso no requerirá consentimiento del titular de los datos por la prescripción del artículo 236 ter 3 LOPJ, pero el simple hecho de que se haya tomado de una fuente de acceso libre no convalida, ni subsana el vicio de ilicitud que grava la obtención de esos datos y el primer tratamiento de los mismos, consistente en su publicación en la web de la empresa sin el debido consentimiento.

son consentidos, ni aceptados por el titular de los datos[61]. En estos casos, el destinario de los datos que no ha sido autorizado por el titular, al tratar los datos incurre en causa ilicitud por no cumplir con las exigencias del artículo 6 del Reglamento (UE) 679/2012, y por ello cuando aporta los datos al proceso penal incurre en causa de exclusión probatoria por tratarse de evidencias obtenidas y tratadas con vulneración del derecho fundamental a la protección de datos del artículo 18.4 CE[62].

(iii) Los datos recopilados lícitamente son cedidos a un tercero con el consentimiento del interesado, pero el tercero destinario los trata para una finalidad diversa de la consentida, antes de su aportación al proceso penal.

En este caso, aunque la aportación al proceso con la finalidad de tratamiento jurisdiccional de los datos queda habilitada por el artículo 236 ter 3 LOPJ, el tratamiento realizado por el tercero destinatario de los datos cedidos no resulta ajustado a la finalidad para la que se consintió y en consecuencia los datos se considerarán ilícitamente obtenidos[63]. Es decir, en este supuesto la recopilación y el inicial tratamiento de los datos por el responsable ha sido lícita por haber sido consentida por el titular, sin

61. Como señala DELGADO MARTÍN "*Si se trata de datos de los que es titular la propia parte que los aporta, no concurre vulneración alguna del derecho reconocido en el art. 18.4 CE. Los problemas surgen cuando se aportan datos personales de otra parte procesal, o de otra persona que no tiene el estatuto de parte en el procedimiento: en estos casos será necesario el consentimiento del interesado; y ante su ausencia, cabe analizar con detenimiento si la cesión del dato (comunicación como forma de tratamiento) se ha producido de forma ilícita (base jurídica que lo legitima)*" (*cfr*. "Protección de datos personales y prueba en el proceso", en *Diario La Ley*, n.º 9383, 22 marzo 2019, p. 10).

62. Por ejemplo, pensemos en el supuesto de un paciente que consiente que una serie de pruebas diagnósticas le sean realizadas en un centro médico y que los resultados de las mismas, que no olvidemos forman parte de las categorías especiales de datos previstos en el artículo 13. 1 LO 7/2021, sean tratados por el personal sanitario a efectos terapéuticos. Y posteriormente esos datos sanitarios son cedidos por el hospital de forma expresa a uno de los médicos que ha tratado al paciente que los utiliza como fuente de prueba de descargo en un proceso penal en el que está siendo investigado por un delito de homicidio imprudente de otro paciente.

63. Un ejemplo puede ser el siguiente: una persona consiente que su historial crediticio (saldo de sus cuentas, deudas que le gravan, etc.) sea cedido por su entidad financiera a una cooperativa de viviendas para que sean usados para decidir si le admiten como cooperativista o no. El presidente de la cooperativa es acusador particular en un proceso contra un tercero ajeno a la cooperativa por un delito societario y procede a aportar los datos bancarios del cooperativista, que fueron aportados exclusivamente para decidir su admisión en la cooperativa. La aportación será posible al amparo del artículo 236 ter 3 LOPJ sin necesidad del consentimiento, pero ese dato podrá ser excluido de su uso como fuente de prueba si cuando se consintió la cesión de esos datos no se autorizó su uso para un proceso un proceso penal, sino exclusivamente para su admisión en el seno de la cooperativa.

embargo, la posterior cesión a un tercero no ha sido consentida, lo que determina que en consecuencia el tratamiento por ese tercero no sea lícito y cuando los aporte al proceso al amparo de la habilitación legal no estará convalidado, ni subsanado, el vicio de nulidad que grava su obtención y tratamiento, debiendo el juzgador acordar su exclusión probatoria en aplicación de la previsión del artículo 11.1 LOPJ.

(iv) Los datos recopilados lícitamente son comunicados por el responsable del tratamiento a un tercero para la prestación de un servicio y el tercero los aporta al proceso penal sin que el titular de los datos los sepa y lo haya consentido.

En estos casos hay que tener presente que nos encontramos en supuestos de comunicación de los datos, que no cesión de los mismos[64], en los que la persona que los ha recibido los trata y los usa sin el debido consentimiento por parte de su titular, dado que recibe los datos de un tercero que fue el que legítimamente los recogió y los trató con el consentimiento del titular de los mismos. De manera que la persona a la que se comunican los datos sin haber sido objeto de autorización por parte del titular, cuando trata esos datos lo está haciendo de forma ilícita, si no cuenta con el consentimiento del titular o si no concurre alguna otra de las condiciones del artículo 6 del RGPD. Y, en consecuencia, a pesar de que pueda aportarlos a un proceso sin el consentimiento del titular gracias a la habilitación legal del artículo 236 ter 3 LOPJ, no hay duda de que, para aceptar esos datos como fuente de prueba, el tribunal deberá comprobar la licitud en la obtención y tratamiento de los datos, al margen de la aportación al procedimiento jurisdiccional, y en su caso acordar la exclusión probatoria de los mismos por vulneración del derecho fundamental a la protección de datos.

64. Sobre esta distinción ARJONA GUAJARDO-FAJARDO señala que "*hay que distinguir entre ceder datos a un tercero, y proporcionar a un tercero acceso a determinada información en orden a posibilitarle que preste un servicio. No todo acto de comunicación de datos a un tercero implica cesión de datos. Hay cesión de datos si el tercero que recibe los datos puede utilizarlos para sus propios fines, decidiendo el objeto y finalidad del tratamiento (v.gr., se vende la base de datos que uno tiene a un tercero, para que se sirva de ella en orden a enviar publicidad de sus propios productos). Hay simple acceso a datos cuando el tercero recibe los datos para realizar determinadas operaciones y prestar con ello un servicio a quien se los ha facilitado, pero no puede decidir sobre su finalidad (v.gr., una empresa pide a un abogado asesoramiento laboral, y para ello le traslada los datos de sus trabajadores; o encarga la gestión de nóminas a un gestor externo, para lo cual le comunica los datos de los trabajadores*)" (*Cfr. op. cit.*, p. 706).

Capítulo 2

Claves y desafíos de la investigación penal mediante GPS en el sur de Europa*

Sabela Oubiña Barbolla

Profesora Contratada Doctora de Derecho Procesal
Universidad Autónoma de Madrid

I. INTRODUCCIÓN: LA GEOLOCALIZACIÓN COMO MEDIO DE INVESTIGACIÓN PENAL

En el curso de la investigación delictiva puede ser extremadamente útil, incluso decisivo, conocer la ubicación espacio temporal pasada y presente del investigado; e incluso, la que ese rastro puede proyectar en un futuro inmediato. Ahora bien, una actividad de esas características representa una injerencia en el derecho fundamental a la intimidad[1]; otra cosa es cuan grave es el alcance o la intensidad de la afectación.

* El presente capítulo se enmarca en la participación de la autora en el Proyecto de investigación: *Límites a la utilización de datos, evidencias e información entre procesos y procedimientos diversos en España y la Unión Europea,* financiado por el Ministerio de Ciencia e Innovación, la Agencia Estatal de Investigación y el Fondo Europeo de Desarrollo Regional (FEDER), con referencia PGC 2018-095735-B-I00.

1. Véase, por todas, las SSTEDH, desde el caso *Uzun* contra *Alemania*, de 2 de septiembre de 2010 hasta el *Ben Faiza contra Francia*, de 8 de febrero de 2012. Desde el caso Uzun contra Alemania, el Tribunal advirtió que la investigación a través de GPS representa una injerencia en la vida privada; no obstante, en el caso concreto, concluyó que no había existido vulneración del derecho fundamental porque el legislador alemán preveía esta posibilidad y la norma en cuestión reunía, a juicio del TEDH, los estándares de calidad de la norma, era necesaria en una Sociedad democrática y proporcionada a los objetivos legítimos perseguidos. El TEDH sustentó su decisión en las siguientes tres claves: i) el (entonces) art. 100c, § 1.1b) de la *Strafprozessordnung* (StPO) permitía el uso de "otros medios técnicos especiales de vigilancia" con el fin de investigar los hechos o localizar al autor cuando la investigación esté relacionada con un delito de extrema gravedad y cuando otros medios tengan menos posibilidades de éxito; y, por tanto que era una norma suficientemente previsible para sus

La geolocalización del investigado puede obtenerse de muy diversas formas, pero con carácter general podrían distinguirse dos grandes métodos. Por un lado, a través de *dispositivos técnicos* basados en algún sistema de posicionamiento global (véase, GPS[2] u otro análogo); un dispositivo que se instalaría en un vehículo a motor, ciclomotor, etc. u otro objeto que pudiese portar el investigado. Y, por otro lado, a través de *medios técnicos* que permitan obtener los datos electrónicos de localización "asociados" al sistema global para las comunicaciones móviles (GSM[3]).

En las siguientes páginas, nos detendremos únicamente en los dispositivos técnicos basados en algún sistema de posicionamiento global, a los que nos referiremos con la abreviatura GPS, por tratarse del sistema más utilizado. En particular esbozaremos con algunas líneas un mapa comparado de la investigación por GPS en el Sur de Europa, repasando brevemente el estado del arte (legal, doctrinal y jurisprudencial) de la geolocalización a través de la instalación de estos dispositivos.

II. ESPAÑA: DE LA ATIPICIDAD A LA EXPRESA REGULACIÓN

Hasta finales de 2015, la LECrim[4] guardaba silencio acerca de la investigación criminal por GPS, igual que ocurría con la mayoría de las

destinatarios y que ofrecía una protección adecuada contra injerencias arbitrarias de las autoridades públicas; ii) la colocación del GPS se enmarcó en una investigación por terrorismo y, por tanto, perseguía fines legítimos y necesarios en una sociedad democrática como son la seguridad nacional y pública, la prevención de infracciones penales y los derechos de las víctimas; iii) la instalación del GPS fue proporcionada por su carácter subsidiario, es decir, se adoptó después de que otros métodos de investigación se revelasen insuficientes. En el caso *Ben Faiza* contra *Francia*, el TEDH concluyo que la norma procesal francesa entonces vigente no cumplía ese estándar de calidad de la norma porque el precepto era muy vago e imprevisible ya que sólo se refería a la posibilidad de recurrir a actos de investigación que se consideraban útiles para la manifestación de la verdad (*vid*. antiguo art. 71 del *Code de Procédure Pénale* francés) y, por tanto, no representaba una garantía suficiente contra los peligros de la arbitrariedad.

2. Siglas que responden a *Global Position System*. Véase, entre otros, GPS, GLONASS, etc.
3. Siglas que responden a *Global System for Mobile Communications*. Debe advertirse que los datos de geolocalización son datos "asociados" a una comunicación, pero no son datos de tráfico porque se pueden generar con independencia del mantenimiento de una comunicación efectiva.
4. RODRÍGUEZ LAINZ, J. L., "GPS y balizas policiales", *Diario La Ley*, N.º 8416, Año XXXV, 7 de noviembre de 2014, disponible a través de la base de datos La Ley, LA LEY *8004/2014; del mismo autor,* "Los Dispositivos electrónicos de posicionamiento GLOBAL (GPS) en el proceso penal", *Diario La Ley*, N.º 7945, 17 de octubre de 2012, disponible a través de la base de datos La Ley, LA LEY *17119/2012.* VELASCO NÚÑEZ, R., "Tecnovigilancia, geolocalización y datos: aspectos procesales penales", *Diario La Ley*, N.º 8338, Año XXXV, 23 de junio de 2014, disponible a través de la

diligencias de investigación con una base tecnológica. Sin embargo, la investigación penal legalmente prevista en la LECrim no podía sustraerse indefinidamente al paso del tiempo.

1. LA OBSOLESCENCIA TECNOLÓGICA DE LA INVESTIGACIÓN EN LA LECRIM ANTES DE 2015

En 1882, la redacción originaria de la LECrim preveía en el Título VIII del Libro II la *entrada y registro en lugar cerrado* (arts. 545-572), el *registro de libros y papeles* (arts. 573-578) y la *detención y apertura de la correspondencia escrita y telegráfica* (arts. 579-588). Por tanto, la única referencia tecnológica que la LECrim recogía inicialmente era al telégrafo; el único aparato que entonces permitía la comunicación inmediata a distancia y que había sido inventado en 1825 por el físico británico William Sturgeon. Este invento llegó a España un tiempo después (1844) y el primer servicio oficial que cubría la línea Madrid-Irún se inauguró en 1855; en 1858, la comunicación entre las ciudades españolas más importantes ya era posible.

Dejando a un lado el telégrafo, en la primera redacción de la LECrim de 1882 no había rastro de otra "tecnología", ni siquiera del teléfono. El teléfono había sido patentado por Graham Bell seis años antes (1876), pero su implantación aún se demoró un tiempo; lo que explicaría que no fuera recogido inicialmente por la LECrim. Ahora bien, si justo es reconocer que esa ausencia era razonablemente comprensible a finales del S. XIX e incluso principios del S. XX, esa misma explicación comenzó a perder sentido a partir de la segunda mitad del S. XX a medida que la utilización del teléfono era más frecuente y se convertía en un medio de comunicación cada vez más habitual.

En ese escenario se aprueba la CE el 6 de diciembre de 1978, cuyo art. 18.3 CE recogía expresamente el derecho fundamental al secreto de las comunicaciones *telefónicas*. Sin embargo, la LECrim seguía sin hacer una referencia concreta al teléfono; es más, ese vacío normativo en la LECrim se prolongó durante una década hasta que la LO 4/1988, de 25 de mayo, reformó el art. 579 de la LECrim[5] a fin de prever expresamente

base de datos La Ley, LA LEY *4014/2014;* del mismo autor, "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", *Diario La Ley*, N.º 8183, Año XXXIV, 4 de noviembre de 2013, disponible a través de la base de datos La Ley, LA LEY *8334/2013.* PEDRAZ PENALVA, E., PÉREZ-GIL, J., "Los datos sobre localización geográfica en la investigación penal", *Protección de datos y proceso penal*, Madrid, La Ley, 2010, disponible a través de la base de datos La Ley, LA LEY *8123/2011.*

5. Sobre la vaguedad de este precepto, *vid*. el FJ 5 de la STC 184/2003, de 23 de octubre, que, entre otras cosas adelantó que, adolecía *de vaguedad e indeterminación en aspectos esenciales, por lo que no satisface los requisitos necesarios exigidos por el art. 18.3 CE para*

la posibilidad de intervenir y/u observar en el ámbito del proceso penal también las comunicaciones telefónicas. Una exigencia, la de la *previsión legal*, que también imponía hacía tiempo el CEDH que habíamos firmado el 24 de noviembre de 1977 y ratificado el 4 de octubre de 1979[6]. Este desfase tecnológico de la LECrim continuó a finales del S. XX y, en especial a principios del S. XXI porque en esas décadas las nuevas formas de delincuencia ligadas al uso de las más novedosas tecnologías ponían constantemente de relieve la insuficiencia de un cuadro normativo concebido para tiempos bien distintos, por no decir casi pretecnológicos.

Hasta finales de 2015, por tanto, la LECrim suspendía[7] la asignatura de adaptación tecnológica. A salvo el telégrafo, desde el S. XIX hasta 2015, los avances tecnológicos aplicados a la investigación penal han llegado siempre muy tarde a la LECrim; y, además cuando lo han hecho como en

---

la protección del derecho al secreto de las comunicaciones, interpretado, como establece el art. 10.2 CE, de acuerdo con el art. 8.1 y 2 CEDH.

6. El art. 8 del CEDH garantiza a toda persona, como *derecho humano, el respeto de su correspondencia* y que, *no podrá haber injerencia de la autoridad pública en el ejercicio de ese derecho, sino en tanto en cuanto esté prevista por ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.* Véase, también los arts. 12 de la DUDH; 17 del PIDCP; 7 de la Carta de Derechos Fundamentales de la UE. DÍAZ REVORIO, F. J., "El derecho fundamental al secreto de las comunicaciones", *Derecho PUCP. Revista de la Facultad de Derecho*, núm. 59, 2006, pp. 159-175. MONTAÑÉS PARDO, M. A., *La intervención de las comunicaciones*, Pamplona, Aranzadi, 2000. JIMÉNEZ CAMPO, J., "La garantía constitucional del secreto de las comunicaciones", *REDC*, núm. 20, 1987; DE LLERA SUÁREZ-BÁRCENA, E., "El régimen jurídico de las observaciones telefónicas en el proceso penal", en *Poder Judicial*, núm. 3, 1986.

7. *Vid.* también sobre lo obsoleto y desfasado de nuestra legislación. MARCHENA GÓMEZ, M., *et al.* GONZÁLEZ-CUELLAR SERRANO, N., "Capítulo 4. La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el art. 18 de la CE, Proceso Penal y Nuevas tecnologías", en *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid, Castillo de Luna, Ediciones Jurídicas, 2015, en particular en las pp. 174-180. ORTIZ PRADILLO, J. C., "El 'remote forensic sofware' como herramienta de investigación contra el terrorismo", en *E-newsletter en la Lucha contra el Cybercrimen*, núm. 4, octubre 2009, p. 6. Sobre esta crítica a la ley procesal antes de la reforma, QUERALT JIMÉNEZ, J. J., "(Tele) Comunicaciones e intimidad: aproximación a su intervención judicial en la instrucción penal", en *El derecho a la privacidad en un nuevo entorno tecnológico*, Colección Cuadernos y debates, Madrid, CEPC/Tribunal Constitucional, pp. 157-158, 160 también nota al pie núm. 3. Otros autores como p. ej., GONZÁLEZ-MONTES SÁNCHEZ, J. L., justifican que las nuevas tecnologías en la investigación no estuvieran previstas en la LECrim en que ésta fuera una Ley del S. XIX, *vid*. "Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas", en *Revista Electrónica de Ciencia Penal y Criminología*, 17-06 (2015), pp. 1, 20, etc.

el caso del teléfono, su regulación no cumplía con las garantías que exige toda injerencia en un derecho fundamental.

Teniendo en cuenta lo anterior el peso de la garantía de los derechos fundamentales en este marco recayó en la interpretación de los órganos judiciales. Por eso, en esa tardanza fue muy meritorio el esfuerzo de todos los Jueces y Tribunales, pero muy especialmente de la Sala 2ª del Tribunal Supremo[8] y del Tribunal Constitucional[9] a la hora definir los límites del Estado en la investigación tecnológica del delito. Con todo, no podemos omitir que desgraciadamente el TEDH[10] tuvo que recordarnos demasiadas veces muchas cosas en esta materia. Véase, por ejemplo: que no puede abandonarse a la creación jurisprudencial lo que ha de ser objeto de regulación legislativa expresa y suficientemente respetuosa con el libre ejercicio de derechos fundamentales; y, que, las deficiencias y lagunas tecnológicas no pueden solucionarse acudiendo a una integración analógica[11] de una norma legal que ya en sí misma es insuficiente porque hacerlo desborda los límites de lo constitucionalmente aceptable.

En esa necesidad inaplazable de que el legislador[12] abordase de una vez por todas una regulación de las intromisiones tecnológicas en la privacidad

8. Véase, entre otras, p. ej. ATS, Sala 2.ª, 18 de junio de 1992; las SSTS, Sala 2.ª, de 14 de junio de 1993; 25 de junio de 1993; 25 de junio de 1993; 18 de abril de 1994; 9 de mayo de 1994; 20 de mayo de 1994; 25 de marzo de 1994; 787/1994, de 18 de abril; 9 de mayo de 1994; 20 de mayo de 1994; de 12 de septiembre de 1994; de 23 de diciembre de 1994; de 12 de enero de 1995; de 3 de junio de 1995; 7 de julio de 1995; 18 de abril de 1997; 7 de noviembre de 1997; 19 de enero de 1998; 20 de enero de 1998; 22 de enero de 1998. A pesar de ese cuerpo de doctrina, la necesidad de una modificación ha ido aumentando y así se ha recogido implícitamente en diversas sentencias. *Vid*. SSTS 165/2013, de 26 de marzo; 712/2012, de 26 de septiembre; 668/2012, de 23 de julio; 639/2012, de 18 de julio; 628/2012, de 11 de julio; 393/2012, de 29 de mayo.
9. SSTC 85/1994, de 14 de marzo; 86/1995, de 6 de junio; 54/1996, de 26 de marzo; 25/2011, de 14 de marzo.
10. *Vid*. caso SSTEDH asunto *Valenzuela Contreras contra España*, de 30 de julio de 1988; *Prado Bugallo contra España*, de 18 de febrero de 2003; *Abdulkadir Coban contra España*, de 25 de septiembre de 2006. En esta última sentencia, el TEDH reconocía que existía una jurisprudencia consolidada y bien establecida, pero incluso a pesar de la reforma de 1988 seguía urgiendo al legislador a una modificación legal que recogiese los principios generales que a este respecto había subrayado el TEDH.
11. En general sobre la idoneidad de la jurisprudencia para legislar, así como la aplicación analógica de intervención de las comunicaciones a otras diligencias de investigación tecnológica, etc., *vid*. MORENO CATENA, V., "Los elementos probatorios obtenidos con la afectación de derechos fundamentales durante la investigación penal", en *Prueba y proceso penal. Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado* (Gómez Colomer, J. L., coord.). Valencia, Tirant lo Blanch, 2008, pp. 75-106; en especial, pp. 90-92.
12. En un epígrafe posterior haremos una breve referencia a los dos anteproyectos que desde 1882 hasta la fecha se han publicado con un texto completo y articulado de

del investigado[13] en el proceso penal insistió[14] el Tribunal Constitucional, poco antes de la reforma de la LECrim en 2015, en la STC 145/2014 de 22 de septiembre a propósito de la posibilidad de intervenir secretamente las comunicaciones orales directas[15].

---

nueva LECrim; el primero en 2011, el Anteproyecto de Ley de Enjuiciamiento Criminal que integra, junto, en el Anteproyecto de Ley Orgánica de desarrollo de los derechos fundamentales vinculados al proceso penal, los Anteproyectos de Ley para un nuevo proceso penal al que nos referiremos como Anteproyecto de LECrim de 2011; y, el segundo, en 2013 el Borrador de Código Procesal Penal, al que nos referiremos como Borrador de CPP. Ahora bien, también han visto la luz en este tiempo otras propuestas desde la Academia y el foro con propuestas de texto; véase, sin ir más lejos, la del Magistrado RODRÍGUEZ LAÍNZ, J. L., "Addenda: propuesta de borrador de modificación del art. 579 de la Ley de Enjuiciamiento Criminal", en *Estudios sobre el secreto de las comunicaciones. Perspectiva doctrinal y jurisprudencial*, Madrid, La Ley, 2011, pp. 772 y ss.

13. *Vid*. GONZÁLEZ-CUELLAR SERRANO, N., "Garantías Constitucionales en la persecución penal en el entorno digital", en *Derecho y Justicia Penal en el S. XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García*, Madrid, Colex, 2006, pp. 887-916. Más recientemente, el mismo autor en "Garantías constitucionales de la persecución penal en el entorno virtual", en *Prueba y proceso penal. Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado* (Gómez Colomer, J. L., coord.). Valencia, Tirant lo Blanch, 2008, pp. 149-182. Esencial en la intromisión en el espacio virtual del titular de un dispositivo son las SSTS, Sala 2.ª, núm. 786/2015, de 4 de diciembre; 342/2013, de 17 de abril. Aunque no directamente en el ámbito del proceso penal, sino desde una perspectiva más general, son muy interesantes las reflexiones sobre la privacidad de DÍEZ-PICAZO GIMÉNEZ, I., *et al.* CÓRDOBA CASTROVERDE, D., "Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico", en *El derecho a la privacidad en un nuevo entorno tecnológico*, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional, Colección Cuadernos y debates, Madrid, CEPC/Tribunal Constitucional, 2016, pp. 99-122; véase entre otros los problemas que plantea la amplitud de su contenido respecto del derecho a la intimidad y, por ende, el correlativo cambio de los parámetros de su ponderación; también, etc. el trasvase con carácter general de una tutela civil a una contencioso-administrativa; margen de interpretación versus principio de supremacía y de equivalencia; etc.
14. *Vid*. ya antes en las SSTC 9/2011, de 28 de febrero; 123/2002, de 20 de mayo.
15. En este caso se trata de las comunicaciones entre detenidos mientras se encontraban en dependencias policiales. *Vid*. sobre el particular la ponencia de URIARTE VALIENTE L. M., "Nuevas técnicas de investigación restrictivas de Derechos Fundamentales", disponible en formato online www.fiscal.es. *Vid*. también el comentario a la sentencia en MARTÍN LORENZO, M., "Crónica de jurisprudencia constitucional en materia de derechos fundamentales sustantivos", Documento Asociación de Letrados del Tribunal Constitucional, pp. 21-22 sobre el caso de las grabaciones de conversaciones de detenidos en calabozos. STC 145/2014: vulneración del derecho al secreto de las comunicaciones. Disponible en formato online a través de la página de la *Asociación de Letrados del Tribunal Constitucional*, https://www.altc.es/Jornadas/BibliotecaDocsJornadas/Cr%C3%B3nica-Mar%C3%ADa_Mart%C3%ADn-29octubre.pdf. Sobre el peso de esta sentencia en la LO 13/2015, *vid*., también, JIMÉNEZ SEGADO, C., *et al.* PUCHOL AIGUALABELLA, M., "Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el

De algún modo el Tribunal Constitucional subrayó la diferencia que existe entre: i) las diligencias de investigación tecnológica que, aun no estando previstas específicamente en la norma, tenían potencial cobertura en el antiguo art. 579.2 de la LECrim pese al defecto de la insuficiencia o calidad de la ley; y ii) las diligencias de investigación tecnológica que no tienen cobertura legal alguna, es decir, cuya ausencia en la ley es total y completa.

Respecto de las primeras, el Tribunal Constitucional[16] reiteró en diversas ocasiones que nuestro ordenamiento jurídico no vulneraba con tales defectos automáticamente las exigencias del art. 8 del CEDH, sino que en ese escenario correspondía al Tribunal Constitucional y al Tribunal Supremo suplir las insuficiencias del precepto en cuestión hasta que de una vez por todas se produzca la necesaria intervención judicial. Sin embargo, esa tesis no puede trasladarse a las segundas diligencias de investigación tecnológica, es decir, a diligencias de investigación que carecen absolutamente de previsión legal[17].

En definitiva, una cosa es que haya una regulación insuficiente y otra muy distinta que no exista previsión legal; sólo donde hay algo, la jurisprudencia puede suplir (y no siempre) el defecto de la insuficiencia o calidad de una norma, pero nunca cuando ni siquiera se ha previsto esa realidad.

---

secreto de las comunicaciones y la protección de datos", *Diario La Ley*, núm. 8676, Sección Doctrina, 7 de enero de 2016, Ref. D-8, disponible a través de la Base de Datos, LA LEY 7944/2015.

16. *Vid*., entre otras, SSTC 169/2001, de 16 de julio, FJ 6; 70/2002, de 3 de abril, FJ 10. Si bien es cierto que esa tesis ha sido objeto de crítica en la doctrina que reclamaba una urgente reforma del art. 579 de la LECrim en materia de intervención de comunicaciones telefónicas.

17. Véanse las reflexiones en esta línea de MARCHENA GÓMEZ, M., *et al.* GONZÁLEZ-CUELLAR SERRANO, N., "Capítulo 4. La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el art. 18 de la CE, Proceso Penal y Nuevas tecnologías", en *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid, Castillo de Luna, Ediciones Jurídicas, 2015, a tenor de la doctrina del Tribunal Constitucional en las pp. 180-189, y en particular a raíz de esta última sentencia en las pp. 194-198. La previsión legal juega de algún modo como implícitamente recoge GONZÁLEZ CUELLAR, un presupuesto de la proporcionalidad, *vid*. "Garantías constitucionales de la persecución penal en el entorno virtual", en *Prueba y proceso penal. Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado* (Gómez Colomer, J. L., coord.). Valencia, Tirant lo Blanch, 2008, p. 176. *Vid*. implícitamente, GONZÁLEZ-MONTES SÁNCHEZ cuando subraya que la jurisprudencia no debe ser quien *establezca las bases de cómo ha de ser una regulación inexistente*. "Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas", en *Revista Electrónica de Ciencia Penal y Criminología*, 17-06 (2015), pp. 21-22.

1.1. En particular, la geolocalización mediante GPS antes de la reforma de la LO 13/2015

Dejando a un lado el desfase tecnológico de nuestra ley procesal penal hasta la LO 13/2015, la utilización de dispositivos de geolocalización no era infrecuente en el curso de la investigación criminal en España antes de su regulación expresa en 2015. Los dispositivos GPS se utilizaban y sus resultados desplegaban efectos probatorios. Sin embargo, esta laguna legal dejaba en manos de la jurisprudencia el *corpus* que definiese los límites de esta diligencia de investigación. El problema es que la Sala 2ª del TS no mantenía un criterio unívoco sobre si la utilización de un GPS debía sujetarse o no a la previa autorización judicial en atención a la graduación de la invasión, para algunos leve y para otros no tan leve, en el derecho fundamental a la intimidad. Con todo, la Sala 2ª del TS parecía inclinarse por entender que no era grave y, por tanto, no era necesario ese previo[18] control judicial.

Este debate no era exclusivamente nacional, sino que también ha sido (y continúa siéndolo) un tema controvertido en otros países[19]. El hecho de que el TEDH[20] avalase los ordenamientos jurídicos que no condicionan la validez de la injerencia que representa un GPS a la previa autorización judicial tampoco ha contribuido a pacificar la discusión doctrinal entre quienes por un lado defienden que esta diligencia de investigación debe exigir con carácter general, salvo casos de urgencia, un control "previo" de la autoridad judicial y quienes, a sensu contrario, mantienen que no es necesario porque la afectación que representa en la esfera de los derechos fundamentales es de menor intensidad.

2. EL SEGUIMIENTO Y LA LOCALIZACIÓN A TRAVÉS DE GPS TRAS LA REFORMA DE LA LECRIM EN 2015

La LO 13/2015, de 5 de octubre[21] introdujo por primera vez en la LECrim, entre otras, diligencias de investigación tecnológica, la *utilización*

18. *Vid*. entre otras, SSTS, Sala 2.ª, 798/2013, de 5 de noviembre; 523/2008, de 11 de julio; 906/2008, de 19 de diciembre; 562/2007, de 22 de junio; 55/2007, de 23 de enero, etc.
19. Como veremos en otro epígrafe, incluso después de las reformas legales expresas que se han producido en otros ordenamientos jurídicos. KROOPS, B. J., NEWEL, B. C., ŠKORVÁNEK, I., "Location Tracking by Police: The Regulation of 'Tireless and Absolute Surveillance' ", *U.C. Irvine L. Rev. 635*, vol. 9, issue 3, paper 5, 2019, disponible en: https://scholarship.law.uci.edu/ucilr/vol9/iss3/5.
20. STEDH, 2 de septiembre de 2010, Caso *Uzun* contra *Alemania*.
21. De modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, *vid*. en adelante LO 13/2015.

de dispositivos técnicos de seguimiento y de localización (arts. 588 quinquies b y 588 quinquies c de la LECrim).

El legislador español resolvió[22] el debate doctrinal y jurisprudencial, que existía hasta entonces sobre la necesidad o no de autorización judicial, subordinando como regla general la "legitimidad" de la invasión en la intimidad que representa la utilización de un dispositivo GPS a la "previa" autorización judicial.

No obstante, la norma prevé que el carácter "previo" del control judicial puede ceder en un escenario de *urgencia que haga temer que de no colocarse el dispositivo GPS se frustraría la investigación.* Ahora bien, esta excepción no es a la autorización judicial, sino a la necesidad de recabar tal control judicial *previamente* porque la legitimidad de la instalación sin esa previa autorización pasa por un control judicial posterior casi inmediato, en tanto que el Juez debe convalidar o revocar esta diligencia de investigación en el plazo máximo de 24hs. Nótese que a diferencia de otras diligencias de investigación limitativas del art. 18 de la CE sujetas también por regla general a "previa" autorización judicial y para las que también se prevén excepciones al control judicial previo, en el caso del dispositivo GPS el posterior control judicial debe producirse en un plazo más perentorio, 24hs frente a las 72hs que existe en otras diligencias de investigación más graves; véase, p.ej. en el caso de la detención correspondencia escrita, telegráfica y postal, la interceptación de las comunicaciones telefónicas y telemáticas, o el registro de dispositivo de almacenamiento masivo de información[23]. Dicho de otra forma, el control judicial de la instalación de un dispositivo GPS sin autorizarlo previamente un juez es más exigente en términos temporales y, por tanto, constitucionalmente más respetuosa con la intimidad potencialmente afectada que en el caso de esas otras diligencias de investigación a priori más invasivas.

Esta pequeña singularidad de la regulación de la utilización de un GPS en una investigación pasa en ocasiones inadvertida; y, a nuestro juicio

22. CASTILLEJO MANZANAREZ, R., "Alguna de las cuestiones que plantean las diligencias de investigación tecnológica", *Revista Aranzadi de Derecho y Proceso Penal*, N.º 45, 2017, disponible base de datos Aranzadi (BIB 2017, 789). REYEZ LÓPEZ, J. I., *et. al*. CABELLO PERRY, J. A., "Los dispositivos técnicos de geolocalización. Régimen jurídico a partir de la LO 13/2015", *Revista Aranzadi Doctrinal*, N.º 4, 2016, disponible base de datos Aranzadi, BIB 2016, 1098. BUENO MATA, F., "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica", *Diario La Ley*, N.º 8627, 19 de octubre de 2015, disponible a través de la base de datos La Ley, LA LEY *5958/2015.* DÍAZ DÍAZ, E., "La abogacía ante la geoinformación. Aplicación de la ley 13/2015", *Revista Aranzadi Doctrinal*, N.º 1, 2016, disponible base de datos Aranzadi (BIB 2015, 18213).

23. Es decir, el triple.

representa una garantía cuya explicación ha de buscarse en la diferente configuración de tres puntos: el *ámbito objetivo*, *el supuesto excepcional al carácter previo de la autorización judicial* y la *autoridad* que puede acordar la diligencia de investigación sin ese previo control judicial[24].

Por un lado, la LECrim no define y, por tanto, no limita el *ámbito delictual* en que cabría plantearse la instalación de este tipo de dispositivos con parámetros cuantitativos en cuanto a la gravedad de la pena, y/o cualitativos en cuanto al tipo penal o al medio de comisión, como sí en cambio ocurre con otras diligencias de investigación del mismo capítulo. Véase, p.ej. otras diligencias de investigación del mismo título acotadas objetivamente en términos generales a delitos dolosos castigados con una pena de prisión igual o superior a tres años; delitos de pertenencia a un grupo u organización criminal, terrorismo; delitos cometidos a través de medios informáticos, de telecomunicación o comunicación.

Por otro lado, la mayor amplitud del enunciado que excepcionalmente permitiría utilizar un GPS sin autorizarlo previamente el juez frente a la más concreta delimitación de tales casos en otras diligencias de investigación del mismo título. Así puede instalarse un dispositivo GPS *en caso de urgencia que haga temer que de no colocarse se frustraría la investigación,* mientras que la excepción en la detención de la correspondencia telegráfica o postal y en la interceptación de las comunicaciones telefónicas o telemáticas sería en *caso de urgencia para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas siempre que existan razones fundadas que hagan imprescindible la medida*. Por tanto, en el caso de las diligencias de investigación limitativas de algún tipo de comunicación el legislador configura la excepción acotando aún más el ámbito objetivo en que, con carácter general cabe imaginar tales medios de investigación, restringiéndolo así a los delitos relacionados con bandas armadas o elementos terroristas; además de que concurran también la nota de apremio (*urgencia*) y las razones fundadas que hagan imprescindible la medida. Visto desde este ángulo, la formulación del supuesto excepcional que permite instalar un GPS sin un control judicial previo, guarda mayor semejanza con la excepción en el registro de dispositivos de almacenamiento masivo de información previsto en *casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida*. No obstante, los enunciados de tales excepciones tampoco son equivalentes[25] porque

24. *Vid*. detención correspondencia escrita, telegráfica y postal; interceptación de las comunicaciones telefónicas y telemáticas; registro de dispositivos de almacenamiento masivo de información.

25. La formulación de la excepción del registro de dispositivos de almacenamiento masivo de información gemela a la del GPS no incluiría esa cláusula. Por tanto, si la

no es lo mismo "el caso de urgencia que haga imprescindible la medida" que "el caso de urgencia en que se aprecie *un interés constitucional legítimo* que haga imprescindible la medida". En el caso excepcional del registro de dispositivos de almacenamiento masivo de información hay una cláusula adicional: un *interés constitucional legítimo* (…); una diferencia que, de algún modo, parece exigir un canon reforzado en uno de los principios rectores de estas diligencias: el principio de necesidad [art. 588 bis a, apartado 4, letra b) de la LECrim].

Por último, la autoridad no jurisdiccional en quien el legislador delega la decisión excepcional sobre la instalación de un GPS corresponde a la policía, mientras que en las diligencias de investigación que afecten a algún tipo de comunicación (postal, telegráfica, telefónica o telemática) corresponde a una autoridad también policial, pero de mayor rango o jerarquía: el Ministro Interior o, en su caso, el Secretario Estado Seguridad.

Las tres circunstancias apuntadas (ámbito objetivo, el supuesto excepcional a la previa autorización judicial y la autoridad no jurisdiccional a quien corresponde acordar excepcionalmente la diligencia) justifican a nuestro juicio la celeridad que se exige al juez en el control posterior para revocar o ratificar la instalación del GPS; un plazo de 24hs frente al de 72hs que tiene el juez, en ese mismo control posterior cuando la investigación excepcional sin autorización judicial previa es la detención de la correspondencia telegráfica y postal, interceptación de las comunicaciones telefónicas o telemáticas o, incluso, el registro de dispositivos de almacenamiento masivo de información cuyo marco regulador parecería más parejo al GPS que ahora nos ocupa. Recordemos que la investigación mediante GPS o a través del registro de dispositivos de almacenamiento masivo de información no se circunscribe a un ámbito objetivo predefinido, la autorización de las dos diligencias de investigación corresponde en general a la autoridad judicial, que en ambas excepcionalmente la decisión puede adoptarse por la policía y que el supuesto extraordinario tiene una fórmula, aunque no idéntica, sí muy similar en tanto que relativamente amplia y no acotada objetivamente.

Frente a la anterior justificación de la diferencia entre el plazo de 24hs que tiene el Juez para controlar la legitimidad de la instalación de un GPS que no haya previamente autorizado él y el de 72hs, que tiene en otras[26]

---

relativa a la colocación de un GPS surge *en caso de urgencia que haga temer que de no colocarse se frustraría la investigación,* en el registro de dispositivos de almacenamiento masivo de información sería el caso de urgencia que haga imprescindible la medida.

26. *Vid*. La intervención de cualquier tipo de comunicación (postal, telegráfica, telefónica o telemática) o en el registro de un dispositivo de almacenamiento masivo de información.

diligencias de investigación limitativas de derechos fundamentales del art. 18 de la CE, podría sostenerse también otra tesis. Y es que la disparidad del plazo que el legislador prevé para el control judicial "posterior" está directamente relacionada con la mayor o menor dificultad que en el fondo conlleva pronunciarse sobre la legitimidad de acuerdo los principios rectores de una y otras diligencias de investigación. Sin embargo, si esa fuese la explicación, en nuestra opinión también entonces el plazo previsto para que el juez se pronuncie, en el caso del control previo, sobre la solicitud de una y otras diligencias de investigación también sería diferente. Sin embargo, la LECrim establece el mismo plazo para que el juez resuelva con carácter general la solicitud del Ministerio Fiscal o la Policía judicial de cualquiera de estas diligencias de investigación [arts. 588 bis b y c de la LECrim]: 24hs desde que se presenta la solicitud.

Dejando a un lado el tema de la explicación a la diferencia del plazo del control judicial posterior de la instalación de un GPS sin la preceptiva preliminar autorización judicial y la de esas otras diligencias de investigación, creemos que el plazo de 72hs previsto para estas últimas[27], es excesivo desde el punto de vista de la afectación de los derechos fundamentales que potencialmente se proyecta en la detención o la intervención de las comunicaciones, por mucho que se limite a la averiguación urgente *de delitos relacionados con la actuación de bandas armadas o elementos terroristas;* y desde luego no tenemos dudas de la desproporción de ese mismo plazo de 72hs cuando se trata del control judicial de la decisión cualquier policía de proceder en la investigación de cualquier delito al registro de un dispositivo de almacenamiento masivo de información sin autorizarlo previamente un juez.

2.1. Otras configuraciones legales alternativas: pasadas y futuras

El marco normativo que acabamos de repasar y que actualmente regula la instalación y la utilización de un GPS en la investigación penal no ha sido el único que ha contemplado el prelegislador, sino que antes de la LO 13/2015 se barajaron otros dos modelos en el ALECrim de 2011 y en el BCPP de 2013; inmediatamente a continuación, veremos algunas similitudes y diferencias con el actual, así como el que parece proyectarse en el futuro proceso penal (*vid*. ALECrim 2020).

El ALECrim de 2011 preveía la utilización de medios técnicos de seguimiento y localización como una forma de vigilancia sistemática (arts. 314-319), pero a diferencia de regulación vigente, no exigía autorización

27. La intervención de comunicaciones postales, telegráficas, telefónicas o telemáticas, así como el registro de un dispositivo de almacenamiento masivo de información.

judicial, sino que bastaba la autorización del Ministerio Fiscal. En el diseño del prelegislador de 2011, la previa autorización del Tribunal de Garantías sólo sería necesaria en el caso de que los dispositivos de localización se utilizasen simultáneamente con la grabación de sonido. La duración máxima se fijaba en 3 meses desde la fecha de la autorización.

El BCPP de 2013 sujetaba[28], como la regulación vigente, la utilización de dispositivos técnicos de seguimiento y localización a la previa autorización del Tribunal de Garantías (*vid*. arts. 331-333); el carácter previo de la autorización judicial podría ceder excepcionalmente en casos de urgencia acreditada que hiciese temer que la demora en la obtención de la autorización pudiese frustrar los fines de la investigación; pero la diligencia seguiría sujeta a la autorización del Fiscal General del Estado, quien lo comunicará por escrito motivado al Juez de Garantías en el plazo máximo de 24hs para que éste revoque o confirme motivadamente en el plazo máximo de otras 24hs el seguimiento y localización excepcionalmente preautorizados por el Fiscal General del Estado. En lo que a la duración se refiere, el BCPP de 2013, era más garantista pues preveía una duración máxima inicial de 1 mes y, su excepcional prórroga hasta un máximo de 3 meses, si así estuviera justificado a la vista de los resultados obtenidos con la medida[29]. Además, el prelegislador preveía un control judicial periódico del resultado de esta diligenciad de investigación más férreo que el vigente de tal modo que el Ministerio fiscal debía dar cuenta al Tribunal de Garantías en el plazo que éste hubiese previsto en la autorización y, en todo caso, "cada 15 días".

¿Y cuál es el régimen que se dibuja para la instalación de un GPS en el futuro proceso penal? El ALECrim de 2020[30] sigue inclinándose, como ya

28. Explicaba la Exposición de Motivos del citado texto su regulación en el Capítulo VIII junto a la investigación mediante vigilancias policiales sistemáticas, pero a diferencia de aquellas, el seguimiento y localización mediante dispositivos técnicos con un régimen de autorización acorde con su naturaleza porque "la incidencia que en la intimidad de cualquier persona puede tener el conocimiento por los poderes públicos de su ubicación espacial, hace que la autorización para su práctica se atribuya al Tribunal de Garantías, sin más excepción que aquellos supuestos de acreditada urgencia en que la demora en la obtención de la autorización pudiera frustrar los fines de la investigación, en cuyo caso el Fiscal puede conceder una autorización provisional, con dación inmediata de cuenta al Tribunal de Garantías y condicionada su vigencia a la ratificación por el órgano jurisdiccional".

29. Por tanto, la duración máxima que preveía era la que en la actualidad prevé la LECrim para el registro remoto de dispositivos de almacenamiento masivo que es una de las dos diligencias de investigación limitativas de derechos fundamentales del art. 18 de la CE que, según el legislador de 2015, es más grave e invasiva y, por tanto, nunca puede adoptarse sin ese previo control judicial, por muy excepcional que sea el caso.

30. GARCÍA MARCOS, J., *et. al*. ZARAGOZA TEJADA, J. I., "Las medidas de investigación tecnológica en el anteproyecto de ley de enjuiciamiento criminal de 2020. Una

hiciera el ALECrim de 2013 y la regulación vigente después de la reforma de 2015, por la necesidad de la previa autorización del Juez de Garantías para la utilización de medios técnicos de seguimiento y localización (art. 396), así como recabar datos de geolocalización de los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como a toda persona que contribuya a facilitar las comunicaciones telefónicas o telemáticas, lógica o virtual. La investigación mediante el seguimiento y localización tendrá una duración máxima inicial de 3 meses a partir de la autorización judicial; excepcionalmente, el Juez de Garantías, podría acordar a instancia del Ministerio Fiscal, prórrogas sucesivas por igual o inferior plazo hasta un máximo de 18 meses, teniendo en cuenta los resultados obtenidos hasta entonces y los que previsiblemente se pudieran obtener manteniéndola.

Dejaremos a un lado la regulación que pudo ser e incluso aquella que quizá se plasme en el (ojalá) nuevo proceso penal para la utilización de un GPS como medio de investigación criminal y veamos qué ocurre a nuestro alrededor.

III. UNA MIRADA COMPARADA AL GPS COMO MEDIO DE INVESTIGACIÓN PENAL

En este epígrafe nos aproximaremos brevemente al régimen a que se debe la investigación penal basada en GPS en nuestro entorno geográfico más cercano. Una mirada comparada en la que haremos un *triage* a este medio de investigación esencialmente a través de los siguientes parámetros: si existe una regulación expresa; la necesidad o no de "previa" autorización judicial; el ámbito objetivo o delictivo en que está prevista; y, la duración.

Este viaje de oeste a este comenzará en Portugal ya que precisamente el interés en esta diligencia de investigación tuvo su origen en un fructífero y entrañable encuentro hispano-luso[31], continuará en Francia y finalizará en Italia.

1. PORTUGAL

El legislador portugués no regula expresamente la posibilidad de utilizar la geolocalización como medio de investigación. De hecho, *el Código*

aproximación preliminar", *Revista Aranzadi Doctrina*l, N.º 2, 2021, disponible base de datos Aranzadi (BIB 2021, 159).

31. Conferência Ibero-Atlântica Justiça Criminal e Novas Tecnologias, 13 a 14 de junho de 2022, São Miguel, Açores, Portugal y la ponencia la *Geolocalização como meio de investigação em processo penal: possibilidades e limites.*

de Processo Penal[32] portugués es, en términos generales, muy escueto en lo que se refiere a aplicación de la tecnología en la investigación criminal; en ese sentido, se asemeja a la LECrim española antes de la reforma ya citada de 2015.

De hecho, al igual que ocurriera en España, el silencio del legislador portugués en este punto ha generado un debate teórico y práctico sobre la utilización del GPS en la investigación y los efectos de sus resultados en el proceso penal. Tanto en la doctrina, como en la jurisprudencia portuguesa encontramos posiciones divididas. Ahora bien, de algún modo quizá puede decirse que la posición crítica es más fuerte en la doctrina, ya que algunos órganos judiciales lusos admitieron inicialmente sin mucha discusión la utilización de estos medios técnicos de seguimiento y localización cual si se tratase de un rastreo ordinario; afortunadamente, como veremos, la interpretación de los órganos judiciales ha evolucionado hacía una posición más restrictiva. Repasemos brevemente algunas de las claves de este debate.

Los tribunales portugueses han admitido en muchas ocasiones su utilización con distintos argumentos, pero en otros se han pronunciado a la inversa. Veamos a continuación como han ido evolucionando esas posiciones a través de algunas de resoluciones judiciales. Inicialmente, en 2008, un *Tribunal de Relaçao de Évora* entendió[33] que se trata de un método de investigación atípico, similar al de la clásica vigilancia policial, que no exige la previa autorización judicial. Cinco años después, el *Tribunal da Relação do Porto*[34] rechazó que la investigación con GPS pueda equipararse al clásico seguimiento convencional porque el GPS permite trazar un perfil detallado de la vida pública y privada de una persona. De hecho, en la búsqueda de diligencia de investigación similar, el Tribunal de apelación de Oporto consideró que el GPS era próximo a la localización de un teléfono móvil y, por ende, que el régimen aplicable al GPS debía ser por analogía el de aquél (localización de un teléfono móvil a través de GSM). A finales del mismo año (2013), en esa misma línea el *Supremo Tribunal de Justiça*[35] confirmó que el GPS no era, ni podía tratarse como una diligencia de investigación similar a un simple rastreo policial, sino que la investigación a través de GPS debía sujetarse a los requisitos de la localización de un móvil y, por tanto, requiere ser autorizado por el Juez de instrucción, pero no necesita una especial motivación en la investigación de delitos de

32. En adelante CPP portugués.
33. Sentencia del Tribunal da Relação *de Évora* de 7 de octubre de 2008, proc. n.º 2005/08-1.
34. Sentencia del *Tribunal da Relação do Porto*, de 21 de marzo de 2013, proc. n.º 246/12-9.
35. Sentencia del *Supremo Tribunal de Justiça* 24 de octubre de 2013, en el proc. n.º 780/10.5JAPRT.S1

gravedad media o alta. En esa afortunada evolución de la posición de los tribunales lusitanos, más recientemente, seguimos encontrando tesis más exigentes desde el punto de vista de los derechos fundamentales y, por ende, críticas con la calidad de la regulación portuguesa. Así, el *Tribunal da Relação de Lisboa*[36] concluyó que, en el estado actual del CPP, el GPS constituye un medio oculto de investigación, cuyos resultados está prohibido valorar y que sólo sería admisible si el legislador regulase expresa y suficientemente su utilización.

La doctrina portuguesa mantiene, al igual que los tribunales, posiciones diversas en torno a esta diligencia de investigación. A falta de una habilitación legal expresa, los defensores de la utilización del GPS buscan, como también han hecho algunos tribunales, el apoyo legal en otros preceptos del CPP portugués; ya sea en el art. 125 del CPP y/o en el art. 187 del CPP.

Así, en lo que la legalidad de esta diligencia de investigación se refiere, un sector de la doctrina[37] se escuda en que el art. 125.º del CPP portugués admite todas las pruebas que no estén prohibidas por ley. Un argumento al que los críticos[38] responden subrayando que la geolocalización de una persona con fines de investigación penal representa una afectación en el derecho fundamental a la intimidad y, en consecuencia, debe ser el legislador quien prevea de modo suficiente cuáles son sus requisitos y sus límites. Y es que en lo que aquí importa, el art. 126.3 del CPP portugués a propósito de los medios de prueba prohibidos advierte que, a excepción de los casos previstos en el CPP, también es nula de pleno derecho la prueba obtenida mediante la intrusión en la vida privada.

A falta de esa previsión legal expresa, otros autores defienden asimismo la utilización del GPS, apoyándose analógicamente en el régimen legal prevista para las escuchas telefónicas en los arts. 187-190 del CPP

36. Sentencia del *Tribunal da Relação do Porto de Lisboa,* de 13 de abril de 2016, proc. n.º 2903/11.8TACSC.L1-3.

37. SANTOS CABRAL, S., "Artigo 189.º", en *Código de Processo Penal Comentado*, Almedina, Coimbra, 2004, pp. 842-843. RODRIGUES NUNES, D. A., "A Admissibilidade de obtenção, diretamente pelas autoridades de dados", *Revista Julgar*, N.º 32, 2017, pp. 97-122.

38. COSTA ANDRADE, M., "Métodos ocultos de investigação, que o futuro para o direito processual penal?", en *Simpósio em homenagem a Jorge de Figueiredo de Doas, por ocasião dos 20 anos do Código de Processo penal Português*, Coimbra Editora, Coimbra, 2009, pp. 545 y ss. PINTO DE ALBUQUERQUE, P., *Comentário do Código de Processo penal à luz da Constituição da República e a Convenção Europeia dos Direitos do Homem*, Universidade Católica Editora, Lisboa, 2011, pp. 332, 545, 696. SILVA RODRÍGUEZ, B., *Da Prova Penal, Tomo II. Bruscamente A(s) face(s) oculta(s) dos Métodos Ocultos de Investigação Criminal,* Lisboa, Editora Rey dos Livros, 2010, pp. 92 y ss. SILVA RAMALHO, D., *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, Coimbra, 2017, p. 237.

portugués. Y, en particular en el art. 189.2 del CPP que en lo que a la extensión se refiere establece que en el curso del proceso (sólo!) el Juez podrá ordenar o autorizar la obtención y la acumulación de registros de datos sobre la ubicación telefónica (…), respecto de determinados delitos (*vid*. art. 187.1 del CPP portugués) y personas (art. 187.4 del CPP portugués).

Frente a ambas tesis, la doctrina lusa crítica[39] con la falta de una previsión legal expresa de esta diligencia de investigación subraya que ninguno de los títulos habilitantes esgrimidos puede entenderse como una norma clara y suficiente en los términos de la jurisprudencia del TEDH. Ahora bien, a partir de ahí la oposición se divide al no ponerse de acuerdo sobre la "intensidad" de la afectación en la intimidad que representa el seguimiento a través de GPS. Y, por tanto, si esa anhelada regulación debe sujetar con carácter general la utilización de un GPS en la investigación penal a la previa autorización, ya sea del Fiscal o del Juez, o si por el contrario, la policía puede utilizarlo sin recabar previamente una autorización. Incluso existen posiciones discrepantes entre quienes se inclinan por la preceptiva autorización acerca de si los requisitos de las escuchas telefónicas deben extrapolarse miméticamente al GPS o, podrían relajarse alguna de las exigencias previstas para las escuchas telefónicas porque la colocación de un GPS para localizar y seguir a un investigado potencialmente representa una invasión menor en la esfera de los derechos fundamentales.

2. FRANCIA

A diferencia de lo que ocurre con la ley procesal penal portuguesa, el *Code de procédure pénale* francés, sí regula expresamente en la actualidad al igual que la LECrim la utilización del GPS como medio de investigación penal (*De la géolocalisation*, arts. 230-32 a 230-44)[40]. De hecho, la regulación francesa es casi coetánea[41] a la española, pero el marco legal es, como

39. SEABRA BRITO, M. B., *Novas Tecnologias e Legalidade da Prova em Processo Penal – Natureza e enquadramento do GPS como método de obtenção de prova*, Coimbra, Almedina, 2018. CARVALHO PEREIRA, B., *O Sistema de Geolocalização GPS no Processo penal Português,* Universidade de Lisboa, Faculdade de Direito, 2016, pp. 57-93. PINTO DE ALBUQUERQUE, P., *Comentário do Código de Processo penal à luz da Constituição da República e a Convenção Europeia dos Direitos do Homem*, *ob. cit*., pp. 332, 545, 696. COSTA ANDRADE, M., "Bruscamente no Verão Passado, a reforma do Código de Processo Penal – Observações críticas sobre uma Lei que podia e devia ter sido diferente", Coimbra, Almedina, 2009, pp. 113-184.

40. Capítulo V, del Título IV (*Dispositions communes*), del Libro I (*De la conduite de la politique pénale, de l'exercice de l'action publique et de l'instruction* del *Code de procédure pénale* francés.

41. *Vid*. la Ley n.º 2014-372 de 28 marzo 2014; cinco años después, algunos de los preceptos de la versión original del capítulo correspondiente al *Code de procédure pénale*

veremos inmediatamente a continuación, muchísimo más detallado que el nuestro.

El legislador francés dibuja, como comprobaremos inmediatamente a continuación, un régimen complejo con un ámbito objetivo acotado que, normalmente (salvo casos de urgencia de los que resulte un riesgo inminente para la investigación o para personas o bienes) requiere previa autorización del Ministerio Fiscal o del Juez competente (el de garantías constitucionales o el de la instrucción) y cuya duración varía en función de la gravedad del delito.

Con carácter general el *ámbito objetivo* se circunscribe[42] a la investigación de: delitos castigados con una pena de prisión igual o superior a 3 años; muerte violenta, por causa desconocida o sospechosa; desaparición de un menor o de un adulto necesitado de una especial protección atendiendo a circunstancias como su edad, su estado de salud, etc.; búsqueda de un prófugo contra el que se hubiera dictado un orden de detención, una condena firme a una pena de prisión igual o superior a un año, persona inscrita en el registro de autores de delitos de terrorismo que incumpliera alguna de las obligaciones del art. 706-25-7, persona inscrita en el

---

fueron objeto de modificación con la Ley n.º 2019-222 de 23 de marzo 2019. LE MONNIER DE GOUVILLE, P., "Le régime juridique de la géolocalisation: une pierre de plus à la mosaïque processuelle pénale", *Gazzete du palais: Recueil bimestral*, Vol. 134, N.º 4, 2014, pp. 2492-2496. VERGÈS, E., "Construire la norme en procédure pénale: une étude des techniques juridiques à travers un cas symptomatique, la géolocalisation", *Revue de science criminnelle et de droit pénal comparé*, N.º 3, 2014, pp. 599-610. PRADEL, J., "De la géolocalisation en procédure pénale. À la recherche d'un statut", *La Semaine Juridique*, N.º 3, 2014, pp. 100-105. Sin embargo, no siempre fue así, antes de 2014 el legislador francés tampoco preveía esta diligencia de investigación y, sin embargo, en la práctica se utilizaba en la investigación penal, a finales de octubre de 2013 la *Cour de cassation*, concluyó que era un medio de investigación que vulneraba el derecho a la vida del investigado porque carecía de un control judicial (*vid*. proc. n.º 13-81945, de 22 de octubre de 2013). FOURMENT, F., "La géolocalisation et la Convention EDH: l'ambivalence de la Cour de cassation", *La Semaine Juridique*, N.º 52, 2013, pp. 2389-2391. BONNET, A., "La licéité du recours à la surveillance par géolocalisation", *La Semaine Juridique*, N.º 3, 2012, pp. 83-86.

42. *Vid*. art. 230-32 del Code de Procédure pénale francés según el cual *(i)l peut être recouru à tout moyen technique destiné à la localisation en temps réel, sur l'ensemble du territoire national, d'une personne, à l'insu de celle-ci, d'un véhicule ou de tout autre objet, sans le consentement de son propriétaire ou de son possesseur, si cette opération est exigée par les nécessités: 1° D'une enquête ou d'une instruction portant sur un crime ou sur un délit puni d'au moins trois ans d'emprisonnement; 2° D'une procédure d'enquête ou d'instruction de recherche des causes de la mort ou de la disparition prévue aux art. 74, 74-1 et 80-4;*

3° D'une procédure de recherche d'une personne en fuite prévue à l'art. 74-2. La géolocalisation est mise en place par l'officier de police judiciaire ou, sous sa responsabilité, par l'agent de police judiciaire, ou prescrite sur réquisitions de l'officier de police judiciaire, dans les conditions et selon les modalités prévues au présent chapitre.

registro de autores de delitos sexuales o violentos que haya incumplido las obligaciones del art. 706-53-5, persona a la que se haya revocado la sustitución o suspensión de la ejecución de una pena o medida de seguridad de la que resulte como remanente la ejecución de una pena de prisión superior a un año.

El Ministerio Fiscal podrá autorizar la utilización de medios técnicos de geolocalización en el marco de la investigación de un delito flagrante por un plazo máximo de 8 días consecutivos, mientras que la autorización puede extenderse por un plazo mayor (de hasta 15 días consecutivos) cuando se tratase de la investigación preliminar de una muerte por causa violenta, sospechosa o desconocida; la desaparición de un menor o de un adulto necesitado de una especial protección atendiendo a circunstancias como su edad, su estado de salud, etc.; la búsqueda de un prófugo en alguna de las situaciones ya descritas; así como diversos delitos atribuidos esencialmente a la criminalidad organizada[43].

La utilización de cualquier dispositivo de geolocalización[44] más allá de cualquiera de estos dos plazos, el de 8 días consecutivos en caso de

43. Arts. 706-73 y 706-73-1 del *Code du Procédure Pénale* francés. Delitos cometidos por bandas organizadas entre los que se encuentran: asesinato, tortura y otros actos de barbarie, narcotráfico, secuestro; delitos graves de trata de seres humanos, proxenetismo, extorsión, falsificación de dinero, terrorismo, los que afectan a los intereses fundamentales de la nación, relativos a armas y productos explosivos, ayuda a la entrada, circulación y residencia ilegales de extranjeros en Francia, blanqueo de capitales y encubrimiento de los efectos resultantes de los delitos anteriores, asociación criminal cuando tengan por objeto alguno de los delitos anteriores o el secuestro de aeronave, barco o cualquier otro medio de transporte cometido, delitos castigados con al menos diez años de prisión, que contribuyan a la proliferación de armas de destrucción masiva; de explotación de una mina o de enajenación de una sustancia transmisible sin título o autorización minera, acompañado de daño al medio ambiente; estafa; ataque a los sistemas automatizados de tratamiento de datos personales implantados por el Estado; fuga; encubrimiento de actividades o empleados, os servicios de persona que realiza trabajo encubierto, negociación laboral, préstamo ilícito de mano de obra o empleo de extranjero sin permiso de trabajo; importación, exportación, tránsito, transporte, posesión, venta, adquisición o permuta de bienes culturales; daño al patrimonio natural cometidos en banda organizada; tráfico de productos fitosanitarios; participación en la dirección de una casa de juego; etc.

44. Art. 230-33 del CPP: *L'opération (…) est autorisée: 1° Dans le cadre d'une enquête de flagrance, d'une enquête préliminaire ou d'une procédure prévue aux arts. 74 à 74-2, par le procureur de la République, pour une durée maximale de quinze jours consécutifs dans les cas prévus aux arts. 74 à 74-2 ou lorsque l'enquête porte sur un crime ou sur une infraction mentionnée aux art. 706-73 ou 706-73-1, ou pour une durée maximale de huit jours consécutifs dans les autres cas. A l'issue de ces délais, cette opération est autorisée par le juge des libertés et de la détention à la requête du procureur de la République, pour une durée maximale d'un mois renouvelable dans les mêmes conditions de forme et de durée; 2° Dans le cadre d'une instruction ou d'une information pour recherche des causes de la mort ou des causes de la disparition mentionnées aux arts. 74, 74-1 et 80-4, par le juge d'instruction, pour une*

delitos flagrantes o el de 15 días consecutivos en el caso de los delitos graves citados, requiere entonces ya un control judicial previo. En tales casos, el Ministerio Fiscal solicitará la previa autorización Juez de libertades y detención; en ese caso el juez puede otorgar la autorización por 1 mes prorrogable; un plazo máximo inicial que se extiende hasta los 4 meses prorrogable por periodo igual o inferior cuando se trate de la investigación judicial por causa de muerte o desaparición previstas en los arts. 74, 74-1 y 80-4 del CPP. El plazo máximo general absoluto es 1 año, si bien excepcionalmente puede extenderse hasta los 2 años, en la investigación de los delitos cometidos por bandas organizadas que recogen los arts. 706-73 o 706-73-1 del CPP francés.

Como ya hemos adelantado, la preceptiva previa autorización del fiscal o del juez competente que, respectivamente dependiendo de su menor o mayor duración, requiere la utilización de un GPS en el marco de una investigación criminal puede ceder excepcionalmente[45] y adoptarse directamente por la policía judicial, bajo su responsabilidad, en casos de urgencia de los que resulte un riesgo "inminente" de pérdida de pruebas o de un daño grave para personas o bienes. El agente de la policía judicial que adoptase esta decisión o el oficial que ordene en tales supuestos la geolocalización está obligado a informar inmediatamente, por cualquier

durée maximale de quatre mois renouvelable dans les mêmes conditions de forme et de durée. La durée totale de cette opération ne peut pas excéder un an ou, s'il s'agit d'une infraction prévue aux arts. 706-73 ou 706-73-1, deux ans. La décision du procureur de la République, du juge des libertés et de la détention ou du juge d'instruction est écrite et motivée par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

45. *Vid*. art. 230-35 del *Code du Procédure Pénale* francés, así *(e)n cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens, les opérations mentionnées à l'art. 230-32 peuvent être mises en place ou prescrites par un officier de police judiciaire.* No obstante, el legislador francés establece algunos límites a la instalación de un GPS cuando ello conlleve de una actuación que puede ser estar en liza con la privacidad de algún lugar (instalarlo o remover), requiriendo entonces la autorización correspondiente y, en su caso, su realización dentro de una franja horaria *(c)elui-ci en informe immédiatement, par tout moyen, le procureur de la République ou le juge d'instruction dans les cas mentionnés aux arts. 230-33 et 230-34. Ce magistrat peut alors ordonner la mainlevée de la géolocalisation. Toutefois, si l'introduction dans un lieu d'habitation est nécessaire, l'officier de police judiciaire doit recueillir l'accord préalable, donné par tout moyen: 1° Dans les cas prévus au 1° de l'art. 230-33, du juge des libertés et de la détention, saisi à cette fin par le procureur de la République; 2° Dans les cas prévus au 2° du même art. 230-33, du juge d'instruction ou, si l'introduction doit avoir lieu en dehors des heures prévues à l'art. 59, du juge des libertés et de la détention, saisi à cette fin par le juge d'instruction. Ces magistrats disposent d'un délai de vingt-quatre heures pour prescrire, par décision écrite, la poursuite des opérations. A défaut d'une telle autorisation dans ce délai, il est mis fin à la géolocalisation. Dans les cas prévus au premier alinéa du présent article, l'autorisation comporte l'énoncé des circonstances de fait établissant l'existence du risque imminent mentionné à ce même alinéa.*

medio, al fiscal o al juez de instrucción, quien podrá revocar o ratificar la decisión. Ahora bien, por si cupiese alguna duda, el legislador francés subraya que esa excepción al control previo ya sea del fiscal o del juez en los casos de urgencia descritos no alcanza al supuesto en que la colocación del dispositivo exija la entrada en el domicilio.

El Tribunal Constitucional francés se pronunció recientemente[46] sobre la constitucionalidad de la decisión del legislador francés de delegar, en la mayoría de los casos y salvo que se vaya a dilatar en el tiempo, en el Ministerio Fiscal la autorización sobre la utilización de un GPS en la investigación. El *Conseil Constitutionnel* avaló la constitucionalidad de este régimen legal, pero subrayó algunas cuestiones muy interesantes. Por un lado, que la investigación mediante GPS constituye una invasión de la privacidad en cuanto representa el seguimiento de una persona mediante una localización continua y en tiempo real de todos sus movimientos, así como el registro y el tratamiento de los datos así obtenidos; ahora bien, insistió en que esa injerencia en la privacidad no conlleva acto alguno de coacción, tampoco daños personales, ni la detención, la interceptación de comunicaciones o la captación o grabación de imágenes o de sonidos. Por otro lado, en cuanto al hecho de que la autorización corresponda con carácter general al Ministerio Fiscal cuando el seguimiento no se prolongue en el tiempo, el alto Tribunal recordó que, en el modelo de proceso penal francés, el fiscal es una autoridad a quien corresponde en particular controlar la legalidad de los medios utilizados por los investigadores y la proporcionalidad de los actos de investigación en relación con la naturaleza y la gravedad de los hechos. Y en esa línea destacó que, de acuerdo con el CPP francés, el Fiscal sólo puede autorizar la investigación mediante GPS cuando así lo exijan las necesidades de una investigación relativa a un delito castigado con al menos tres años de prisión, la investigación para determinar las causas de una muerte de una persona o su desaparición en los casos expresamente previstos o la búsqueda de un fugitivo también en supuestos singulares; y, por tanto, que el Ministerio Fiscal no puede autorizar la colocación de un GPS en las investigaciones de los delitos citados por tiempo superior a 8 días o en la investigación de delitos relacionados con bandas organizadas por encima de 15 días porque por encima de tales plazos el control corresponde a la autoridad judicial por un plazo máximo inicial de 1 mes prorrogable hasta un máximo de 1 año con carácter general o de 2 años en materia de delincuencia organizada.

46. Sentencia del *Conseil constitutionnel,* de 23 de septiembre de 2021. Ya lo había hecho con anterioridad a propósito de la primera versión en 2014 de la geolocalización en el *Code du Procédure Pénale*, *vid*. Sentencia del *Conseil constitutionnel*, de 25 marzo 2014. MATSOPOULOU, H., "L'illégalité des surveillances par 'géolocalisation' autorisées par le ministère publicnote sous Crim. 22 oct. 2013 [2 arrêts]", *Recueil Dalloz*, N.º 2, 2014, pp. 115-120.

En definitiva, en opinión del *Conseil Constitutionnel*, el legislador francés ha rodeado la utilización de GPS en la investigación criminal de garantías suficientes que aseguran, dentro del respeto a las prerrogativas de la autoridad judicial, un equilibrio entre el fin constitucionalmente legítimo de encontrar al autor del delito y el derecho fundamental al respeto la vida privada.

3. ITALIA

Al igual que en Portugal y que en España antes de la LO 13/2015, el *Codice di procedura penale*[47] italiano no regula específicamente la geolocalización como medio de investigación penal. Sin embargo, en la práctica se utiliza con relativa frecuencia como técnica de seguimiento y localización, al igual que como hemos visto ocurre en Portugal. Sin embargo, a diferencia de la evolución de la interpretación de los órganos judiciales lusos, la jurisprudencia italiana no sólo aceptó hace más de una década esta medida de investigación atípica, sino que además concluyó con carácter general que la policía puede utilizar los dispositivos y/ los medios técnicos sin necesidad de ningún un control previo, ya sea del Ministerio Fiscal o de la autoridad judicial.

La *Corte de Cassazione* italiana ha mantenido de forma constante que es un medio atípico de búsqueda de pruebas que la policía puede utilizar sin autorización previa y su resultado puede ser objeto de valoración judicial. La *Corte di Cassazione* equipara el seguimiento por GPS con la vigilancia policial (*pedinamento*) de la que, a su juicio, sólo difiere en que el GPS facilita ese rastreo tecnológicamente a distancia. Los arts. 55, 347 y 370 del CPP italiano permiten a la policía realizar actividades que no vulneren sustancialmente los derechos y las libertades fundamentales; y en opinión de la Corte, en términos de injerencia en la privacidad, la localización y el seguimiento a través de GPS no puede equipararse a otras diligencias de investigación tecnológica más lesivas como pueden ser la interceptación de las comunicaciones porque a lo sumo representa leve invasión en la privacidad, por lo que no requiere previamente una orden del Ministerio Fiscal y tampoco la autorización del Juez. De hecho, la *Corte di Cassazione* ha convalidado que el resultado puede valorarse incluso en casos extraordinarios[48], como p.ej. falte el archivo original bien porque se hubiese perdido o el soporte informático que lo contuviese sufriese un error técnico,

47. *Decreto del Presidente della Repubblica*, 22 settembre 1988, n. 447.

48. *Vid*. entre otras, Sentencias de la Corte de *Cassazione penale*, sección III de 4 de febrero de 2019, n. 36364; sección II de 7 de noviembre de 2012, n.º 40611; sección IV de 27 de noviembre de 2012, n. 48279.

ya que en su opinión ello no afectaba a la fiabilidad probatoria de las coordinadas transcritas en anotaciones e informes y que podían introducirse también en el juicio a través de las declaraciones de los policías.

La doctrina[49], sin embargo, no comparte unánimemente el criterio jurisprudencial. Si bien un amplio sector coincide con la *Corte de Cassazione* en que este tipo de diligencia de investigación tecnológica no debe exigir un control previo del Ministerio Fiscal o del Juez por la escasa a su juicio afectación que conlleva en el derecho fundamental a la intimidad, afortunadamente también existen voces críticas con esa posición al entender que infravalora la injerencia que potencialmente representa en la privacidad de un individuo el seguimiento por GPS. Ahora bien, incluso, la mayoría del sector doctrinal que defiende que la utilización de un GPS en el marco de investigación penal no requiere una autorización previa, sí reclama por seguridad jurídica al legislador italiano una regulación clara al respecto.

IV. BALANCE DE LA INVESTIGACIÓN POR GPS EN EL SUR DE EUROPA

La aproximación realizada nos ofrece un dibujo muy heterogéneo sobre la investigación penal a través de GPS en España, Portugal, Francia e Italia. Y es que, si bien el GPS se utiliza con mayor o menor frecuencia en los procesos penales de los países objeto de estudio, este medio de

49. FANUELE, C., "Il rilevamento satellitare tramite GPS: una prassi da ancorare ai principi stabiliti dalla Cedu", *Diritto penale e proceso*, N.º 12, 2019, pp. 1701-1711. BENE, T., *"Il pedinamento elettronico: truismi e problemi spinosi"*, en AA.VV. *Le indagini atipiche* (Scalfati, A., Dir.), Torino, Giappichelli Editore, 2014, pp. 350 y ss. COSTANZO, P., "Note preliminari sullo statuto giuridico della geolocalizzazione (a margine di recenti sviluppi giurisprudenziali e legislativi)", *Diritto dell'informazione e dell'informatica*, Vol. 30, N.º 3, 2014, pp. 331-344. SERRANI, A., "Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie", en *Archivo penale*, 2013. IOVENE, F., "Pedinamento satellitare e diritti fondamentali della persona", *Cassazione penale*, Vol. 52, N.º 10, 2012, pp. 3556-3565. SIGNORATO, S., "La localizzazione satellitare nel sistema degli atti investigativi", en *Rivista italiana di diritto e procedura penale*, 2012, pp. 580-607. BRUNO, O., "La localizzazione elettronica tra indagine e prova", en *Giustizia penale*, III, 2011, pp. 684 y ss.; STRAMAGLIA, M., "Il pedinamento satellitare: ricerca ed uso di una prova atípica", en *Diritto penale e proceso*, N.º 2, 2011, pp. 213-224. GENTILE, D., "Tracking satellitare mediante GPS: attività atipica di indagine o intercettazione di dati?", en *Diritto penale e proceso*, 2010, N.º 12, p. 1464. CHELO, A., "Manchia, Localizzazione tramite GPS: quali garanzie?", en *Rivista giuridica Sarda*, 2006, 432; VELANI, L. G., "Nuove tecnologie e prova penale: il sistema d'individuazione satellitare GPS", en *Giurisprudenza italiana*, 2003, pp. 2372 y ss. PERETOLI, P., "Controllo satellitare con GPS: pedinamento o intercettazione?", en *Diritto penale e proceso*, N.º, 9, 2003, pp. 93-101. LARONGA, A., "L'utilizzazione probatoria del controllo a distanza eseguito con sistema satellitare g.p.s.", en *Cassazione penale*, 2002, pp. 3050 y ss.

investigación no siempre está regulado, e incluso allí donde lo está sus requisitos y límites son muy diversos.

A continuación, trataremos de ofrecer un balance del GPS en estos sistemas procesales penales desde el punto de vista de la garantía de los derechos fundamentales. Para ello, tomaremos en consideración cuatro variables: i) la previsión legal (o no) de la localización y el seguimiento a través de GPS; ii) la delimitación (o no) del ámbito objetivo de delitos o circunstancias en cuya investigación puede utilizarse el seguimiento mediante GPS; iii) la necesidad (o no) de una previa autorización; iv) el plazo, menor o mayor, por el que puede extenderse la geolocalización.

En lo que a la regulación se refiere, en la actualidad de los cuatro países del estudio sólo España y Francia recogen expresa y suficientemente la utilización de dispositivos de GPS o similares. De hecho, las reformas legales que introdujeron esta diligencia de investigación en sus respectivas leyes procesales fueron casi simultáneas: 2014 en Francia y 2015 en España. Sin embargo, antes de esa previsión legal, la jurisprudencia española y francesa no compartían en general la misma posición sobre la injerencia que representaba el seguimiento por GPS. Mientras hasta 2015 el Tribunal Supremo[50] español avalaba que en la mayoría de los casos la colocación por la policía de un GPS no requería su previa autorización judicial, en cambio *Cour de cassation*[51] francesa mantenía de forma constante que las pruebas obtenidas de GPS eran nulas precisamente porque no existía esa norma legal que determinase las condiciones de utilización de la geolocalización y que cumpliese los requisitos de previsibilidad, claridad y precisión del art. 8.2 del CEDH. En una situación diametralmente opuesta se encuentran Portugal e Italia, donde el GPS continúa siendo en la fecha en que se escriben estas líneas una diligencia de investigación *atípica*.

Si ponemos el foco en el ámbito objetivo de delitos en cuya investigación podría utilizarse el GPS, volvemos a encontrarnos con escenarios relativamente antagónicos. Desde el *Code de Procédure Pénale* francés donde el GPS no sólo se circunscribe a un ámbito objetivo de investigaciones muy concreto, sino que además los límites son de algún modo estrictos. Pasando a países como España, Portugal e Italia en los que el legislador no establece fronteras objetivas para el seguimiento y la localización a través de GPS. Ahora bien, la ausencia de esos límites objetivos no significa que la situación en España, Portugal e Italia sea idéntica. Y es que, como

50. SSTS 798/2013, 5 de noviembre; 906/2008, 19 de diciembre; 523/2008, 11 de julio; 562/2007, 22 de junio¸ 55/2007, 23 de enero.

51. Sentencias de la *Cour de Cassation* de 15 de octubre de 2014 o la de 22 de octubre de 2013.

ya hemos adelantado, en Portugal e Italia la indefinición de un ámbito objetivo concreto obedece a un déficit absoluto de norma legal, mientras que España sí regula esta diligencia de investigación lo único que ocurre es que el legislador español, a diferencia del francés, decidió no delimitar (y, por tanto, restringir) el ámbito objetivo de las investigaciones en las que puede utilizarse un GPS. La LECrim no acota estrictamente el ámbito delictual de la investigación por GPS, a través de parámetros cualitativos o cuantitativos, pero eso no significa que la investigación a través de GPS esté desprovista de límites. Por un lado, debe recordarse que el legislador español recoge unos principios rectores[52] (especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida) a los que queda plenamente sujeta, entre otras[53], la investigación por GPS. Y, por otro lado, que las disposiciones específicas[54] relativas al seguimiento y la localización, contrarrestan de algún modo la ausencia de límites objetivos concretos subrayando que la utilización del GPS debe circunscribirse a investigaciones en que *concurran acreditadas razones de necesidad y la medida resulte proporcionada*[55].

El repaso comparado de la investigación mediante GPS en lo relativo a la exigencia de un control previo nos ofrece de nuevo una imagen dual.

52. *Vid*. art. 588 bis a de la LECrim.

53. Recordemos la rúbrica Capítulo IV del Título VIII del Libro II de la LECrim lleva por rúbrica "(d)isposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, *la utilización de dispositivos técnicos de seguimiento, localización* y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos" (la cursiva es nuestra).

54. Véase, el apartado primero del art. 588 quinquies b de la LECrim.

55. BERNAOLA LORENZO, A., "Los dispositivos técnicos de geolocalización. Garantías y límites", *Revista Aranzadi Doctrinal*, N.º 11, 2021, disponible base de datos Aranzadi (BIB 2021, 5362). RUIZ RODRÍGUEZ, A., "¿Puede una confidencia anónima justificar una invasión estatal de la intimidad a través de la colocación de balizas de seguimiento? Comentario a la STS 141/2020, de 13 de mayo", *La Ley Penal*, N.º 146, septiembre-octubre 2020, disponible a través de la base de datos La Ley LA LEY *13093/2020.* MAGRO SERVET, V., "Requisitos para la validez de la geolocalización policial por dispositivos electrónicos como mecanismo de investigación", *Diario La Ley*, N.º 9723, 26 de octubre de 2020, disponible a través de la base de datos La Ley LA LEY *12507/2020.* RODRÍGUEZ LAINZ, J. L., "La nueva jurisprudencia sobre dispositivos de seguimiento y localización", *Diario La Ley*, N.º 9650, 10 de junio de 2020, disponible a través de la base de datos La Ley, LA LEY *6377/2020.* RICHARD GONZÁLEZ, M., "Ilicitud de la prueba por falta de motivación del Auto de autorización judicial de un dispositivo de seguimiento GPS en el vehículo del sospechoso", *LA LEY Probática*, N.º 1, Tercer trimestre de 2020, disponible a través de la base de datos La Ley, LA LEY *11338/2020.* GUTIÉRREZ MAYO, E., "Admisión y valoración de pruebas obtenidas afectando los derechos de la privacidad", *LA LEY privacidad*, N.º 6, Cuarto trimestre de 2020, disponible a través de la base de datos La Ley, LA LEY *13483/2020.*

En España y en Francia, el legislador procesal exige –desde mediados de la década de 2010– como regla general que el seguimiento y la localización mediante GPS sea previamente autorizado, en España por el Juez de Instrucción y en Francia de acuerdo con el modelo de proceso penal francés por el Fiscal por un tiempo máximo de 8 o 15 días, mientras que en Portugal y en Italia al faltar una regulación expresa, los tribunales se han inclinado por entender que esta diligencia de investigación no requiere una previa autorización. No obstante, la posición jurisprudencial no es idéntica en los dos países ya que si bien en Italia, la *Corte de cassazione* parece (hasta el momento) tener una opinión unívoca, en los tribunales lusos se han alzado voces discrepantes en los últimos tiempos que sí entienden que debe recabarse autorización previa.

Volviendo sobre el caso español y francés, la analogía en la regla general del requisito de autorización previa se extiende a los supuestos excepcionales en que ese control previo, del Ministerio Fiscal o de la autoridad judicial, puede ceder. Así el legislador recoge casi de forma idéntica en ambos países que un GPS puede excepcionalmente colocarse por la policía sin solicitar y esperar autorización previa, en casos de urgencia que pudiesen hacer fracasar la investigación. En palabras de la LECrim cuando *concurran razones de urgencia que hagan razonablemente temer que de no colocarse inmediatamente* (…) *se frustrará la investigación*; que enuncia *mutatis mutandis* el *Code de Procédure Pénale*[56] en los siguientes términos *en caso de emergencia resultante de un riesgo inminente de pérdida de pruebas o daños graves a personas o bienes.* No obstante, la similitud de tales supuestos no puede interpretarse aisladamente, sino que en la práctica han de ponerse en relación con *el ámbito objetivo* más estricto de investigaciones en las que en Francia cabe utilizar un GPS que el que como ya hemos visto establece nuestra LECrim que no circunscribe objetivamente el ámbito de investigaciones en que puede utilizarse el GPS.

Por último, en lo que a la configuración temporal se refiere, como parece lógico sólo allí donde existe una regulación expresa, como ocurre en España y Francia, existe un sistema de plazos preciso para la investigación criminal mediante GPS. El régimen francés es en este punto, como ya ocurriera con el ámbito objetivo, más detallado que el español. El *Code de Procédure Pénale* francés establece una duración preliminar máxima en el caso de que la diligencia sea autorizada por el Ministerio Fiscal de 8 días o de 15 días en la investigación de delitos de bandas organizadas, más allá de ese ínterin de tiempo la autorización corresponde a la autoridad

56. *Vid*. art. 230-35 del *Code du Procédure Pénale*: (*e)n cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens, les opérations mentionnées à l'art. 230-32*.

judicial estableciéndose un máximo inicial en general de 1 mes prorrogable hasta un máximo de 1 año o de 2 años (24 meses) en materia de delincuencia organizada. La LECrim española extrapola el sistema general de plazos que prevé como regla general para todas las diligencias de investigación limitativas de derechos fundamentales del art. 18 de la CE que pueden prolongarse en el tiempo: un plazo máximo inicial de 3 meses, prorrogable por periodos iguales o inferiores hasta el máximo absoluto de un año y medio (18 meses). A priori el régimen de plazos español y francés sobre la utilización del GPS en una investigación penal no parece sustancialmente muy diferente. Sin embargo, si se observa en detalle, a nuestro juicio el sistema francés es un poquito más garantista que el español por dos matices. Por un lado, el establecimiento de un plazo inicial mucho más perfilado. Recordemos en el caso de que lo autorice el fiscal un máximo provisionalísimo de 8 días o de 15 días en el caso de bandas organizadas, a lo que se une algo que debemos destacar el que la decisión judicial menos provisional pueda extenderse por un máximo inicial de 1 mes[57] mientras que en España ese plazo es tres veces superior (3 meses); deberíamos advertir que el legislador español únicamente fija este mismo plazo inicial en el registro remoto de equipos informáticos, que es una de las dos diligencias de investigación tecnológica que considera más graves. Parece fuera de toda duda que supeditar un medio de investigación a un control judicial periódico de como máximo 1 mes es más estricto que hacerlo cada 3 meses. Por otro lado, el plazo máximo general absoluto es ¼ menor en Francia que en España, 12 meses frente a 18 meses; otra cosa es que el legislador francés prevea un máximo excepcional superior en casos de investigaciones por delincuencia organizada de hasta 24 meses frente a los 18 meses que como máximo puede prolongarse en España.

En definitiva, en una escala de mayor a menor protección de los derechos fundamentales, el análisis comparado de la utilización del GPS en la investigación criminal en los cuatro países objeto de estudio ofrece el siguiente resultado: en primer lugar, Francia; inmediatamente a continuación y muy próximo, España; seguido, de Portugal y, en último lugar muy alejado, Italia.

57. Arts. 230-32 y 706-73-1 del *Code du Procédure Pénale.*

Capítulo 3

La Directiva 2016/680/UE: un nuevo paradigma para el tratamiento de datos de carácter personal con fines penales

Juan Alejandro Montoro Sánchez[1]

Investigador Postdoctoral Margarita Salas[2]
Universidad Pablo de Olavide de Sevilla-Instituto de Justicia y Litigación "Alonso Martínez" de la Universidad Carlos III de Madrid

I. LA ERA DIGITAL: EL NUEVO ESCENARIO GLOBAL REGIDO POR LA TECNOLOGÍA Y EL TRATAMIENTO DE LA INFORMACIÓN

En las cuatro últimas décadas, aunque con más intensidad desde inicios del siglo XXI, estamos siendo testigos de la radical transformación, sin paragón en toda la historia de la humanidad, que está sufriendo la sociedad a nivel global. El incesante desarrollo y la alta penetración que presentan las cada vez más avanzadas e innovadoras Tecnologías de la Información y Comunicación (en adelante TICs) en prácticamente todas las esferas de nuestras vidas, pueden señalarse como dos de las principales causantes y motores de este este nuevo contexto mundial.

La expansión de las TICs ha llegado a tal punto, que es posible afirmar, sin miedo a equivocación, que resultan imprescindibles para realizar

1. Trabajo vinculado al Proyecto de Investigación de Excelencia del Ministerio de Economía y Competitividad "Límites a la utilización de datos, evidencias e información entre procesos y procedimientos diversos en España y la Unión Europea (LUDEI)".
2. Esta publicación ha sido financiada por la Unión Europea "NextGenerationEU", por el Plan de Recuperación, Transformación y Resiliencia y por el Ministerio de Universidades, en el marco de las ayudas Margarita Salas, para la Recualificación del sistema universitario español 2021-2023 convocadas por la Universidad Pablo de Olavide, de Sevilla.

la práctica totalidad de las tareas y actividades que llevamos a cabo en nuestro día a día. De hecho, es difícil pensar en algún reducto en que estas tecnologías no hayan encontrado alguna utilidad y conseguido implementarse de alguna manera. Así, las utilizamos como herramientas indispensables de nuestros puestos de trabajo, hacemos uso de ellas para comunicarnos y relacionarnos con nuestros familiares y amigos, para adquirir los bienes y servicios más tradicionales o los más punteros que se ofrecen el mercado o incluso para relacionarnos y hacer trámites con las Administraciones Públicas.

Podría decirse que es inconcebible que hoy día, una persona, incluidos los adolescentes menores de edad y nuestros mayores, no disponga de un teléfono inteligente[3] o que un hogar no cuente, al menos, con acceso a internet a través de fibra óptica[4]. Y es que hemos pasado en las últimas cuatro décadas, de vivir en una sociedad analógica, a estar inmersos en una sociedad plenamente digital ante la denominada revolución industrial 4.0[5]. Ha sido tal el nivel de la transformación, que difícilmente encajan en la sociedad actual o cuanto menos ven impedido el desarrollo de su vida cotidiana, aquellas minorías que rechazan la dependencia forzosa de estas tecnologías o aquellas otras que meramente no dominan su uso por razones de edad o por la dificultad de acceso a las mismas[6].

Ahora bien, si algo caracteriza a estas tecnologías disruptivas y a la multitud de servicios que han surgido en torno a ellas, es que su

3. De acuerdo con las últimas estadísticas publicadas por la CNMC sobre el sector de las telecomunicaciones, en agosto de 2022, existían en España, en activo, un total de 56896715 de líneas móviles, de las cuales 49.435.554 contaban además con servicio de acceso a internet de banda ancha. Es decir, existen más líneas en activo que población al existir una tasa de penetración –líneas/100 habitantes– de 107,5. Consultado en http://data.cnmc.es/datagraph/jsp/inf_anual.jsp (Último acceso, 20 de agosto de 2022).
4. En este caso, los datos de la CNMC arrojan un total de 16.710.090 líneas de banda ancha fija, lo que representa una tasa de penetración de 35,3. Consultado en http://data.cnmc.es/datagraph/jsp/inf_anual.jsp (Último acceso, 20 de agosto de 2022).
5. Se recomienda la lectura del excelente trabajo de BARONA VILAR, S., *Algoritmización del derecho y de la justicia: de la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021, pp. 42-76. En el mismo se hace un completo estudio de no sólo de las notas que caracterizan a la Revolución Industrial 4.0 en la que nos encontramos inmersos, si no que efectúa un completo recorrido histórico de las anteriores fases que se han sucedido hasta llegar al presente.
6. Especialmente preocupante es la situación de las personas mayores ante los usos impuestos de las TICS por parte de empresas y Administraciones Públicas, situación que ha contribuido a crear una importante brecha digital que incluso puede desembocar en situaciones de vulnerabilidad. *Vid*. CÍVICO ARIZA, A., "Vulnerabilidad de las personas mayores ante la brecha digital: análisis bibliométrico", en TORRES FERNÁNDEZ, C. (Coord.) *Avances y prospectiva en la protección jurídico-social de las personas en situación de vulnerabilidad*, Tirant lo Blanch, Valencia, 2022, pp. 223-239.

funcionamiento se sustenta fundamentalmente en una actividad primordial: el procesamiento de información. Y muy particularmente en el de la información que tiene carácter personal. Es decir, aquella que directa o indirectamente concierne a una concreta persona física identificada o que alternativamente puede identificarse por el prestador, sin un esfuerzo desproporcionado. Baste decir que sin la captación y el posterior tratamiento de datos personales, los proveedores se verían impedidos, sino de la prestación de los servicios digitales más extendidos y exitosos, de muchas de sus funcionalidades más relevantes y apreciadas por los consumidores.

Por ello, la carga de facilitar los datos recae, por lo general, en los propios usuarios, hasta el punto de que se ven obligados a entregarlos si desean hacer un uso plenamente funcional de tales herramientas. Así sucede, por ejemplo, con la información que se incorpora a los perfiles de las redes sociales[7] o con la información que se proporciona a los cada vez más usuales dispositivos y electrodomésticos del Internet de las Cosas (IoT)[8]. Otros datos, en cambio, se generan automáticamente durante el funcionamiento de los propios servicio o incluso se extraen deliberadamente por el proveedor a través del análisis inteligente del conjunto de datos de los usuarios, como ocurre respectivamente, con los datos de tráfico que resultan del uso de cualquier servicio de comunicaciones electrónicas y con de los perfiles de consumo y hábitos elaborados por los proveedores mediante herramientas de BigData o Inteligencia Artificial[9].

La paradoja de este panorama es que en la mayoría de los supuestos, tales datos se facilitan o generan incluso sin que los propios titulares sean plenamente conscientes de ello y del verdadero alcance de la cesión y de su destino. Prácticamente, ningún usuario se lee las extensas y complejísimas condiciones contractuales impuestas que regulan las prestaciones de dichos servicios[10]. Y es que no debe obviarse que tales datos se erigen

7. MARTÍNEZ MARTÍNEZ, R., "Protección de datos personales y redes sociales: un cambio de paradigma" en RALLO LOMBARTE, A. (Coord.) *Derecho y redes sociales*, Civitas, Cizur Menor, 2010, pp. 83-116.

8. ARELLANO TOLEDO, W., Privacidad e Internet de las Cosas: (Internet of Things, IoT) en *Revista de privacidad y derecho digital*, núm. 6, 2017, pp. 25-56.

9. CHAVES VALDIVIA, A. K., "Entre los perfiles a la carta y la protección de datos personales: el producto eres tú", en BUENO DE MATA, F. (Dir.) *Hacia una Justicia 2.0: actas del XX Congreso Iberoamericano de Derecho e Informática*, Ratio Legis, Salamanca, 2016, pp. 67-79.

10. En el estudio realizado por el Consejo Noruego del Consumidor en 2020 se estimó que la lectura detenida de las condiciones de uso de las aplicaciones y redes sociales más utilizadas puede llevar incluso más de una hora, superando el tiempo que habría que dedicar a obras literarias como Macbeth.. https://magnet.xataka.com/preguntas-no-tan-frecuentes/tiempo-que-tardarias-leer-terminos-condiciones-uso-tus-apps-grafico. (Última consulta, 20 de agosto de 2022).

además en moneda de cambio, puesto que constituyen la auténtica contraprestación para el proveedor por el acceso a las aplicaciones, habida cuenta de su carácter gratuito o del precio simbólico de la mayoría de estas. Es decir, el modelo de negocio arquetípico funciona del siguiente modo: los servicios se prestan gratuitamente a condición de que los datos que se capten de los usuarios y terceras personas puedan ser reutilizados y explotados empresarialmente por los operadores para otras finalidades comerciales distintas, que son las que les proporcionan el verdadero y principal beneficio económico.

Dada la extrema utilidad y el consecuente inmenso valor que han alcanzado los datos personales, no es de extrañar que a la actual época se la denomine la Era de la Información, o que a los datos personales se les califique como el petróleo del siglo XXI. Para confirmarlo no hay más que comprobar como las empresas con mayor capitalización bursátil a nivel mundial basan su modelo de negocio, directa o indirectamente, en el tratamiento y análisis de la información personal que recopilan masivamente a través de las aplicaciones y servicios que ofrecen al público, habiendo conseguido desplazar muchos puestos atrás a las compañías y corporaciones multinacionales cuyo negocio se ha centrado en la venta de bienes y servicios tradicionales y que hasta hace recientes fechas ocupaban dichos puestos[11].

II. LA DIRECTIVA 2016/680/UE: UN INSTRUMENTO PARA GARANTIZAR LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES DE LOS CIUDADANOS EN EL ÁMBITO PENAL

La utilidad de muchas de las categorías de datos personales que se procesan a través de las variadas tecnologías y herramientas digitales que están al alcance de la población, no se reduce a los fines meramente comerciales o técnicos previamente mencionados. Debido a la extraordinaria y variada información que albergan y a la que son susceptibles de revelar, ya sea por sí mismos o analizados en su conjunto, los datos de carácter personal son en la actualidad elementos esenciales del sistema de justicia penal[12], puesto que permiten a las autoridades implicadas el

11. A cierre del ejercicio 2021, siete de las diez primeras empresas con mayor valor a nivel global, son tecnológicas y utilizan los datos personales como fuente directa o indirecta de ingresos. Únicamente la petrolera saudí Aramco, se cuela entre las cinco primeras. https://cincodias.elpais.com/cincodias/2021/12/30/companias/1640886339_354215.html. (Última consulta, 20 de agosto de 2022).
12. ORTIZ PRADILLO, J. C., "Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal", *Diario La Ley*, núm.

desarrollo de las labores de investigación penal, el esclarecimiento de multitud de hechos de naturaleza criminal así como a la determinación de sus autores y partícipes. Máxime, en este momento en que gran parte de la delincuencia cuenta con, al menos, algún componente electrónico o digital en los medios o fines comisivos, lo que implica que necesariamente existan huellas digitales –datos personales en muchos supuestos– susceptibles de ser aprehendidas y utilizadas[13]. Dicho con otras palabras, los datos personales pueden convertirse en trascendentes evidencias y fuentes de prueba que pueden ser utilizados en las actividades llevadas a cabo por las autoridades policiales y judiciales de detección, investigación y enjuiciamiento de delitos. Y ello, hasta el punto de haberse erigido en elementos imprescindibles e inherentes a todo proceso penal, puesto que no es posible su normal desarrollo sin que exista un tratamiento, siquiera meramente identificativo de las partes y demás intervinientes, de datos personales. La localización de un terminal móvil en los alrededores de la escena del crimen, las muestras de fluidos corporales o las grabaciones de un sistema de videovigilancia son buena muestra de datos personales que sirven a tal capital función.

Por otro lado, debemos tener en cuenta que los datos y la información en formato electrónico cuentan con la gran ventaja de ser fácilmente conservables durante largos periodos de tiempo y dejar una huella digital, prácticamente indeleble, que permite asegurar, no solo su trazabilidad e integridad, sino incluso su fiabilidad[14]. Siendo consciente del gran potencial de los datos en el ámbito penal –e incluso en el sancionador administrativo– y de su alta disponibilidad, no sólo las autoridades recurren con más frecuencia a obtenerlos de proveedores y terceros como fuentes de prueba o incluso como cuerpo o efecto del delito en su sentido más amplio, sino que el propio legislador ha promovido la aprobación de normas encaminadas a la creación de diversas bases de datos tanto públicas como privadas con miras a conservar masiva y preventivamente, diversas categorías de datos personales vinculados a distintos ámbitos, por si algún momento resultaren necesarios para una concreta investigación penal. Es el caso de las bases de datos de tráfico de las comunicaciones electrónicas que los operadores de telecomunicaciones deben mantener en virtud de las obligaciones impuestas por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas

9955, 2021, p. 3 y MONTORO SÁNCHEZ, J. A. *Uso y cesión de datos de carácter personal en el proceso penal*, Aranzadi, Cizur Menor, 2022, p. 331.

13. ORTIZ PRADILLO, J. C., "Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal", *op. cit.*, p. 3.
14. DELGADO MARTÍN, J., "La prueba electrónica en el proceso penal" en Diario La Ley, núm. 8167, 2013.

y a las redes públicas de comunicaciones[15] o la base de dato PNR –Passsenger Name Records– creada *ex* Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves[16].

Visto lo anterior, podría pensarse que tanto los operadores privados como las autoridades implicadas en la represión criminal cuentan con plena libertad para recopilar y hacer uso de los datos de carácter personal de los ciudadanos para perseguir sus propios intereses o ejercer las funciones pública que legalmente le competen. No obstante, nada más lejos de la realidad, toda vez que los datos de carácter personal cuentan con una férrea protección constitucional al situarse bajo el halo protector que brinda el derecho fundamental a la protección de datos de carácter personal, que en España se proclama en el art. 18.4 CE y en el ámbito europeo en el art. 8 tanto del Convenio Europeo de Derechos Humanos Mientras como de la Carta de Derechos Fundamentales de la Unión Europea.

Sobre este derecho, nuestro Tribunal Constitucional, en su célebre Sentencia 292/2000, de 30 de noviembre, ya determinó que se trataba de un derecho fundamental autónomo, distinto de la intimidad personal y familiar, de naturaleza instrumental, que tiene por misión proteger al individuo de los riesgos y peligros que pueden derivarse para los demás derechos reconocidos en el ordenamiento jurídico, de la utilización de sus datos de carácter personal por parte de terceros, incluido el Estado. Y para prestar dicha protección, otorga al titular, como contenido esencial, amplios poderes de control y disposición sobre sus propios datos, que le facultan para decidir cuáles proporciona a un tercero o cuáles puede este recabar, saber quién los posee y para qué finalidad, y oponerse a dicha posesión y uso. Además, para garantizar la efectividad de dichos poderes, se atribuyen al titular una serie de facultades de las que se derivan obligaciones de contenido positivo para el responsable del tratamiento, que se materializan a través de los conocidos por

15. COLOMER HERNÁNDEZ, I., "Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016" en RUDA GONZÁLEZ, A. y JEREZ DELGADO, C. (Coords.) *Estudios sobre Jurisprudencia Europea: materiales del I y II Encuentro anual del Centro español del European Law Institute*, Sepín Editorial Jurídica, Las Rozas, pp. 767-781.

16. CATALINA BENAVENTE, M. A., *El uso de los datos PNR en el proceso penal*, Aranzadi, Cizur Menor, 2022 y CATALINA BENAVENTE, M. A., "Entrada en vigor de la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves" en *Diario La Ley*, núm. 9737, 2020.

su acrónimo como derechos ARCO –acceso, rectificación, cancelación y oposición–[17].

Ahora bien, habiendo transcurrido prácticamente cuarenta años desde que se aprobara la primigenia ley reguladora de este derecho fundamental, la ya derogada Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, hallamos un panorama prácticamente disfuncional en lo que atañe a la adecuada y genérica aplicación de las garantías dimanantes de este derecho en el ámbito de la justicia penal, lo cual no ha sucedido, en cambios, en otros ámbitos extrajurisdiccionales dónde también tienen cabida éstas. Por ejemplo, en el sector privado y en el ámbito de las Administraciones Públicas, nos encontramos con una aplicación bastante aceptable y prácticamente generalizada del grueso de la normativa, al menos desde que se aprobara la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal con la que se transpuso al ordenamiento nacional la primera norma europea sobre la materia, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. Si bien, es cierto que cuando se ha conseguido adquirir una verdadera cultura de cumplimiento y la consciencia de la importancia del respeto de la normativa, ha sido a raíz de la entrada en vigor del Reglamento General de Protección de Datos en el año 2016 –en parte por el peso de su rotundo régimen sancionador– y de la intensa y loable labor formativa y educativa llevada a cabo por la Agencia Española de Protección de Datos.

Lamentablemente, en la Administración de Justicia y particularmente en el orden jurisdiccional penal, el nivel de cumplimiento por parte de los órganos judiciales en el ejercicio de sus funciones jurisdiccionales no ha sido equivalente. Puede decirse que se arrastra un importante déficit en la observancia de las garantías asociadas a la privacidad, pese a la especial trascendencia que adquiere este derecho fundamental en el proceso[18]. Y es que, como veremos con posterioridad, la privacidad opera en el ámbito procesal con varias manifestaciones exclusivas que no tienen cabida en otros ámbitos extrajudiciales, que tienen la capacidad de provocar importantes consecuencias jurídicas. De hecho, únicamente en el aspecto organizativo de los medios informáticos utilizados en la oficina judicial es

17. Sentencia 292/2000, de 30 de noviembre de 2000. «BOE» núm. 4, de 4 de enero de 2001.
18. ORTIZ PRADILLO, J. C., "Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal", *op. cit*., p. 7 y PÉREZ GIL, J., "Investigación penal y nuevas tecnologías: algunos de los retos pendientes" en *Revista Jurídica de Castilla y León*, núm. 7, p. 226.

dónde puede haber existido un nivel más satisfactorio de cumplimento, pero en los aspectos puramente procesales, es más complicado verificar una escrupulosa observancia de los principios y obligaciones asociados al derecho a la protección de datos. Salvo casos aislados, la práctica judicial ha demostrado que no suele ir más allá de la mera incorporación a pie de resolución de un mero aviso informativo genérico y estereotipado dirigido a las partes, que en ningún caso no colma las exigencias legales mínimas requeridas.

Gran parte de esta problemática se debe a la inexistencia de un marco jurídico específico destinado a reglamentar las actividades de tratamiento de los datos personales por parte de la autoridad judicial. Las distintas leyes que han precedido al nuevo paquete legislativo aprobado por la Unión Europea en el año 2016, ni siquiera mencionaban a los Juzgados y Tribunales como destinatarios y operadores sujetos al cumplimiento de las garantías establecidas en las mismas. De hecho, la Directiva 95/46/CE, norma origen de la Ley Orgánica 15/1999, exceptuaba expresamente de su ámbito de aplicación al procesamiento de datos llevado a cabo por las autoridades con fines de salvaguarda de la seguridad pública y al destinado en materia penal[19]. Por su parte, aunque la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, sí resultaba aplicable a la actividad penal, excluía específicamente de su ámbito el tratamiento llevado a cabo por los órganos judiciales nacionales de los Estados miembros, pues se destinaba específicamente a establecer un nivel de protección mínimo a la información intercambiada mediante mecanismos de cooperación judicial y policial transnacional.

Tan solo en el año 2015, el legislador introdujo en la Ley Orgánica del Poder Judicial un pequeño capítulo de diez artículos[20] –236 *bis* a *decies*– con el objeto de dotar a la Administración de Justicia de un marco jurídico sobre la materia. No obstante, el mismo se limitaba a regular únicamente ciertos aspectos residuales, principalmente de carácter organizativo, por

19. Véase el art. 3.1 de la Directiva 95/46/CE sobre ámbito de aplicación en el que se especificaba que: *"Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales: – efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal…".*

20. Dicho marco jurídico se articuló a través de la Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

lo que resultó claramente insuficiente, al no despejar la práctica totalidad de interrogantes que surgían en torno a la práctica procesal. Finalmente, la inercia de la costumbre en las prácticas judiciales, la falta de formación específica de los operadores jurídicos implicados en el proceso –jueces y magistrados, abogados y fiscales– y la inactividad del Consejo General del Poder Judicial como autoridad de control en la materia, han otros sido los demás factores que han contribuido a la latencia de este escenario de inobservancia general en detrimento de los derechos de los interesados.

No obstante, este panorama está llamado a cambiar a raíz de la aprobación de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Con ella el legislador europeo ha pretendido poner remedio a esta situación de incertidumbre estableciendo las bases de un marco jurídico común para los Estados miembros, con el potente objetivo de permitir la circulación e intercambio de datos personales con fines de represión del delito, garantizando a la par, un alto y homogéneo nivel de protección para los ciudadanos[21].

Se trata del instrumento legislativo revulsivo que está llamado a transformar radicalmente el modo en que todas las autoridades penales de los Estados miembros, pero especialmente, los juzgados y tribunales del

21. Para un estudio del proceso legislativo seguido para la aprobación de la Directiva y de sus fines y principios se recomienda la lectura de: PILLADO GONZÁLEZ, E., "Principios generales de protección de datos en la cesión de información en la persecución criminal a la vista de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por la que se deroga la Decisión Marco 2008/977" en *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano*, MORENO CATENA, V. y ROMERO PRADAS, M. A. (Dirs.), Tirant lo Blanch, Valencia, 2021, pp. 783-820; COLOMER HERNÁNDEZ, I., "Control y límites en el uso de los datos personales penales en la investigación y represión de los delitos a la luz de la Directiva 2016/680" en *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano*, MORENO CATENA, V. y ROMERO PRADAS, M. A. (Dirs.), Tirant lo Blanch, Valencia, 2021, pp. 737-782 y FIODOROVA, A., "Directiva 2016/680: hacia mayor coherencia de protección de datos personales en la cooperación policial y judicial penal" en MORENO CATENA. V. y ROMERO PRADAS, M. I. (Dirs.) *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano*, Tirant lo Blanch, Valencia, 2021, pp. 709-736 y CARUANA, M., "The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement" en *International Review of Law*, Computers & Technology, núm. 33, 2019, pp. 249-270.

orden penal recopilan y procesan datos de carácter personal no sólo en las distintas fases del proceso penal, sino incluso en las actividades de índole preventiva. Y para ello, impone a los órganos judiciales, como autoridades competentes incluidas expresamente dentro de su ámbito de aplicación, toda una serie de principios, reglas y limitaciones de obligada observancia en todas las actividades y funciones en que tenga lugar el tratamiento de datos con la finalidad última de garantizar, en la medida de lo posible, los poderes de control y disposición que se atribuyen al interesado, en tanto que representan los ejes nucleares sobre los que se articula del derecho fundamental a la autodeterminación informativa.

Antes de examinar su contenido, es imprescindible señalar que la Directiva 2016/680/UE ha sido transpuesta al ordenamiento interno –con prácticamente tres años de retraso[22] y mediando la sanción más elevada impuesta por el Tribunal de Justicia de la Unión Europea hasta la fecha por incumplimiento del plazo máximo previsto en su articulado– a través de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Tal dilación, ha contribuido, sin duda alguna, y a pesar del indiscutible efecto directo de la Directiva, a prolongar innecesariamente el disfuncional escenario reinante en nuestros órganos judiciales penales respecto a las condiciones y garantías en que se desarrolla del tratamiento de datos.

Apuntado todo lo anterior, procede analizar, en primer lugar, las diferentes dimensiones con las que opera el derecho a la protección de datos en el marco del proceso penal, dado que ello permitirá obtener una panorámica de su trascendente influencia. Para después examinar las novedades más relevantes que se derivan de la aplicación efectiva de las medidas contempladas en la Directiva 2016/680, con particular énfasis en aquellas que presentan connotaciones procesales, y que en definitiva, veremos que son de tal alcance, que nos permiten colegir de un cambio de paradigma en lo que respecta al tratamiento de datos judicial encaminado a la investigación y enjuiciamiento del delito.

22. El art. 63 de la Directiva establecía como plazo límite para la adopción y publicación de las disposiciones legales, reglamentarias y administrativas necesarias para su transposición, el pasado 6 de mayo de 2018. Dado el retraso del legislador español, la Comisión Europea instó ante el Tribunal de Justicia de la Unión Europea, en fecha 4 de septiembre de 2019 un recurso por incumplimiento con arreglo a los artículos 258 TFUE y 260 TFUE, que dio lugar a la Sentencia de 25 de febrero de 2021, asunto C-658/19, en la que se condenó al Estado al abono de 15 millones de euros a tanto alzado y 89 mil euros por cada día de retraso adicional, todo ello en concepto de multa.

III. LAS DIMENSIONES DEL DERECHO A LA PROTECCIÓN DE DATOS EN EL PROCESO PENAL

El vínculo de conexión entre los datos personales y el proceso penal es particularmente estrecho e intenso. Podría decirse que ambas realidades son indisociables, dado que el tratamiento de datos se prolonga durante todo el desarrollo del proceso, a lo largo de sus distintas fases, sin perjuicio de que sea la instrucción la etapa en la que éste es especialmente relevante por su función recopiladora. Este vínculo es incluso más trascendente si atendemos a la operativa y los efectos con los que se presenta el derecho fundamental a la protección de datos de carácter personal en este ámbito. Y es que este tiene la particularidad de operar desde una perspectiva multidimensional[23] con manifestaciones propias y exclusivas de este entorno que no concurren en otros ámbitos. Procede analizar brevemente a cada una de estas dimensiones y las implicaciones que se derivan de las mismas, puesto que nos permitirá comprobar el importante alcance y repercusión de este derecho fundamental en la justicia penal.

1. DERECHO A LA PROTECCIÓN DE DATOS COMO DERECHO SUBJETIVO: DIMENSIÓN SUSTANTIVA

El derecho fundamental a la protección de datos de carácter personal despliega sus efectos en el marco del proceso judicial a través de su dimensión puramente sustantiva. Esto es, desde su vertiente de derecho subjetivo reconocido a la persona física que atribuye a su titular un haz de facultades positivas, en este caso frente al órgano judicial como responsable del tratamiento, en aras de permitirle el control y el poder de disposición que ostenta sobre sus propios datos personales. Mientras, por su parte, el órgano judicial como responsable del tratamiento, se encuentra sometido a la obligación de dar oportuno cumplimiento a los deberes dimanantes de este

23. MARCOS AYJÓN también destaca las diversas implicaciones del derecho fundamental a la protección de datos en el proceso, mas solo respecto al orden penal, exponiendo que: "*… desde todos los aspectos posibles, se puede estructurar en tres apartados perfectamente diferenciados: 1.º En el ámbito organizativo y de gestión, donde el Letrado de la Administración de Justicia cumple un papel principal. 2.º En el ámbito procesal, ya sea en el aspecto referido a recabar pruebas con pleno respeto al derecho fundamental a la protección de datos de carácter personal, o cuando se accede a los datos e información contenidas en el proceso penal. 3.º En el aspecto sustantivo: Los delitos que protegen el derecho fundamental a la protección de datos de carácter personal*". MARCOS AYJÓN, M., "Protección de datos personales y Letrado de la Administración de Justicia. Un difícil encaje en el marco legal actual" en GUTIÉRREZ ZARZA, M. A. (coord.) *Los retos del espacio de Libertad, Seguridad y Justicia de la Unión Europea en el año 2016: Reunión anual ReDPE*, Wolters Kluwers, Madrid, 2016. En el mismo sentido MONTORO SÁNCHEZ, J. A., *Uso y cesión de datos de carácter personal en el proceso penal*, *op. cit.*, pp. 252-253.

derecho, especialmente el de información así como a dar curso a las solicitudes de derechos ARCO que le sean planteadas respecto al tratamiento que efectúe de los datos personales de los interesados en tanto ejercita la función jurisdiccional. Se trata ésta, de la faceta genuina de este derecho fundamental, correspondiendo a la que se extiende genéricamente a cualquier ámbito en el que sea de aplicación la normativa de protección de datos. En cualquier caso, habida cuenta del cúmulo de derechos e intereses privados y públicos que intervienen en el proceso, el derecho a la protección de datos puede verse modulado en diferentes grados de afección. Por tal motivo, nos encontramos con un régimen específico y modulado de este derecho el orden jurisdiccional penal, que permita aunar el interés del Estado en la represión del delito con los derechos fundamentales de los intervinientes en el mismo. Nos encontraríamos, por tanto, ante una dimensión del derecho a la protección de datos que, aunque vinculada al proceso en tanto que se trata de una fuente de tratamiento de datos personales ante la que despliega su cobertura protectora, carece de naturaleza procesal alguna y actúa, por tanto, en paralelo, desligada del desarrollo y desenlace del proceso. Incluso en el plano legal la normativa de protección de datos atinente a esta faceta discurre de forma separada y no convergente respecto de la normativa procesal en sentido estricto, sin perjuicio de la existencia de algún aspecto que puntual y tangencialmente pueda afectar a este derecho.

2. DERECHO A LA PROTECCIÓN DE DATOS COMO CONDICIONANTE DE LA ORGANIZACIÓN DE MEDIOS DE LOS ÓRGANOS JUDICIALES

Muy ligada a la anterior dimensión, e incluso pudiendo tildarse como su complemento indispensable, el derecho a la protección de datos afecta a la justicia penal desde una perspectiva organizativa. Así tanto el personal perteneciente a la Administración de Justicia, como los medios materiales –especialmente los sistemas y aplicaciones informáticas que intervienen en el tratamiento– que se utilizan y contribuyen en el desarrollo de la actividad jurisdiccional, deben estar orientados y configurados de tal modo que permitan garantizar los principios organizativos y de seguridad reconocidos en la normativa de protección de datos y con ello, la seguridad e integridad de los datos. Ello se traduce en la necesidad adaptar toda la organización judicial a una serie de políticas, directrices, reglas y prácticas que tiendan a garantizar la seguridad e integridad de los datos y con ello los derechos de los interesados cuyos datos son tratados[24].

24. Para un estudio más detallado y pormenorizado de las medidas de seguridad y sus implicaciones en la organización, puede consultarse: TRONCOSO REIGADA, A.,

Aspectos nucleares de esta dimensión del derecho lo constituyen el respeto a las exigencias de seguridad establecidas en el art. 29 y siguientes de la Directiva, la preceptiva realización de la evaluación de impacto y la observancia escrupulosa de los principios de protección de datos desde el diseño y por defecto[25] que deben tenerse en cuenta a la hora de desarrollar e implementar soluciones tecnológicas, protocolos y prácticas por parte de las Administraciones encargadas de proveer las herramientas técnicas utilizadas por los órganos judiciales.

3. DERECHO A LA PROTECCIÓN DE DATOS COMO LÍMITE A LA ACTIVIDAD INVESTIGATORIA Y A LA ACTIVIDAD PROBATORIA

El derecho fundamental a la protección de datos puede operar además en el ámbito del proceso bajo una dimensión puramente procesal, dado que es susceptible de condicionar el modo en que se realizan diversos actos y fases del proceso. Ello viene determinado por la consideración del derecho fundamental que se ve afectado por ciertas actividades procesales de investigación propias de la fase de instrucción penal y en algunos casos por la actividad probatoria pueden efectuar las partes, habida cuenta de que requieren del desarrollo previo de operaciones que suponen un tratamiento de datos de carácter personal. Así pues, el derecho a la protección de datos se constituye como afirmó la Segunda del Tribunal Supremo en su sentencia 471/2017 de 23 de febrero en "*una fuente de limitación de la actividad estatal, en la medida en que la vulneración en el proceso de derechos y libertades fundamentales del investigado abre una grieta en la estructura misma del proceso penal y puede generar efectos contaminantes no solo respecto de las pruebas así obtenidas sino también en lo que concierne a otros actos procesales conectados con las mismas*". Por tanto, la adopción y ejecución de diligencias de investigación de las que se desprenda una aprehensión, recogida o

"La seguridad en el Reglamento General de Protección de Datos de la Unión Europea" en *Actualidad administrativa*, núm. 1, 2019; RECIO GAYO, M., "Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control" en PIÑAR MAÑAS, J. L. (Dir.) *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, pp. 351-366 y PRADA ESPINA, D., "Análisis y gestión de riesgos de los tratamientos de datos personales" en MURGA FERNÁNDEZ, J. P., FERNÁNDEZ SCAGLIUSI M. A. y ESPEJO LERDO DE TEJADA, M. (Dirs.), *Protección de datos, responsabilidad activa técnicas de garantía*, Reus, Madrid, 2018, pp. 349-374.

25. DUASO CALÉS, R., "Los principios de protección de datos desde el diseño y protección de datos por defecto" en PIÑAR MAÑAS, J. L. (Dir.) R*eglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, pp. 295-320.

tratamiento de datos deben producirse con pleno respeto al derecho fundamental, lo que exige la toma en consideración de los principios rectores y demás reglas establecidas en la Directiva como elementos adicionales tradicionales establecidos en la Ley de Enjuiciamiento Criminal. Idéntico planteamiento puede ser extrapolado a la actividad de obtención y práctica de fuentes de prueba en el plenario. Los efectos de la transgresión de dichas prácticas es susceptible de provocar, en los supuestos más graves, la exclusión e ineficacia procesal de los resultados de dichas diligencias o de las fuentes de prueba por operatividad de la regla establecida en el art. 11.1 LOPJ[26].

4. DERECHO A LA PROTECCIÓN DE DATOS COMO LÍMITE LA TRANSFERENCIA E INTERCAMBIO DE DATOS ENTRE AUTORIDADES PENALES INTERNACIONALES

La última de las facetas con las que este derecho fundamental se presenta guarda relación con uno de los objetivos perseguidos por el legislador europeo en la Directiva 2016/680: la libre circulación e intercambio de datos personales entre autoridades de los Estados miembros y de terceros. Si bien este se marca como un objetivo perseguido, no es menor cierto, que también está sujeto a estrictas limitaciones para garantizar los derechos de

26. Alcanzan las mismas conclusiones: COLOMER HERNÁNDEZ, I., "Control y límites en el uso de los datos personales penales en la investigación y represión de los delitos a la luz de la Directiva 2016/680" en Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano, MORENO CATENA, V. y ROMERO PRADAS, M. A. (Dirs.), Tirant lo Blanch, Valencia, 2021, pp. 737-782; GUTIÉRREZ ZARZA, M. A., "La protección de datos personales como derecho fundamental del imputado, ¿también en el ámbito del proceso penal?" en *La ley penal: revista de derecho penal, procesal y penitenciario*, núm. 71, 2010; PÉREZ ESTRADA, M. J., "Efectos de la vulneración de la protección de los datos personales en el proceso penal" en *La Ley Penal: revista de derecho penal, procesal y penitenciario*, núm. 135, 2018; FRÍAS MARTÍNEZ, E., "Obtención de datos personales en procesos penales y administrativos" en *Diario La Ley*, núm. 9404, 2019; DELGADO MARTÍN, J., "Protección de datos y prueba en el proceso" en *Diario La Ley*, núm. 9383, 2019 y CASERO LINARES, L., "Nulidad de la prueba por vulneración de los principios y derechos sobre protección de datos" en GUTIÉRREZ ZARZA, M. A. (coord.) *Nuevas Tecnologías, protección de datos personales y proceso penal*, La Ley, Las Rozas, 2012, pp. 399-400; AZAUSTRE RUÍZ, P., "Acercamiento al régimen jurídico-procesal previsto para la utilización de la información obtenida en un proceso penal distinto" en COLOMER HERNÁNDEZ, I. (Dir.) *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*, Aranzadi, Cizur Menor, 2017, pp. 345-366 y GÓMEZ ÁLVAREZ, F. J., "La cesión de datos de carácter personal entre procesos penales ante la doctrina del tribunal constitucional y el nuevo marco normativo de la protección de datos de carácter personal" en COLOMER HERNÁNDEZ, I. (dir.) *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Aranzadi, Cizur Menor, 2019, pp. 69-118.

los interesados. En un marco de cooperación judicial cada vez más desarrollado, que pivota sobre el reconocimiento mutuo y el principio de disponibilidad, el derecho a la protección de datos aparece como un límite a dichos intercambios. Por tal motivo, se requiere que el ordenamiento jurídico del Estado o el instrumento convencional de la organización internacional al que se destinen los datos garantice niveles de protección de este derecho, al menos equivalentes a los de la Unión Europea.

IV. LOS PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS EN LA JUSTICIA PENAL

En el Capítulo II de la Directiva 2016/680, que tiene como rúbrica "Principios" se enuncian una serie de reglas y fundamentos heterogéneos sobre los que se articula todo el sistema de protección de datos[27]. Estos principios vertebradores constituyen el núcleo fundamental de las obligaciones que incumben a los órganos judiciales como autoridades responsables del tratamiento, motivo por el que deben ser observados minuciosa y diligentemente a lo largo de todas las fases del tratamiento[28].

Son, por tanto, elementos que gozan de especial trascendencia en la materia puesto que se erigen en parámetros de referencia para la toma de decisiones y el aseguramiento de una respuesta respetuosa con los derechos fundamentales[29]. Es más, estos actúan como auténticos principios informadores, en tanto en cuanto permiten extraer criterios con los que cubrir las lagunas normativas que puede surgir ante la ausencia de soluciones específicas en la legislación sectorial. Por su parte, a los interesados, el modo en que se apliquen estos principios les permiten valorar la adecuación del tratamiento llevado a cabo por la autoridad judicial a las exigencias que dimanan del derecho a la protección de datos y su regulación. Por tanto, su inobservancia, especialmente en la adopción o ejecución de

27. APARICIO SALOM, J., "La calidad de los datos", en TRONCOSO REIGADA, A. (Dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Cizur Menor, 2010, p. 324, alude a la heterogeneidad de los principios, si bien, todos ellos contribuyen a un fin común, garantizar los poderes de control y disposición que atribuye al interesado el derecho fundamental a la protección de datos sobre sus propios datos.
28. *Vid*. TRONCOSO REIGADA, A., "El principio de calidad de los datos", en TRONCOSO REIGADA, A. (Dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Cizur Menor, 2010, pp. 340-343.
29. PILLADO GONZÁLEZ, E., "Principios generales de protección de datos en la cesión de información en la persecución criminal a la vista de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por la que se deroga la Decisión Marco 2008/977", *op. cit*., pp. 783-820.

diligencias de investigación, podrá servir a las partes como motivo para impugnar e intentar excluir datos del proceso que se hayan tratado sin la suficiente adecuación. Motivo por el que los órganos instructores deben velar especialmente por su estricto cumplimiento. Y es que, a pesar de que los mismos no se dispongan expresamente en la Ley de Enjuiciamiento Criminal, es posible colegir que los mismos adquieren una relevancia procesal indiscutible, hasta el punto de que deben ser tenidos en cuenta por el juez, de forma adicional a los principios rectores genéricos establecidos en el art. 588 bis a) LECrim, cuando se adopte una medida de investigación de la que se derive el tratamiento de datos.

Estos principios rectores se proclaman en el art. 4 de la Directiva –art. 6 de la Ley Orgánica 7/2021–, encontrándose entre éstos: el principio de licitud; principio de lealtad; principio de limitación de la finalidad del tratamiento; principio de minimización; principio de exactitud; principio de seguridad y principio de proactividad. No obstante, nos centraremos en el estudio de los que cuentan con un mayor protagonismo en el ámbito procesal.

1. PRINCIPIO DE LICITUD

Es el art. 8 de la Directiva 2016/680/UE el que conceptúa y configura a este principio rector. En virtud del mismo, el tratamiento de datos será lícito cuando se cumplan acumuladamente los siguientes presupuestos: 1) Como presupuesto subjetivo, que se acometa por una autoridad competente del sistema de justicia penal. En este caso, los tribunales de dicho orden jurisdiccional lo son. 2) Como factor teleológico, que el tratamiento de datos tenga por finalidad la investigación o enjuiciamiento de un delito, o la ejecución de una pena. 3) Como factor legitimador, que la autoridad cuente con la correspondiente habilitación legal para el tratamiento de los datos que se pretenden procesar. Reserva de ley que viene motivada por la necesaria adecuación que debe existir entre la medida restrictiva de derechos fundamentales a la que nos enfrentamos y los cánones y parámetros de proporcionalidad y necesariedad establecidos en la Carta de Derechos Fundamentales de la Unión Europea y la jurisprudencia del Tribunal Europeo de Derechos Humanos. Y es que no debe obviarse, que toda recogida y/o posterior tratamiento de datos por una autoridad competente supone una injerencia en el derecho a la vida privada de las personas y a la protección de sus datos de carácter personal tal y como ha reiterado el TJUE en su constante jurisprudencia[30].

30. Las sentencias del Tribunal de Justicia de la Unión Europea, caso *Schwarz* (C-291/12), de 17 de octubre de 2013, apartado 25, y caso *Digital Rights Ireland y otros* (C-293/12

En base a lo expuesto, toda obtención de datos que se consiga sin cobertura legal específica debe reputarse ilícita, y en consecuencia, los datos así obtenidos no deberían teóricamente tener entrada en el proceso de conformidad con la regla prevista en el art. 7.3 de la Directiva 2016/680. Lo cierto es que en nuestro ordenamiento encontramos en el art. 236 ter LOPJ una cláusula general habilitante para el tratamiento de datos por parte de los órganos judiciales. No obstante, es imprescindible advertir que el tratamiento de categorías de datos sensibles o especialmente protegidos a los que se hace referencia en el art. 10 de la Directiva 2016/680 –datos relativos a la salud, vida sexual y genética, a las creencias y convicciones internas de todo tipo, datos biométricos, etc.–, requiere de una base legal específica que habilite el tratamiento[31] habida cuenta de su naturaleza y la especial capacidad que presentan para revelar aspectos nucleares sobre la vida privada de las personas. Es decir, la base legitimadora del art. 236 *ter* LOPJ no ampara, por sí misma, la obtención de datos pertenecientes a estas categorías especiales, si no que se exige una reserva de ley específica. En el ordenamiento jurídico podemos encontrar diversos ejemplos de habilitaciones específicas para el acceso y uso de dichos datos por los órganos judiciales penales, como la prevista en el art. 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación

y C-594/12), de 8 de abril de 2014, apartado 36, recogen la doctrina jurisprudencial por la que se considera que se produce una injerencia los derechos a la protección de datos de carácter personal por el mero hecho de que un responsable trate datos personales, y ello con independencia de la operación en que consista éste, al expresar que *"Dichas operaciones [comunicación, acceso, etc.] son asimismo constitutivas de una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta, puesto que constituyen tratamientos de datos de carácter personal"*. Dicha doctrina se confirma de modo específico, en lo que respecta a las autoridades competentes del orden penal en la sentencia del Tribunal de Justicia de la Unión Europea, caso *Ministerio Fiscal* (C-207/16), 2 de octubre de 2018, en cuyo parágrafo 51 se expresa que *"En cuanto a la existencia de una injerencia en los derechos fundamentales, procede recordar que (…) el acceso de las autoridades públicas a estos datos constituye una injerencia en el derecho fundamental al respeto de la vida privada, consagrado en el artículo 7 de la Carta, incluso a falta de circunstancias que permitan calificar esta injerencia de «grave» y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia. Tal acceso también constituye una injerencia en el derecho fundamental a la protección de los datos personales garantizado por el artículo 8 de la Carta, puesto que constituye un tratamiento de datos personales [véase, en este sentido, el Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 124 y 126 y jurisprudencia citada]"*.

31. El art. 10 de la Directiva exige para su tratamiento una autorización específica y concreta para la autoridad en el ordenamiento interno o de la Unión, únicamente cuando los datos fueren manifiestamente públicos o el uso fuere imprescindible proteger los intereses vitales del interesado o de otra persona física, podrían tratarse sin esa base.

clínica respecto del acceso al historial clínico y datos de salud o la prevista en el art. 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria respecto a los datos con trascendencia tributaria. No obstante, debe advertirse que existen ciertos datos sensibles, como los relativos a convicciones religiosas o la vida sexual, que no cuentan con dicha habilitación, lo que impide teóricamente su utilización en el proceso penal.

2. PRINCIPIO DE LIMITACIÓN DE LA FINALIDAD DEL TRATAMIENTO

El principio de limitación de la finalidad puede calificarse como la clave de bóveda del sistema protector del derecho a la protección de datos. Se reconoce en el art. 4.1.b) de la Directiva 2016/680/UE y en el ámbito interno ha sido transpuesto a través del art. 6.1.b) Ley Orgánica 7/2021 bajo la fórmula: *"Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines"*.

Debe partirse de que la recogida de cualquier dato personal –ya sea directamente del propio interesado o de otra fuente alternativa mediante una medida de investigación– y su posterior tratamiento deben obedecer, necesariamente, a la consecución de unos fines perfectamente definidos. A su vez, estos fines pueden interpretarse en dos sentidos diferenciados[32]. En primer lugar, como fines generales para los que la autoridad está legalmente habilitada a actuar, que en este caso sería la investigación o enjuiciamiento de unos actos delictivos o para la ejecución de una pena. En segundo, como fines específicos, y que se refieren al concreto delito que se pretende investigar o enjuiciar o a la pena que se pretende ejecutar, y que por lo tanto deben ser correctamente predefinidos por la propia autoridad judicial con carácter previo a la obtención del dato a través de la resolución habilitante que permita su recogida o tratamiento.

Pues bien, consideramos que es ésta última concepción del término "fines" a la que se refiere necesariamente el principio de limitación de la finalidad del tratamiento, pues es la única interpretación que resulta coherente de un análisis sistemático de la Directiva y especialmente de sus objetivos.

32. RODRÍGUEZ-MEDEL NIETO, C., "La Directiva 2016/680 relativa a la protección de las personas físicas en el tratamiento de sus datos personales para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales" en ARANGÜENA FANEGO, C. y HOYOS SANCHO, M. (Dirs.) *Garantías procesales de investigados y acusados: situación actual en el ámbito de la Unión Europea*, Tirant Lo Blanch, Valencia, 2018, pp. 381-420.

Ello implica que, en principio, los órganos judiciales se verían impedidos de destinar los datos obrantes en un sumario que han sido obtenidos para investigar un concreto delito, para ser utilizados en la investigación o enjuiciamiento de otros delitos distintos. Es decir, existe una prohibición de transmutar o ampliar los fines específicos a los que se destinan los datos personales que obran en poder de un órgano judicial.

No obstante, en nuestro ordenamiento procesal encontramos dos preceptos que chocan frontalmente con este planteamiento. Nos referimos a los arts. 579 *bis* y 588 *bis* i) LECRim, los cuales permiten la reutilización de datos obtenidos en un procedimiento en otro distinto, bien como medio de investigación o como fuente de prueba, sin ningún tipo de límite.

Lo cierto es que la Directiva 2016/680 prevé en el apartado 2.º del artículo 4 una regla excepcional a dicho principio de limitación de la finalidad, que permite a las autoridades competentes que puedan destinar los datos, por sí mismas o a una tercera, previa cesión, a unos fines penales distintos y desconectados de los que motivaron su recogida inicial. En cualquier caso, esta cesión de datos está fuertemente restringida y para que se repute conforme con las garantías del derecho fundamental a la protección de datos exige que concurran acumuladamente los siguiente requisitos.

1) En primer lugar, que la autoridad que dedique los datos a una nueva finalidad esté legitimada, mediante ley, para desarrollar la actividad a la cual se destinan los datos. Es decir, la legislación del Estado miembro debe atribuir el ejercicio de competencias penales a la autoridad para el desarrollo de los fines genéricos a los que se destinan y de la que se derive la necesidad de tratamiento de datos. Por ejemplo, cuando con motivo de un hallazgo casual, un Juzgado de Instrucción comunica los datos a otro órgano judicial de idéntica naturaleza, a efectos de que se despliegue la investigación, es imprescindible, que el cesionario de los datos esté legitimado por ley para la investigación del delito y, además, ostente competencia.

2) En segundo lugar, que el nuevo tratamiento pretendido debe ser necesario y proporcionado con relación a los nuevos fines. Es decir, cada cesión debe ser individualmente sometida a un previo juicio de proporcionalidad desde la óptica de la jurisprudencia constitucional y del Tribunal Europeo de Derechos Humanos, que atienda a las circunstancias específicas de cada caso y a los derechos e intereses confrontados.

De este modo, únicamente cuando se supere dicho filtro, debería operar la regla de reutilización establecida en la LECrim y permitirse la limitación del principio de finalidad del tratamiento[33].

3. PRINCIPIO DE MINIMIZACIÓN

El principio de minimización de los datos, se establece en el art. 4.1c) Directiva 2016/680. En su virtud, los datos personales que se traten por una autoridad judicial deben de ser *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"*. Como puede comprobarse, mediante este principio se persigue minimizar, en la medida de lo posible, el número de datos personales que se tratan para conseguir unos fines concretos[34]. Por ello, la autoridad debe de ceñirse, de modo estricto, a la recopilación y utilización de aquellos datos que resulten imprescindibles para lograr los fines perseguidos. De esta manera, se consigue reducir el riesgo de afección sobre aquella de la privacidad superflua para la investigación del delito. Se trata, por tanto, de una limitación que afecta a la actividad que desarrolla la autoridad judicial, tanto a nivel cuantitativo como cualitativo.

La primera regla que deben cumplir los datos personales que se utilicen para un tratamiento de datos por mor de este principio básico del derecho a la autodeterminación informativa son las de adecuación y pertinencia. Elementos que implican en primer lugar que los datos deben ser apropiados para el tratamiento[35] y además tener cierta relevancia para el alcance del fin perseguido respectivamente.

En segundo lugar, este principio conculca que los datos personales que se traten deben de limitarse a aquellos estrictamente necesarios en

33. Idéntica conclusión alcanzan LÓPEZ JIMÉNEZ, R., "Régimen jurídico de los datos personales obtenidos en los descubrimientos casuales durante la investigación de los delitos" en COLOMER HERNÁNDEZ, I. (Dir.) *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*, Aranzadi, Cizur Menor, 2017, pp. 315-343 y AZAÚSTRE RUÍZ, P., "Acercamiento al régimen jurídico-procesal previsto para la utilización de la información obtenida en un proceso penal distinto"…*op. cit.*, pp. 345-366.

34. Señala TRONCOSO REIGADA que mediante este principio se consigue frenar el conocimiento excesivo sobre el interesado que es posible conseguir mediante el tratamiento de sus datos, ya sea directamente o bien a través de técnicas avanzadas. *Vid.* TRONCOSO REIGADA, A. "El principio de calidad de los datos"…*op. cit.*, p. 345.

35. El concepto de adecuación se refiere a la eficacia del dato para conseguir la finalidad fijada del tratamiento, es decir, un dato será adecuado, cuando sea estrictamente necesario. Los datos serán pertinentes, cuando su recolección se encuentre plenamente justificada, en función de la naturaleza y la finalidad que se persigue por el tratamiento. *Vid*. PUYOL MONTERO, J. "Los principios del derecho a la protección de datos", en PIÑAR MAÑAS J. L. (Dir.), *Reglamento general de protección de datos: hacia* un *nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, 2016, p. 135.

relación a los fines para los que son tratados. Vemos como por razón de la aplicación de estas máximas, los datos personales a tratar resultan restringidos fundamentalmente por la estricta necesidad que marquen los fines perseguidos por el responsable del tratamiento, sin que sea posible exigir datos innecesarios o prescindibles, que no aporten ninguna utilidad para alcanzar los fines del tratamiento o que puedan ser sustituidos por otros menos invasivos. Por tanto, de no ser necesarios todo o parte de los datos personales, debe evitarse su tratamiento, tal y como reseña el Considerando 26 de la Directiva 2016/680.

Las implicaciones procesales de este principio son notorias, especialmente durante la fase de instrucción y la adopción de medidas limitativas de derechos orientadas a la recopilación de datos en soporte papel o digital. Véase como el cumplimiento de este principio va a exigir, que en la medida de lo posible, el órgano judicial que pretenda obtener datos personales necesarios, delimite y acote cuantitativa y cualitativamente, en la medida de lo posible, siquiera relativamente o en base a ciertos criterios, la información cuya obtención se requiere. Esta concreción deberá de definirse necesariamente en la resolución judicial que acuerde la medida de investigación consistente en la aprehensión o recogida de datos. Requiere por tanto, una especial diligencia del órgano judicial, e incluso una labor proactiva en favor de los derechos fundamentales del interesado que pueden verse injeridos por la medida a adoptar.

Más complejo resulta el estricto cumplimiento de dicho principio en los supuestos en los que se lleva a cabo una medida limitativa de derechos sobre soportes y dispositivos que almacenen o conserven importantes cantidades de información y datos de carácter personal, que impidan filtrar y discriminar, durante el propio registro inicial, los que presentan relevancia para el proceso. En estos supuestos, sería imprescindible articular en la Ley de Enjuiciamiento Criminal un procedimiento posterior al registro, con intervención de las partes implicadas, dirigida a determinar la información que debe ser objeto de expurgo por no resultar pertinente ni útil para la investigación. De este modo se conseguiría un mayor respeto al principio de adecuación y se evitaría, la acumulación gratuita de datos en manos de las autoridades con la tentación de utilización para otros fines distintos.

4. PRINCIPIO DE LIMITACIÓN DEL PLAZO DE CONSERVACIÓN

En virtud de dicho principio, la autoridad judicial responsable del tratamiento debe de limitar de manera general el plazo de conservación de los datos personales mantenidos en los ficheros por el plazo imprescindible para el cumplimiento de la finalidad para la que fueron recogidos.

Consecuentemente, una vez que los datos dejen de ser útiles para los fines perseguidos, debe de procederse a su borrado definitivo, evitando de este modo prolongar su uso o facilitar su destino a otros fines[36]. Para conseguir tal objetivo, se exige que la autoridad competente establezca de antemano los plazos previstos o previsibles para su supresión, de acuerdo a los criterios adecuados para ello. No obstante, dada la incertidumbre temporal que acontece con la duración de un proceso y sus diferentes modos de resolución, lo cierto es que no es posible predefinir dichos plazos de modo absoluto, operando los plazos relativos definidos en el art. 588 *bis* k) LECrim. En cualquier caso, es necesario enfatizar en la necesariedad de que al término de los plazos, el órgano judicial adopte las medidas necesarias para que se proceda a la correcta destrucción de los datos y de todas las copias que pudieran conservarse en manos de la Policía Judicial cuando hubieren intervenido en su obtención.

5. PRINCIPIO DE PROACTIVIDAD O RESPONSABILIDAD ACTIVA

Como colofón a los principios rectores vinculados al tratamiento de datos, el legislador europeo ha introducido *ex novo* al principio responsabilidad activa o proactividad[37], que se recoge en los arts. 4.4 Directiva 2016/680/UE. Dicho principio puede, además, considerarse como una de las grandes novedades en la materia, por provocar un giro copernicano en cuanto al sistema de responsabilidad al que se sujetan las autoridades intervinientes en el tratamiento. Éste se proclama bajo la siguiente consigna: *"El responsable del tratamiento deberá garantizar y estar en condiciones de demostrar el cumplimiento de lo establecido en este artículo"*.

El principio de responsabilidad proactiva determina que la responsabilidad del cumplimiento de las distintas obligaciones y garantías

36. *"La conservación de datos personales con una determinada finalidad despierta el deseo de hacer uso de dichos datos con otros fines"*. Con esta reveladora sentencia dio inicio el escrito de conclusiones de la Abogada General del TJUE de fecha 18 de julio de 2007 relativas a la cuestión prejudicial planteada por el Juzgado Mercantil núm. 5 de Madrid en el caso Promusicae contra Telefónica de España S.A.U. (C-275/06), y en la que se pone de relieve los riesgos que se crean de la mera acumulación de datos de interesados.

37. Los términos de responsabilidad activa o proactividad –tal y como ha sido señalado mayoritariamente por la doctrina– han sido los vocablos utilizados para la traposición al castellano del término anglosajón *accountability*, que es el concepto al que alude el legislador europeo para definir a tal principio. Véase ALBERTO GONZÁLEZ, P., "Responsabilidad proactiva en los tratamientos masivos de datos" en *Dilemata*, núm. 24, 2017, p. 120 y MARTÍNEZ MARTÍNEZ, R. "Diligencia y responsabilidad en protección de datos: la llamada accountability" en *El Derecho*, 2019. Éste último autor considera que los vocablos por los que se ha trasladado el término accountability al castellano no acaban de reflejar la riqueza material de este concepto anglosajón.

establecidas en el marco jurídico vigente del derecho a la protección de datos, con especial atención de los principios vertebradores del sistema, recae en último término en la autoridad competente[38]. Por tanto, los órganos judiciales, en tanto autoridad, deben no solamente cumplir diligentemente con los principios y obligaciones dispuestos en la normativa, sino que, además, deben de ser capaces de demostrarlo al propio interesado, a la autoridad de control o incluso a las instancias superiores que pudieran conocer de recursos planteados frente a cuestiones que afectaren a la obtención y posterior tratamiento de datos. O, dicho en otros términos, la autoridad competente, en tanto organiza y gestiona el sistema de protección de datos se encuentra sujeto a la condición inexcusable de cumplir férrea y escrupulosamente todos los principios y obligaciones esenciales de la materia con el fin de respetar los derechos y libertades del interesado, debiendo estar en disposición de poder acreditar fehacientemente tal cumplimiento[39], máxime ostentando el juez la posición de garante de sus derechos.

6. EL AUTO MOTIVADO: RESOLUCIÓN IMPRESCINDIBLE PARA LA OBTENCIÓN DE DATOS

De acuerdo con lo establecido en el art. 141 LECrim, las resoluciones que adopten forma de auto serán siempre fundadas, contendrán en párrafos separados y numerados los antecedentes de hecho y los fundamentos de derecho y, por último, la parte dispositiva, debiendo ser firmados por el juez o magistrado. Prosigue el precepto preceptuando que revestirán forma de auto las resoluciones del juez, que entre otros aspectos, decidan sobre *"la admisión o denegación de prueba (…) o afecten a un derecho fundamental…"*. Por su parte, el art. 588 *bis* c) LECrim exige que las medidas

38. BAJO ALBARRACÍN, J. C. "Consideraciones sobre el principio de responsabilidad proactiva y diligencia (accountability). Experiencias desde el Compliance" en LÓPEZ CALVO, J. (Coord.) *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Wolters Kluwer, Las Rozas de Madrid, 2019, p. 975.

39. El Considerando (50) Directiva 2016/680/UE describe a la perfección las implicaciones esenciales de este principio para el responsable, tal que así "Se debe establecer la responsabilidad del responsable del tratamiento en relación con cualquier tratamiento de datos personales realizado por él mismo o en su nombre. En particular, el responsable del tratamiento debe estar obligado a poner en marcha medidas oportunas y eficaces y a poder demostrar la conformidad de las actividades de tratamiento con la presente Directiva. Estas medidas deben tener en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo que representan para los derechos y las libertades de las personas físicas. Las medidas adoptadas por el responsable del tratamiento deben incluir la formulación y puesta en marcha de salvaguardias específicas en relación con el tratamiento de los datos personales de personas físicas vulnerables, en particular los niños".

de investigación tecnológica sean adoptadas por el juez de instrucción durante dicha fase se acordarán mediante auto motivado, una vez oído el Ministerio Fiscal.

Cuando en la práctica forense debe adoptarse una medida de investigación tecnológica –o incluso una tradicional no tecnológica– de las expresamente reguladas en Ley de Enjuiciamiento Criminal, no hay dudas sobre la necesariedad de que se recoja en un auto motivado de acuerdo con los preceptos anteriormente citados y que haga mención al contenido mínimo exigible en el art. 588 bis c) LECrim. Sin embargo, no es infrecuente que todavía, cuando se pretenden obtener datos personales como medio de investigación o fuente de prueba a través de un requerimiento efectuado a un tercero o una de las partes del proceso, se continue utilizando la providencia –recordemos que es una resolución inmotivada– como modalidad escogida de resolución habilitante o mediante auto carente de motivación o insuficiente.

Habiendo constatado a lo largo de este trabajo que de acuerdo con la jurisprudencia europea toda recopilación de datos personales constituye por sí misma una injerencia en el derecho fundamental a la protección de datos, con independencia del uso que posteriormente se efectúe de los mismos y de su propia naturaleza, no cabe duda de que el auto debe ser la resolución que debe adoptarse para su obtención en cualquier caso– ya sea mediante requerimiento o a través de una medida limitativa de derechos–, lo que nos lleva a descartar a la providencia como resolución apta para tal finalidad. Y es que como tiene establecido la doctrina constitucional acerca de los requisitos necesarios para la adopción de una medida restrictiva de derechos fundamentales, ésta debe de estar *"prevista por la Ley, [debe ser] adoptada mediante resolución judicial especialmente motivada, y que sea idónea, necesaria y proporcionada en relación con un fin constitucionalmente legítimo"*. Resolución que además deberá exponer las razones que justifiquen la adopción de la medida y la posible contribución a la investigación o enjuiciamiento[40].

Pero amén de los anteriores puntos, debemos hacer énfasis en la necesidad de que cuando se pretenda obtener datos de carácter personal, el juez deberá de justificar y motivar de modo suficiente e independiente la adecuación de la medida a los principios rectores del derecho a la protección de datos que puedan verse implicados. De este modo, será imprescindible hacer mención a la base legitimadora del tratamiento de los

40. MORENO CATENA, V., *Derecho Procesal Penal*, Colex, Madrid, 1997, p. 266 y SSTEDH de 25 marzo 1998, *Kopp*, de 30 julio 1998. En el plano constitucional son relevantes las SSTC 299/2000, 236, 171, 166, 141 y 49/1999, 229 y 58/1998.

datos, en función de su naturaleza y tipología; se deberá especificar los fines concretos a los que los datos se destinan, es decir al delito o delitos objeto de investigación; y se deberán de delimitar del modo más estrecho posible los datos o categorías de datos que deben ser objeto de entrega o aprehensión, ponderando la imposibilidad de obtener dicha información a través de otros medios distintos menos lesivos para la privacidad. La insuficiencia de dicha motivación, podrá servir de base indiscutiblemente para impugnar la resolución judicial habilitante, hasta el punto de conseguir su ineficacia procesal y la imposibilidad de utilización de los datos obtenidos.

V. EL DEBER DE INFORMACIÓN

Los arts. 12 y 13 de la Directiva 2016/680 imponen a la autoridad judicial responsable del tratamiento que procese datos de carácter personal en el ejercicio de sus competencias, la obligación de cumplir con el deber de información con los interesados cuya información se vea afectada en el curso de una investigación o proceso penal. Y ello con independencia de la posición que ocupe el titular en el proceso, o incluso de que sus datos se utilicen de forma accidental, como sucede en el caso de que los datos pertenezcan a un tercero que se ve afectado por una medida restrictiva de derechos sin tener la condición de investigado.

La información que debe prestarse, relacionada en el segundo de los preceptos citados[41], se refiere principalmente a los principales parámetros que caracterizarán las operaciones de tratamiento que se van a desarrollar y a las facultades y derechos que asisten al interesado respecto al uso. Se trata, en definitiva, del derecho del interesado a recibir una síntesis de los elementos esenciales que configuran el tratamiento al que se van a someter sus datos personales, con el objeto de que pueda tomar consciencia

41. En particular, la autoridad judicial está obligada a poner en disposición del interesado, al menos, la siguiente información: *"a) La identificación del responsable del tratamiento y sus datos de contacto. b) Los datos de contacto del delegado de protección de datos, en su caso. c) Los fines del tratamiento a los que se destinen los datos personales. d) El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma. e) El derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, supresión o la limitación de su tratamiento"*. Y además, atendiendo a las circunstancias del caso concreto, deberá de trasladar asimismo los siguientes datos: *"a) La base jurídica del tratamiento. b) El plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo. c) Las categorías de destinatarios de los datos personales, cuando corresponda, en particular, los establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales. d) Cualquier otra información necesaria, en especial, cuando los datos personales se hayan recogido sin conocimiento del interesado"*.

del tratamiento y verificar *ab initio* y durante todo el periodo en que se prolongue éste, la adecuación y mantenimiento de éste a los principios y garantías establecidos en la legislación, y a la par, asistirle en el ejercicio de las eventuales acciones y facultades que le corresponden como titular de los datos en aras de garantizar el cumplimiento de la legislación. Nos encontramos ante un derecho cuya función principal es asegurar la plenitud de las facultades de control y disposición inherentes al derecho a la protección de datos de carácter personal, pues como concluyera al respecto la STC 292/2000, de 30 de noviembre, en su Fundamento de Derecho 6.º, *"el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado (…). Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin"*. Debe advertirse que este derecho posee un contenido y fines distintos a los derechos informativos estrictamente procesales que derivan de la Directiva 2012/13/UE del Parlamento Europeo y del Consejo, de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales.

Por tanto, nos situamos ante una obligación de la autoridad que adquiere especial relevancia en la materia junto al elenco de derechos ARCO, tal y como ha confirmado el TJUE, habida cuenta de que es el medio que permite a los interesados tener constancia de que sus datos han sido recopilados y son tratados por un órgano judicial concreto, a efectos de poder ejercitar cualquiera de las facultades reconocidas en le legislación sectorial, reclamar la tutela de la autoridad de control o plantear los recursos que procedan para impugnar el tratamiento[42].

Si bien dicha información debe proporcionarse a la mayor brevedad tras la recogida de los datos, lo cierto es que en ciertos supuestos es posible retrasar el cumplimiento de dicho deber, aunque no anularlo. En concreto cuando su prestación pueda obstaculizar, comprometer o perjudicar una investigación o enjuiciamiento penal en curso o poner en riesgo la seguridad nacional o los derechos y libertades fundamentales de un tercero. No obstante, el uso de dichas causas debe estar plenamente justificada y una vez desaparecida el órgano judicial deberá de comunicar al interesado la información exigida[43].

42. Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2020, *La Quadrature du Net*, C-511/18, C-512/18 y C-520/18, apartados 190-192.

43. Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, apartados 222-224.

VI. CONCLUSIONES

Tal y como hemos podido comprobar a lo largo del presente trabajo, el derecho a la protección de datos es un instituto protector de los demás derechos del ordenamiento jurídico que pueden verse en riesgo por razón del uso de datos personales, que ha adquirido una relevancia inusitada en esta época caracterizada por la digitalización de la sociedad y la penetración de las tecnologías de la información y comunicación en todas las facetas de nuestra vida cotidiana. No obstante, a la par, los datos personales objeto de protección por dicho derecho, se erigen en elementos indispensables del proceso penal, que se incorporan a este como medios de investigación o fuentes de prueba especialmente fructíferos para el esclarecimiento de los delitos en general y particularmente los que presentan un componente informático o telemático.

Hasta recientes fechas y por lo general, cuando las autoridades judiciales tenían que recurrir a la obtención de datos, no proporcionaban un tratamiento que tuviera en cuenta las garantías y limitaciones dimanantes del derecho fundamental a la protección de datos para los interesados, pese a tener plena vigencia. Podría decirse que primaba el interés público en el uso de los datos para el esclarecimiento de los hechos delictivos. Ello desde luego ha supuesto que durante un largo espacio de tiempo ha existido un escenario judicial en el que las injerencias e intromisiones excesivas, injustificadas o inmotivadas en la esfera de la privacidad han sido una constante.

No obstante, este panorama ha venido a solventarse de la mano del paquete legislativo en materia de protección de datos aprobado en el seno de la Unión Europea en el año 2016. A través del mismo se ha incorporado al ordenamiento europeo una Directiva específica, con la que se pretende extender las garantías tradicionalmente vinculadas a este derecho, aunque con ciertas modulaciones, al tratamiento acometido por las autoridades del sistema de justicia penal con fines de investigación y persecución del delito. Si bien, compaginando dicho objetivo con el de creación de un contexto en el que se facilite el intercambio y circulación de datos entre las autoridades nacionales y de los Estados miembros.

La Directiva 2016/680 prevé una extensa y compleja regulación en la que se incorporan expresamente todo un elenco de novísimos principios, condiciones y límites de obligada observancia por las autoridades responsables, así como toda una serie de derechos en favor de los interesados con el objeto de establecer un equilibrio entre el interés del Estado en reprimir el delito y los derechos fundamentales de los ciudadanos.

La vigencia y efectividad de dichos principios y reglas, va a suponer un cambio sustancial en las arraigadas prácticas judiciales, toda vez que

como hemos desarrollado a lo largo del trabajo, van a implicar que cualquier actuación orientada a la obtención de datos, va a requerir, entre otros puntos, la verificación de la legitimidad de la obtención, de la finalidad el uso y de la adecuación y pertinencia de los datos a los fines perseguidos. Examen judicial que desde luego deberá exteriorizarse a través de las oportunas resoluciones judiciales habilitantes, al igual que cualquier otra actuación que pudiera surgir incidentalmente respecto a los datos.

Desde luego, la aplicación de la normativa en su integridad, va a suponer en toda regla un cambio de cosmovisión y de cultura en lo que respecta al tratamiento de datos que tiene lugar en el seno del proceso penal. La observancia y respeto general a esta nueva norma, requerirá de cierto tiempo de adaptación y de concienciación de todos los operadores jurídicos, si bien, en buena medida, dependerá de la labor formativa que el Consejo General del Poder Judicial efectúe entre jueces y magistrados en su calidad de autoridad de control.

II
Inteligencia Artificial y Justicia Penal

Capítulo 4

Algoritmización de la prueba y la decisión judicial en el proceso penal: ¿utopía o distopía?

Prof. Dra. H.c. mult. Silvia Barona Vilar

Catedrática de Derecho Procesal
Universitat de València

I. SIMBIOSIS JUSTICIA Y SOCIEDAD. ENTENDIMIENTO DE LA SOCIEDAD ACTUAL DIGITAL Y ALGORÍTMICA

A lo largo de la Historia hemos asistido a constantes cambios, transformaciones, fruto de una evolución propia de la Humanidad que la ha conformado. Los hábitos, las ideas, el poder físico, la agricultura, las enfermedades, la climatología, y un sinfín de elementos han incidido en la evolución del ser humano, en su manera de comportarse y en su modo de agruparse, de defenderse, de desarrollarse. En ese hábitat llamado Humanidad han habido a lo largo de la Historia distintos modelos de convivencia, siendo necesaria la integración, cada vez más palmaria, en grupos, comunidades, tribus, etc., que ofrecían ventajas a quienes los integraban, a cambio de respeto y lealtad al grupo. De este modo, a medida que se fueron estructurando estas pseudosociedades primitivas, asentándose y generando una fórmula muy primitiva de derecho a la tierra, al espacio, al uso de las aguas, a la caza, a la siembra o a la recolección, surgieron paulatinamente las necesidades de conformar reglas para el uso, disfrute, reparto, beneficios, y para evitar los abusos entre ellos, para garantizar, en suma, una suerte de seguridad *ad intra* y *ad extra.* Esos primeros estadios de la humanidad organizada vinieron representados esencialmente por la influencia ejercida por las tradiciones y, paulatinamente, evolucionando hasta una suerte de *Derecho*, primitivo y no conformado formalmente, hasta el asentamiento de las denominadas sociedades primitivas, esto es,

Mesopotamia, India y Egipto, amén de las denominadas civilizaciones clásicas posteriores, y muy especialmente Grecia y Roma.

Así, se fue progresivamente dando paso, desde las tradiciones y costumbres, a las normativas de obligado cumplimiento, aprobándose códigos, en los que se establecían reglas de actuación para la guerra, el trabajo, los ceremoniales, etc.. Es el momento en la historia de la humanidad en el que se gesta una suerte de derecho escrito, primitivo, pero regulador de las conductas, conformando una serie de reglas que hicieran más sencilla la vida pacífica entre los pueblos, favoreciendo acuerdos, estructuras e instituciones[1]. Es el periodo que los historiadores del derecho denominan como "ordenamientos jurídicos no formulados", en los que existe una suerte de conciencia o convicción común que todos comparten sin necesidad de que se haya predefinido previamente, coincidiendo en una apreciación conjunta de lo que es justo e injusto, lo que puede hacerse y lo que no, por ser ilícito[2].

Esa conformación u orden jurídico inicial ha venido, de forma cíclica y siempre asimétrica, desarrollándose a medida que las coordenadas sociales, culturales, económicas, políticas, sociológicas y tecnológicas han ido cambiando. El modelo jurídico se conforma para favorecer la convivencia pacífica social y ofrece las respuestas ante la quiebra de esa paz social, configurando un sistema de Justicia, con principios, estructuras e instituciones. La imbricación de la Justicia con el modelo social es innegable, de manera que el Derecho y la Justicia se adaptan y evolucionan a la par que la sociedad misma. Las transformaciones sociales han venido propulsando los cambios jurídicos y por supuesto en los instrumentos, protagonistas y principios de la Justicia. En suma, la conformación de la Justicia a lo largo de los siglos ha venido en gran medida anudada a los valores de la sociedad del momento. Caminando por la historia de la Humanidad se halla una enorme riqueza sobre las evolutivas coordenadas que mueven la sociedad y la vida de las personas; unas coordenadas que provocan un movimiento cíclico y asimétrico, con un permanente estado de mudanza que camina pausadamente o que se altera volcánicamente por elementos exógenos que insuflan una suerte de metamorfosis societaria[3]. De este modo, en consecuencia, la historia de la Justicia va a estar intrínsecamente vinculada a esa evolución de la sociedad.

1. BARONA VILAR, S., *Proceso penal desde la Historia. Desde su origen hasta la sociedad global del miedo*, Valencia, Tirant lo Blanch, 2017, pp. 27-28.
2. GARCÍA GALLO, A., *Manual de Historia del derecho español. El origen y la evolución del Derecho,* Madrid, 10 ed., 1984, p. 180.
3. BARONA VILAR, S., "La digitalización y la algoritmización, claves del nuevo paradigma de justicia eficiente y sostenible", en COLOMER HERNÁNDEZ, I., *Uso de la información y de los datos personales en los procesos: los cambios en la era digital*, Pamplona, Aranzadi, 2022, pp. 75-76.

Si la sociedad y la justicia son dos componentes intrínsecamente anudados, el entendimiento de la Justicia deberá efectuarse en el contexto histórico, social, económico, político, cultural, etc.. De este modo, la Justicia del Siglo XXI se muestra como un retrato estereotipado de lo que es la sociedad digital, innovativa y disruptiva actual, asentada en la tecnología y muy específicamente en sus valores, eficacia y eficiencia, inmediatez, más por menos, internacionalización, sostenibilidad, transparencia, etc. La tecnología se ha convertido en la imprescindible compañera de viaje de la sociedad, mudando nuestro paisaje esféricamente, y propulsando la transformación del exhausto modelo revolucionario de contrato social –que ha servido durante tanto tiempo para conformar no solo el modelo de sociedad, sino, muy especialmente, el modelo de Estado– en un contrato social algorítmico. ¿Mejor o peor? Podríamos responder con una frase de Charles Dickens: "Era el mejor de los tiempos y era el peor de los tiempos, la edad de la sabiduría y también de la locura" (en su obras *Historia de dos ciudades*), muy apropiada si se trata de dar una respuesta a la pregunta formulada.

El desarrollo de la tecnología encontró un momento esencial en la denominada revolución 3.0. (década de los sesenta del siglo pasado), que permitió iniciar los primeros pasos de la digitalización, con especial énfasis en el uso de la computación y las tecnologías digitales para transformar la comunicación. Uno de sus ejes fue el internet, que se convirtió en una especie de "bien global" de la sociedad, un instrumento que se presentaba como esencial para garantizar una sociedad acomodada, eficiente y ágil. Con este punto de partida se iba produciendo paulatinamente un cambio en la organización y gestión profesional, científica, económica, productiva, etc., emergiendo igualmente nuevas fuentes de energía, que también comenzaron a alcanzar al mundo jurídico y, muy especialmente, a la investigación criminal, que se fue sirviendo de estos avances[4], pero no solo, dado que permitió ir desarrollando el denominado derecho electrónico, en el que se ubica la notaría electrónica, el registro electrónico, los expedientes administrativos electrónicos, y la aparición de la *eJustice*, con la consolidación instrumental del internet y el *hardware* en el mundo jurídico, lo que impregna de celeridad y eficiencia los sistemas jurídicos.

Este primer escalón no solo implicaba una atribución de mejora instrumental del derecho, sino que, a la vez, se presentaba como una fórmula mágica para sanar la patología social que venía presentándose desde el siglo XIX por la sociedad moderna, lo que Max Weber denominó como el

4. BARONA VILAR, S., *Algoritmización del Derecho y de la justicia. De la Inteligencia Artificial a la Smart Justice,* Valencia, Tirant lo Blanch, 2021, pp. 55-56.

desencanto (*die Entzauberung*)[5]; un desencanto generado por la pérdida de referentes místicos y religiosos que habían colmado tuitivamente a las sociedades predecesoras y cuya desaparición generaba un enorme vacío existencial. Si bien la modernidad aportó laicidad, pensamiento racional y científico, abandonando las cadenas del pasado, enfrentaba empero a la Humanidad al sentimiento de saberse libre y, lo más difícil, de ejercitar esa libertad, lo que resultaba paradójicamente complejo y doliente. Es esa sensación de sentirse "a la intemperie" lo que propiciaría en el Siglo XX la crisis de la modernidad, sobre la que tan brillantemente disertaron los integrantes de la Escuela de Frankfurt. Explicaron ese vacío existencial humano y social, el nihilismo que provocó la aparición –favorecida por la globalización[6]–, de la búsqueda de la uniformidad, de la masa[7], así como la necesidad de búsqueda en otro ámbito ilusión, magia, fantasía, y hasta en ocasiones superchería y conspiranoia (se ha visibilizado en el periodo de pandemia). Ese retrato de sociedad en movimiento, en completo estado de mudanza[8], favorece la sociedad de consumo, el pensamiento acrítico, bajo control[9] y una liquidez[10] global de la vida, las sociedades, la cultura, la educación y en cierta medida también de la Justicia. Esos vacíos existenciales y esa tristeza, desencanto y desasosiego, la hemos alimentado de tecnología, una pócima que permite sanar la melancolía, las falencias humanas y sociales de la masa (Byung-Chul Han lo denomina el *enjambre digital*[11]). Una pócima fomentada desde las últimas décadas del siglo pasado a través de las políticas neoliberales que permiten introducir una suerte de generalización de la calculabilidad y una sistematización de la política de indicadores, gracias a los datos contables, que tiene trascendencia en todos los ámbitos de la vida humana y social[12].

El imparable desarrollo de la computación, vinculando además los desarrollos de la tecnología con los avances científicos, especialmente desde finales del siglo XX, fueron generando una nueva etapa de industrialización, en la que se combinan digitalización, conectividad, automatización, robotización e inteligencia artificial. Surgió así la cuarta revolución industrial, o Industria 4.0. El origen del término Industria 4.0. se encuentra en un

5. WEBER, M., "Wissenschaft als Beruf" (1919), en WINCKELMANN, J., *Gesammelte Aufsätze zur Wissenschaftslehre*, J.C.B. Mohr, 7 ed., 1988, p. 594.
6. LEFEBRE, H., *Introducción a la modernidad*, Madrid, Tecnos, 1971.
7. LIPOVETSKY, G., *L'ere du vide– Essais sur l'individualisme contemporain*. 1989.
8. BARONA VILAR, S., "Una justicia 'digital' y 'algorítmica' para una sociedad en estado de mudanza", en la obra colectiva BARONA VILAR, S., *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, Valencia, Tirant lo Blanch, 2021, pp. 21 a 64.
9. GABRIEL, M., *El sentido del pensamiento*, Barcelona, Pasado&Presente, 2 ed., 2020.
10. BAUMAN, Z., *Vida líquida,* Barcelona, Ed. Paidós, 2013, p. 109.
11. HAN, B-CH., *En el enjambre,* Barcelona, Ed. Herder, 2020, p. 26.
12. CARDON, D., *Con qué sueñan los algoritmos: Nuestras vidas en el tiempo del Big Data*, Dado ediciones, 2018, p. 15.

proyecto de estrategias de alta tecnología realizado por el gobierno alemán, cuyo objetivo era la creación de la fábrica inteligente o también conocida como Ciberfábrica, caracterizada por la gran interconexión entre máquinas automatizadas, la concurrencias de redes de comunicaciones, la integración de tecnologías avanzadas de procesamiento de datos, la robótica avanzada, la capacidad de autodiagnóstico de situaciones, el mejor intercambio de información y una mayor eficiencia en la gestión de recursos naturales y humanos[13]. En sus inicios, hubo voces contrarias a su consideración como nueva revolución, manifestando que no era sino la evolución de la tercera revolución. Frente a este idea, SCHWAB consideraba que se trataba de un nuevo paso, más allá de la revolución 3.0. por: la velocidad con la que camina, presentando un mundo interconectado, con una tecnología nueva mucho más poderosa; la amplitud y profundidad con la que ha irrumpido, que incide, allende los negocios y la economía, en la sociedad y en las personas; y, en tercer lugar, produce un impacto transfronterizo sin delimitación territorial[14]. Una nueva etapa que trae consigo innovaciones científicas y tecnológicas que inciden no solo en la digitalización de las cadenas industriales de producción, sino también en la aparición del internet de las cosas, el big data, y otros más, que han mutado la sociedad analógica hacia un mundo digital, innovativo y disruptivo. Técnica, tecnología, ciencia, neurociencia, ética y derechos se van poco a poco integrando para presentar un entorno adecuado en un escenario preparado para el 4.0.: la globalización, la sociedad de masas y la sociedad de consumo, bajo el paraguas neoliberal[15].

En sus orígenes el 4.0. respondía a una necesidad de implementar un *modus operandi* empresarial revolucionario, arrolladoramente eficiente. De ahí que se hablara de ciberindustria, *smart factory, smart industry*, aun cuando poco a poco fue expandiéndose imparablemente a todos los sectores y ámbitos de la vida, convirtiéndose en una suerte de *modus vivendi*, transportando maneras de actuar del *homo economicus* a la cotidianeidad vital, pasando de lo que Norbert WIENER *Mensch* al *Menschmaschine*[16], y emergiendo un nuevo fenotipo denominado *Homo digitalis*[17], de modo que efectivamente, como apunta Byung-Chul HAN, el hombre digital digita

13. Este término por vez primera empleado por Hennig KAGERMANN, Presidente de la Academia alemana de Ciencias e Ingeniería (Acatech), que vio la luz en la feria de Hannover de 2011. *Vid.*, FINSTERBUSCH, S., "Den digitalen Heckenschüzen auf der Spur", en *Frankfurter Allgemeine Zeitung*, 10 de marzo de 2014.
14. SCHWAB, K., *La cuarta revolución Industrial,* Barcelona, Ed. Debate, 4 ed., 2018, p. 15.
15. *Ad extensum,* BARONA VILAR, S., *Algoritmización del Derecho y de la justicia; cit.*, pp. 60-67.
16. WIENER, N., *Mensch und Menschmaschine*, Frankfurt, Alfred Metzner Verlag, 1952, 4.º ed., pp. 150-194.
17. MARTÍNEZ OJEDA, B., *Homo digitalis: etnografía de la cibercultura*, Bogotá, Universidad de los Andes, 2006; también puede verse LASALLE RUIZ, J. M., *Ciberleviatán.*

en el sentido de que cuenta y calcula constantemente[18]. Ese paso es no solo innovativo, sino esencialmente disruptivo, en valores, principios, protagonistas, instrumentos, estructuras, etc.. que permiten la hiperconectividad. Esa hiperconectividad es fruto de la donación constante de nuestros datos; pagamos con datos, que son el gran negocio, el petróleo, el carburante de toda la máquina digital del siglo XXI[19].

Y todo ello tienen una enorme incidencia en el mundo jurídico, tanto respecto de la aparición de numerosas normas reguladoras, nacionales y supranacionales, de nuevos sectores que vienen a conformar criterios de actuación, conceptos jurídicos nuevos, etc., tratando de conformar un marco jurídico adecuado y protector, como respecto de la emergencia de infinitas manifestaciones de esta nueva era con repercusiones jurídicas: la protección de datos, el derecho al olvido, la regulación de las cookies, el marketing relacional, el régimen legal de las aplicaciones o herramientas algorítmicas y su capacidad de incidir en las decisiones públicas, la economía tecnológica colaborativa, el ciberespacio, la cibercriminalidad, la ciberseguridad, la protección de los derechos fundamentales en internet, la *eJustice,* las nuevas técnicas de investigación criminal tecnológicamente avanzadas, la incidencia del *Big Data,* la regulación de internet con especial referencia a la protección de los menores por internet, etc.

En suma, la digitalización y la incorporación de herramientas algorítmicas en la sociedad han propiciado un nuevo estilo de vida, en el que el solucionismo tecnológico[20] ofrece la pócima de la felicidad, nos presenta un mundo paralelo al presencial, en el que caminamos inexorablemente hacia una vida híbrida, una integración de la Humanidad y la Tecnología, que destella con una luz que embarga y se expande a todos los ámbitos, a todas las áreas, un verdadero estilo de vida que nos lleva a considerar ese nuevo "contrato social algorítmico" para la *terra digitalis.*

II. LA JUSTICIA EN LA *TERRA DIGITALIS:* ¿UN ECOSISTEMA DE JUSTICIA MAQUÍNICA INTELIGENTE?

En el mundo de la Justicia el paisaje ha ido cambiando, del mismo modo que lo ha hecho la sociedad en general. Desaparecen fronteras

El colapso de la democracia liberal frente a la revolución digital, Barcelona, Ed. Arpa, 2019, p. 42.

18. HAN, B-CH., *En el enjambre, cit.*, p. 60.
19. BARONA VILAR, S., *Algoritmización del Derecho y de la justicia, cit.*, p. 70.
20. MOROZOV. E., *La locura del solucionismo tecnológico,* Madrid, Katx Editores, 2015.

físicas, el hábitat analógico quedó catapultado y se expande una nueva manera de concebir el mundo, las relaciones jurídicas, y también la justicia en general y el *modus operandi* en especial. Curiosamente, las utopías imaginativas que mostraban obras como la de "1984" de George Orwell, que se basó en la obra *Nosotros* publicada en 1921 por Yevgueni Zamiatin, o la de "El informe de la minoría" de Philip K. Dick, que dio lugar a la famosa película de Steven Spielberg en 2002 "*Minority Report*", entre otras, en las que se reflejaba una sociedad bajo el control tecnológico, no resultan ajenas ni meras ficciones en la realidad actual. Antes al contrario, referencias a las mismas se encuentran en prácticamente cuantos trabajos se realizan en torno a la aplicación de los sistemas digitales y sistemas inteligentes al mundo de la Justicia[21].

Se habla de internet, de la red, del espacio digital, de la irrupción de los sistemas inteligentes y de los avances de la inteligencia artificial. Irrumpieron, innovaron las relaciones personales, profesionales, comerciales, de consumo, públicas, y se instalaron en un escenario que presenta una vida digital indiscutible. Los efectos se están dando en todas las áreas y provocan una manera de actuar diversa, unas consecuencias de esa manera de actuar y una necesidad de adaptar la realidad jurídica a esas maneras innovativas también el mundo jurídico.

Por un lado, el *modus operandi* de los operadores jurídicos ha venido cambiando de forma exponencial, y más aun lo hará en los próximos años. La incorporación de los primeros sistemas de expertos anglosajones (*Expert Systems)* permitían actuar en determinados campos, convirtiéndose en asistentes inteligentes, modelos de computación lógica clásica que también se llevaron al mundo jurídico pero con éxito relativo, dado que ofrecían una suerte de razonamiento jurídico[22], pero presentaban inicialmente un defecto en el mundo jurídico: ausencia de argumentos que sostuvieran las respuestas. Paulatinamente se fueron mejorando las herramientas de argumentación jurídica, ofreciendo una función analítica e interpretativa, con argumentación de escritos, solicitudes o resoluciones. Estos sistemas de expertos han sido resultado de un aprendizaje estadístico, a través de la denominada *deep learning*.

En este orden de cosas, los impulsos que se vienen dando desde mitad de siglo pasado por extrapolar el modelo digital a la esfera jurídica son numerosos, si bien merece destacar la labor realizada por la Escuela

21. BARONA VILAR, S., *Algoritmización del Derecho y de la justicia, cit.*, p. 344.
22. KALINOWSKY, G., *Introducción a la lógica jurídica*, Buenos Aires, Ed. Eudeba, 1973, p. 67.

americana de Jurimetría[23], gracias a Norbert WIENER[24], padre de la Cibernética (1950), y su sucesor Lee LOEVINGER[25]. Trasladaron la jurimetría al mundo jurídico, aplicando herramientas predictivas con análisis del caso, magistrado, hecho, administración, abogado, etc.; un instrumento asistencial –no sustitutivo– que puede permitir gestionar tiempos, ahorrar recursos y ser más eficientes en la elaboración de la estrategia a seguir. No es infalible, empero se presenta como una suerte de evitación de lo ineficiente, al predecir soluciones jurídicas, eludiendo, por ello, trámites innecesarios o absurdos.

Por otro lado, la regulación jurídica general y el modelo de Justicia en particular están mutando, en la medida en que las fronteras geográficas delimitadoras de las capacidades legislativas de actuación no sirven en el mundo digital. Se hace necesario configurar una serie de principios éticos y jurídicos que permitan garantizar los derechos y las libertades también en el mundo etéreo del espacio digital. Es más, emergen nuevos conceptos jurídicos y algunos existentes deben ser objeto de replanteamiento para poder seguir integrados en un modelo jurídico innovativo. No solo los instrumentos han cambiado, los tiempos y las formas, sino también las consecuencias jurídicas. Han aparecido actuaciones en la red que antes no existían, y se ha ido generado un área (no-lugar o multi-lugar) que cada vez demanda más seguridad, el ciberespacio. Nuevos actores, nuevos delitos, nuevas consecuencias jurídicas y especialmente nuevas maneras de investigar y probar, propulsando en muchos casos una necesidad de transformación de las legislaciones nacionales para adaptar o crear el marco jurídico más adecuado a esa nueva ciberrealidad. Un nuevo paisaje favorece la *eJustice*, con infraestructuras, necesidades de planta judicial, tecnologías procedimentales, medidas digitales, agendas electrónicas, y un gran número de manifestaciones en el escenario innovativo y digital.

Los operadores jurídicos comienzan a encontrar soportes en el mundo digital que antes no tenían[26] (sistemas asistenciales para preparar demandas, querellas, para argumentar calificaciones de fiscalía, sistemas de predictibilidad a la hora de determinar la estrategia de defensa de los clientes, información sobre tribunales, magistrados, árbitros, grado de estimación o desestimación, asuntos anteriores, y un largo etcétera). El mercado

23. BOURCIER, D.; CASANOVAS, P., (ed.)., *Inteligencia Artificial y Derecho,* Barcelona, Ed. UOC, 2003, pp. 64-67.
24. WIENER, N., *The Human Use of Human Beings*, Torino, 1953.
25. LOEVINGER, L.; "JURIMETRICS –The Next Step Forward", *33 Minnesota Law Review*, 1949, pp. 456-493.
26. RUSSELL, S.& NORVIG, P., "Artificial Intelligence: A Modern Approach" http://aima.cs.berkeley.edu/contents.html.

nos ha inundado de software de argumentación jurídica, pero también de estrategias de negociación, mediación o conciliación. La manera de enfrentarse a un asunto es distinta y la información obtenida a través de estos sistemas programados ofrece un punto de partida bien diverso a aquel al que se enfrentaban los abogados hace veinte años. Y todo ello de forma mucho más célere, ofreciendo "*más por menos y en menos tiempo*", los grandes disvalores de la sociedad global, un atractivo lema neoliberal que difícilmente escapa de cuanto rodea al marco mundo de la Justicia.

Los soportes a los tribunales y a la policía también han cambiado. Especialmente en sede penal asistimos a una revolución actuacional, relacional y resolutiva. La manera de investigar ha cambiado; los instrumentos electrónicos han abierto un inmenso océano de predictibilidad, de prevención, de investigación y también de fundamento de la decisión judicial. Atrás quedó la investigación intuitiva de la policía; esa que veíamos en las obras de ficción con el comisario Montalvano, Brunetti, Poirot, Petros Márkaris, Cayetano Brulé, Carvalho, entre otros. Esa percepción personal intuitiva ha dejado paso al empleo de las tecnologías que ofrecen una investigación algoritmizada y con mayores dosis de fiabilidad.

En suma, también en este escenario digital asistimos a un modelo de Justicia al que ha alcanzado la disrupción innovativa. Nuevas relaciones, nuevas comunicaciones que se realizan en línea, un mundo digital en el que también las diferencias y la manera de afrontarlas, los hechos reprochables y los procesos para su reproche quedan influenciados por el escenario digital. Coordenadas bien diversas a la sociedad analógica que nos antecedió. Nada ni nadie escapa de esta era disruptiva digital, de la imparable algoritmización de la Justicia. Nuevos instrumentos digitales, software, hardware, sistemas de control, gestión, planificación, integración en la capacidad decisora y argumentativa, entre otros, se expande y avanzan a una velocidad inusitada, exigiendo respuestas jurídicas que no siempre llegan a tiempo. E incluso, la aparición y actuación, como "humanos", de las máquinas inteligentes, artefactos y robots requiere un replanteamiento jurídico en su conjunto, tanto para otorgarle capacidad, como para establecer el modelo de responsabilidad de los mismos[27].

En suma, asistimos a la conformación de un ecosistema de Justicia digital maquínico inteligente, que incide en la construcción de nuevas

27. *Vid.*, NEUHÄUSER, Ch., "Roboter und moralische Verantwortung", en HILGENDORF, E., *Robotik im Kontext von Recht und Moral*, en la colección "Robotik und Recht", Band 3, Baden-Baden, Nomos, 2014, p. 269. Este autor defiende la necesidad de desarrollar la responsabilidad del robot desde tres ámbitos: la responsabilidad individual, la responsabilidad colectiva y la política social.

categorías y respuestas jurídicas, que integra funciones hasta el momento exclusivamente humanas, que van dejando de serlo exclusivamente o incluso van siendo sustituidas por la máquina. Hemos asistido a una verdadera algoritmización de la vida, de la sociedad, del mundo y de la Justicia, algo que ha reflejado el filósofo INNENARITY al afirmar que "los algoritmos tienen una dimensión política en la medida que intervienen en el orden social y estructuran nuestras decisiones"[28]. Esa misión algorítmica está penetrando poco a poco en la toma de decisiones en el mundo de la justicia, ora de forma instrumental, asistencial o colaborativa, ora de forma disruptiva, sustituyendo la toma de decisiones de los operadores jurídicos por las máquinas. Esto ofrece un verdadero cambio de paradigma, aun cuando las herramientas algorítmicas y los sistemas que se emplean serán asimétricos y más o menos incisivos. Hay las que permiten análisis de textos, documentos, resoluciones, extrayendo información relevante, presentando respuestas; las que elaboran documentos escritos, redacción de contratos, propuestas de informes, etc., las que facilitan las tareas organizativas, las que realizan predicciones económico-financieras; hay plataformas (*On line Dispute Resolution Systems)*, las que asisten o complementan la función legislativa, hay abogados electrónicos o chatbots, hay sistemas que redactan reclamaciones, demandas, acusaciones, etc. Son todas ellas herramientas instrumentales, cierto, pero que penetran en la esencia de las funciones de los operadores de justicia.

III. MODELOS ALGORÍTMICOS PREDICTIVOS POLICIALES, MODELOS ALGORÍTMICOS EN LA INVESTIGACIÓN PENAL Y SISTEMAS BIOMÉTRICOS

En el contexto de proliferación de sistemas algorítmicos merece especial referencia aquellos que tienen fines predictivos de riesgos, empleados, cada vez con mayor asiduidad, como herramientas esenciales en la predicción y en la investigación delictiva. Estas herramientas han encontrado un terreno muy propicio en el marco político e ideológico del control y de la seguridad, favoreciendo cuantos instrumentos permiten obtener mucha información, controlar el entorno y adoptar de forma eficiente decisiones que permitan garantizar un modelo de prevención o, si cabe, de derecho penal *ex ante.* Esta coyuntura[29] es, por ende, la que ha favorecido la

28. INNENARITY, D., "Igualdad Algorítmica", en *El País Semanal,* 13 de mayo de 2022.
29. JUAN SÁNCHEZ, R., "Proceso penal preventivo en España: elementos y criterios de contención", en BARONA VILAR, S., *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*, Valencia, Tirant lo Blanch, 2019, p. 573.

penetración de la electrónica y la tecnología y con ella un camino fácil hacia la fascinante "Justicia predictiva", que realmente tiene poco de Justicia[30].

1. DE LA VIGILANCIA PREDICTIVA A LA JUSTICIA PREDICTIVA POLICIAL (*PREDICTIVE POLICING* O *PREDPOL*) Y EL CAMBIO DEL *MODUS OPERANDI* POLICIAL

El desarrollo de estos métodos predictivos y su proliferación dieron lugar a la aparición de la *predictive policing* o *PredPol*[31], "justicia predictiva policial", o vigilancia predictiva, propulsando la construcción de la denominada criminología ambiental[32] o criminometría. Con ella se ofrecen respuestas desde el uso de técnicas cuantitativas de análisis que permiten identificar objetivos que potencian la intervención policial, además de "prevenir delitos o resolver crímenes pasados mediante pronósticos estadísticos"[33].

Desde sus orígenes hasta la actualidad, las técnicas empleadas y la metodología han ido modulándose con el tiempo. Se ha ido perfeccionando tanto la alimentación de datos (ya no se busca mucho e indiscriminado, sino la calidad de los datos y, por ende, su selección y discriminación), como las técnicas analíticas que arrojan los resultados predictivos. En la actualidad se obtienen más datos, a través de la información policial, foros, webs, redes sociales u otros medios que pueda emplearse en el mundo digital, sin olvidar la gran información que puede obtenerse a través de las aplicaciones de los móviles[34]. Pero paralelamente se trabaja con la selección más restrictiva de los mismos. En su estudio podemos esencialmente establecer dos estadios diversos de desarrollo:

30. BARONA VILAR, S., "Una justicia 'digital' y 'algorítmica' para una sociedad en estado de mudanza", en BARONA VILAR, S., *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, *cit*., p. 38.
31. PERRY, W. L.; MCINNIS, B.; PRICE, C. C.; SMITH, S. C.; HOLLYWOOD, J. S., Predictive Policing. The role of crime forecasting in Law Enforcement operations, RAND Corporation, Santa Mónica, 2013, pp. 33-41.
32. MEDINA, J., *Políticas y estrategias de prevención del delito y seguridad ciudadana,* Madrid, Editorial Bdef, 2001; ECK, J. E.; WEISBURD, D., "Crime places in crime theory", *Crime and place, Crime Prevention Studies,* vol. 4, 1995, pp. 1-33; y WORTLE, R.; MAZEROLLE, L., *Enviromental Criminology and Crime Analysis*, Portland, 2008.
33. PERRY, W. L.; MCINNIS, B.; PRICE, C. C.; SMITH, S. C.; HOLLYWOOD, J. S, Predictive Policing. The role of crime forecasting in Law Enforcement operations, *cit*., pp. 33-41.
34. MIRÓ LLINARES, F., "Inteligencia Artificial y Justicia Penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología, 3,* Época n.º 20, 2018, pp. 98-99.

En primer lugar, en sus inicios estos análisis predictivos servían para favorecer la detección de los lugares identificados como de alto riesgo o *hot spots*[35], en los que invertir esfuerzos y medios para reducir la delincuencia y, con ello, garantizar la seguridad pública, realizando mapas digitales del delito (técnica del *mapping*), dirigiendo la implementación de más recursos personales y materiales en la lucha contra la misma[36]. Lo importante, como objetivo esencial de estas herramientas, era, por ende, predecir los lugares en los que existían riesgos de criminalidad; eran herramientas predictivas de localización de lugares donde previsiblemente podían cometerse hechos delictivos. En suma, herramientas predictivas de riesgos delictivos.

Inicialmente fue EEUU donde se desarrollaron los primeros softwares predictivos. En este sentido, el más conocido es el BIG DATA, una herramienta que se empleó en Chicago, conformada bajo los principios ecológicos defendidos por la Escuela de Chicago en la década de los años 20 del siglo pasado, centrada en la ecología del crimen, considerando, entre otros criterios a valorar, el entorno social, la temperatura ambiente, la meteorología[37]. No obstante, la incorporación de estas herramientas algorítmicas predictivas de riesgos delictivos en Europa, aunque algo más tardía, comenzó a desarrollarse.

El primer país fue Francia, en 1994, con *Anacrim*, una herramienta que se reemplazó en 2005 por *i2 Analyst Notebook* (i2AN), un programa predictivo de la Gendarmería Nacional francesa, que sustituyó a Anacrim. Dicho programa trabaja con datos policiales, privadas y gubernamentales, que fue implementado en el marco de un proyecto gubernamental consistente en la digitalización y centralización de todas las bases de datos a nivel estatal para compartir información entre los diferentes organismos públicos. Utiliza metodología de investigación de redes sociales, el software establece conexiones entre personas y crímenes, cosa que a un investigador-analista humano le sería mucho más complejo realizar, debido a la información de que dispone el programa. Es herramienta esencial para identificar, predecir, prevenir e interrumpir actividades fraudulentas terroristas y redes criminales. Hay otras herramientas, como *Salvac*, en el análisis de crímenes violentos o sexuales, o el programa *Chardon*, que identifica hechos criminales perpetrados por la misma persona.

35. ECK, J., CHAINEY, S., CAMERON, J.; WILSON, R., *Mapping crime: Understanding hotspots*, U.S. Departament of Justice, 2005.
36. CHANEY, S.; TOMPSON, L., UHLIG, S., "The Utility of Hotspot Mapping for Predicting Spatial patterns of Crime", *Security Journal, 2008– n 21,* pp. 4-28.
37. AEKBAL, S., *et al.*, "The Crime Ecology: Ambient Temperature vs. Spatial Setting of Crime (Burglary)", en *Procedia-Social and Behavioral Sciences,* 2012, n. 40, pp. 212-222.

Tras Francia, se fueron sucediendo los países en los que se han desarrollado herramientas predictivas de riesgos de delincuencia, de manera que le sucedió Suecia primero, e Italia, después. Fue en Italia donde el primer software de análisis predictivo fue *KeyCrime* en 2007, un programa que permite predecir crímenes en serie además de dónde, cuándo y cómo. Trabaja con datos almacenados, aplicando análisis de prácticas y herramientas de las matemáticas, psicología comportamental, la estadística y el análisis geoespacial. Solo se utiliza en Milán. Le siguió Reino Unido con el *PredPol*, elaborado en California en 2011 que fue extrapolado por la Policía de Kent en 2013 para conseguir procesar datos y analizarlos, ofreciendo predicciones sobre dónde y cuándo podrían tener lugar (previsión) esos hechos delictivos. Les siguió Bélgica y posteriormente se aplicaron en Países Bajos las herramientas *Crimen Anticipation System* (*CAS*), desarrollado por la policía de Ámsterdam en 2013 y extrapolado a todos los Países Bajos en 2017, que ofrece una predicción sobre dónde, cuándo y por quién (supone un aporte objetivo-subjetivo, por lo que es más amplio que los anteriores) y *Visual Analytics for sense-making in Criminal Intelligence Analysis (VALCRI)*, que es un sistema que permite generar ideas plausibles acerca de cómo, cuándo y por qué se cometió un delito, si bien se extiende subjetivamente a quién podría ser su autor, realizando un análisis de la escena del delito que permite detectar patrones sospechosos y reconstruye escenas, empleando incluso el reconocimiento facial; en ambos casos, la extensión a la esfera subjetiva es palmaria.

Tras estos países han continuado desarrollándose numerosos sistemas en Alemania, España, Dinamarca y Austria. A título ilustrativo, en Alemania el primer programa de análisis predictivo implementado fue *Precobs*, centrado en la predicción de las localizaciones donde podría perpetrarse el robo en una vivienda. Existe otro software, *Skala*, que fue originalmente desarrollado en 2015 por la Oficina Estatal de Investigación Criminal del Estado de Rhine Westphalia del Norte y la empresa tecnológica IBM, convirtiéndose en la actualidad en el principal programa de análisis predictivo de Alemania. Además de la renta per cápita, porcentaje de desempleo y media de edad de los residentes locales (datos socioeconómicos), el software valora aspectos como la presencia de autopistas o estaciones de tren y/o autobús, ligando este hecho a la probabilidad de que los delincuentes tengan más facilidad para evadirse tras la comisión de un delito, y por tanto siendo áreas más susceptibles de albergar criminalidad. Este sería el caso, por ejemplo, del robo de vehículos.

La mayoría de los programas desarrollados en Europa se circunscriben a centros urbanos, centrándose en la evaluación de riesgos comunitarios (*predictive mapping*), no individuales, aun cuando va cambiando, como lo

demuestran las múltiples herramientas que tratan de predecir la reincidencia. Se ha ido pasando de la predicción exclusivamente objetiva a la también predicción subjetiva, por lo que anticipan la posible comisión de hechos delictivos de las personas en función de unos criterios que alimentan el algoritmo.

En España, por ejemplo, la aplicación de los *SIG (sistema de información geográfica*), ha sido algo más tardía, en diversos ámbitos para identificar las concentraciones delictivas, en atención a características sociales de la zona, meteorología, topología. Se permite una mejor gestión de medios policiales en lugares y momentos determinados. Se ha utilizado por la Policía Municipal de Madrid a través del Centro Integrado de Seguridad y Emergencias (CISEM)[38], para realizar mapas de riesgo, permitiendo planificar los servicios. El *CISEM* se constituye como una modalidad de "geoprevención", consistente en el análisis de las relaciones existentes entre los agentes del crimen y el territorio, la integración de estrategias preventivas necesarias y su implementación mediante las tecnologías SIG, para favorecer la reducción de la delincuencia y una mayor seguridad[39]. Desde 2015 la Policía Nacional ha empleado estos sistemas también para la delimitación de las zonas o lugares de patrullaje, tomando en consideración las características sociales de la zona, meteorología, topología, empleándose estos modelos de información geográfica, que ofrece identificación de concentraciones delictivas, de manera que permita una mejor gestión de medios policiales en lugares y momentos determinados.

Por tanto, hoy concurren las herramientas predictivas objetivas con las subjetivas. Un sistema interesante es el diseñado en el Reino Unido, por la Policía de Durham, *HART* (*Harm Assesment Risk Tool)* para predecir si los sospechosos tienen un bajo, moderado o alto riesgo de cometer más delitos en un periodo de dos años, a efectos de aplicar medida limitativa o privativa de libertad, así como programa de rehabilitación. HART utiliza datos de 34 categorías diferentes (entre ellas, edad, sexo, domicilio, antecedentes penales, profesión, estado civil, etc.)[40].

Una de las herramientas más citadas, en gran medida por la posición contraria que generó su aplicación fue COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions)* que realiza cálculos

38. ARIAS, A., "Centros de Seguridad y Emergencias en Ayuntamientos", en *Auditoría y Seguridad,* 2009, n. 33, p. 82; e igualmente puede verse GONZÁLEZ, F., "Gestión de Información en los Servicios de Seguridad", en *DINTEL Alta Dirección*, 2010, n. 12, pp. 146-149.
39. HERNANDO, F., "La seguridad en las ciudades: El nuevo enfoque de la Geoprevención", en *Scripta Nova, 2008,* Vol. XII, N. 270 (14).
40. https://www.durham.police.uk/Information-and-advice/Pages/Checlpoint.aspx.

probabilísticos sobre la posible comisión de delitos por una persona, permitiendo la adopción de medidas cautelares más gravosas o una condena más grave; su aplicación en el caso del ciudadano americano Eric Loomis en 2013 suscitó un enorme debate, al condenarle con pena más grave por aplicación de esta herramienta, que avizoraba una reincidencia delictiva. Planteada apelación, se solicitaba conocer la herramienta, para ejercitar el derecho de defensa, lo que se negaba por la empresa diseñadora de la herramienta al considerar que se vulneraba la protección de los derechos de autor y de propiedad inmaterial. Se plantea el equilibrio entre los derechos de autor de la empresa y el derecho al debido proceso[41].

En España resulta muy interesante la herramienta predictiva *VIOGÉN*[42], para supuestos de violencia de género, en marcha desde el 26 de julio de 2007 por el Ministerio del Interior, que trabaja con una red que permite el seguimiento y la protección de forma rápida, integral y efectiva de las mujeres maltratadas, y de sus hijos e hijas, en cualquier parte del territorio nacional[43]; en función del nivel de riesgo resultante, el protocolo contempla la adopción de determinadas medidas de protección policial que pretenden evitar la reincidencia[44]. Igualmente, la herramienta predictiva empleada en Galicia para configurar perfiles de posibles incendiarios forestales; era un sistema en el que, a partir de indicios encontrados en el incendio, buscaban la identificación y localización de sus posibles autores[45].

Todos estos sistemas algorítmicos y herramientas predictivas de riesgos han propulsado una metamorfosis del modelo policial. Se produce una transformación actuacional que muta la concepción de persecución penal, dado que la actuación *ex post* se traslada a la actuación *ex ante*, o

41. LARSON, J.; MATTU, S.; KIRCHNER, L.; ANGWIN, J., "How we analyzed the COMPAS recidivisim algorithm", *ProPublica,* 23 de mayo de 2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.
42. Sobre los datos estadísticos del sistema de seguimiento integral en los casos de Violencia de Género puede verse el Informe presentado en noviembre 2021 por el Ministerio del Interior. http://www.interior.gob.es/documents/642012/12866658/NOVIEMBRE+21/0103d9bb-faeb-411f-9351-e947e8db6135.
43. http://www.interior.gob.es/web/servicios-al-ciudadano/violencia-contra-la-mujer/sistema-viogen.
44. Se emplean formularios VPR (Valoración Policial del Riesgo) y VPER (Valoración Policial de Evolución del Riesgo). Los niveles de riesgo son cinco: "No apreciado", "Bajo", "Medio", "Alto" y "Extremo", según lo recoge la Instrucción 4/2019, de la secretaría de Estado de Seguridad, con entrada en vigor el 13 de marzo de 2019 y cada nivel lleva asociadas una serie de Medidas de Protección y seguimiento, de aplicación obligatoria, que varían en intensidad según el nivel de riesgo del caso en cada momento.
45. SOTOCA, A.; GONZÁLEZ, J. L.; FERNÁNDEZ, S.; KESSEL, D.; MONTESINOS, O.; RUIZ, M., "Perfil del incendiario forestal español: aplicación del perfilamiento criminal inductivo", *Anuario de Psicología Jurídica* n. 23, pp. 31-38.

si se quiere de la función reactiva a una función preventiva (proactiva). Y ello muestra un escenario con una actora protagonista, la Policía, que participa con un papel diverso, a saber, se abandona el viejo *modus operandi* intuitivo humano para actuar con las herramientas computacionales y algorítmicas que trabajan con predicción de riesgos, lo que favorece la neutralización de la delincuencia amén de su persecución. Tarea que no realiza *ex post*, sino que la despliega *ex ante*. El modelo actuacional policial cambia. Estas herramientas permiten la optimización de los medios y de la gestión, amén de recopilar y elaborar un número importante de datos que facilitan la elaboración de patrones, tendencias o relaciones secuenciales que pueden ser empleadas para prevenir la delincuencia o para favorecer futuras investigaciones.

Ahora bien, una de las falencias de este modelo policial es la falta de transparencia, ante el desconocimiento de estas herramientas en su diseño, materialización y uso, generando lo que se ha denominado como modelo de caja negra[46], sin saber cuál es el contenido de la fórmula que se emplea para poder alcanzar el resultado. La concurrencia de sesgos en las herramientas algorítmicas (racistas, homófobos, sexistas, clasistas, etc.), provoca injusticias, desigualdades y vulneraciones de derechos. O, lo que es lo mismo, los sesgos pueden manipular ideas, pensamientos, culturas, comportamientos, etc., generando segregación, etiquetas, desigualdades, desprotección, etc.[47] y pueden dar lugar incluso a la aparición de los denominados "falsos positivos". De ahí que se insista, especialmente en Europa, en la necesidad de capacitación adecuada de los agentes policiales en el uso de estos modelos predictivos. Y se asuma, en todo caso, que no son neutras y, por supuesto, tampoco son infalibles.

2. MODELOS ALGORÍTMICOS EN LA INVESTIGACIÓN PENAL

La empleabilidad de la tecnología en la función policial ha transformado el *modus operandi* actuacional policial. Hemos asistido a la optimización de los medios, de la gestión y muy específicamente del capital humano policial, gracias a estas herramientas. Es cierto que con ellas se

46. Los datos están encerrados en estas cajas negras, que forman parte de una suerte de ecosistema cerrado digital que no interacciona ni se retroalimenta de los flujos de información que se hallan al aire libre. *Vid*. CARDON, D., *Con qué sueñan los algoritmos, cit*., p. 92.

47. Como apunta BAUMAN, Z., *Posmoderne Ethik,* Hamburgo, Hamburger edition, 1995, p. 290, el mundo construido por la tecnología se presenta como *exquisitamente flexible, fluido, rebosante de oportunidades y resistente a cualquier fijación*, si bien también se presenta como *moldeable, vulnerable e indefenso, presa fácil del ingenio y del know-how tecnológico, un campo fértil para apetitos insaciables.*

ha favorecido la intervención policial *ex ante,* la predictibilidad desde la previsión de riesgos. Ahora bien, esta manera de actuar no queda ahí tan solo, sino que se ha ido trasladando al mundo jurídico penal *ex post*. De este modo, estos sistemas están convirtiéndose en el medio para llevar a buen término una investigación penal adecuada. Esta incorporación está favoreciendo una mutación de la piel de la Justicia penal; una Justicia que se encuentra en un estado de mudanza constante y a velocidad célere y en la que también la traslación de la vida digital, la sociedad digital y el pensamiento digital ha alcanzado las maneras de investigación penal[48].

1.º– En primer lugar, desde el punto de vista de los protagonistas en la investigación, hemos asistido a un cambio trascendental. La policía asume un rol protagónico. En gran medida la atribución subjetiva de este protagonismo viene paralela al crecimiento exponencial de la incorporación de herramientas tecnológicas, computacionales y algorítmicas en el desarrollo de la investigación. Su capacitación en el manejo de esos modelos computacionales y algorítmicos ofrece un soporte asistencial esencial e innegable en la investigación de la delincuencia y muy especialmente de determinada delincuencia. En nuestro país, la lectura de los arts. 282 a 298 de LECRIM (Título III. "De la Policía Judicial") es enormemente ilustrativa del aumento funcional policial y de su papel protagonista.

La consecuencia directa de esta premisa expuesta ha sido la necesaria reformulación de las legislaciones procesales, adaptando las normas a esta nueva realidad digital. El desarrollo de las ciencias forenses, la criminalística, ha sido espectacular, propulsado, en gran medida, por la incorporación de la tecnología, anudada a la ciencia, que ha permitido la introducción de técnicas idóneas para buscar y analizar evidencias, amén de favorecer su conversión en fuentes de prueba en el proceso penal. Los instrumentos tecnológicos que permitieron detectar riesgos (predecir) se adentran en la investigación (fuentes) para convertirse en fuentes de prueba (predicción-investigación y prueba), incluso favoreciendo las medidas de seguridad postcondena, siempre con el eje nuclear de los riesgos que hay que evaluar para la toma de decisiones (con consecuencias jurídicas penales importantes). Esta realidad es indiscutible, ofreciendo una gran eficiencia actuacional, empero también acrecentando la preocupación de la difuminación entre la naturaleza jurídica de las diversas actuaciones, principios, sujetos y consecuencias, de manera que las medidas de investigación tecnológicas se permiten para actuaciones preventivas y para la investigación.

48. BARONA VILAR, S., "La digitalización y la algoritmización, claves del nuevo paradigma de justicia eficiente y sostenible", en COLOMER HERNÁNDEZ, I., *Uso de la información…, cit.,* pp. 96-99.

Esa confusión no es neutra y supone la reformulación de un derecho penal *ex post* hacia un derecho penal *ex ante*, que reacciona ante riesgos y amenazas, y lo hace con carga en profundidad sobre las garantías y los derechos; nuestro núcleo esencial de preocupación[49]. Asistimos a una coyuntura existencial –política, ideológica, económica y jurídica– en la que el modelo de Justicia penal que se diseñó desde el Estado liberal y revolucionario, completado por las políticas del Estado social, que fue caminando y asentándose entre la *racionalización y la civilización*[50], ha sido absolutamente superado por un modelo neoliberal[51], en el que se ha fomentado una imparable y clara regresión en materia penal, procesal penal y política criminal. No es algo local, sino una transformación progresiva o una metamorfosis integral del modelo de Justicia Penal del planeta[52]. Una involución que claramente responde a las políticas del neoliberalismo político neoconservador[53]. Esta involución es consecuencia de las políticas neoliberales anglosajonas, origen de la globalización, que arrastró desigualdades, descontentos, violencia, delincuencia callejera, incluso criminalidad sofisticada, fomentaron la teoría del control social, asentada en los conceptos de tradición, ley y orden[54], jerarquía y autoridad, como valores esenciales. Las decisiones de política criminal se dirigían a paliar el descontento social, a través de la adopción de múltiples medidas[55]. Este retrato social fue acompañado de una ola de involucionismo penal, que se escenificó con mucha expansión y derecho penal simbólico, mucho control y mucho discurso de la seguridad, escenificando un Estado débil y frágil, minimalista y atópico[56], que había aceptado ceder espacio a otros

49. Puede verse mi obra BARONA VILAR, S., *Algoritmización del Derecho y de la Justicia…, cit.*, especialmente pp. 424-435.
50. GARLAND, D., *The culture of control. Crime and Social Order in Contemporary Society*, Oxford University Press, 2001, p. 34.
51. DEL ROSAL BLASCO, B., "¿Hacia el Derecho penal de la postmodernidad?", en *Revista Electrónica de Ciencia Penal y Criminología*, 2009, p. 3.
52. BARONA VILAR, S., *Proceso penal desde la Historia, cit.*, pp. 470-471.
53. MIR PUIG, S., "Evoluzione política e involuzione del Diritto Penale", en la obra a cura di Alfonso Maria Stile, *Democrazia e autoritarismo nel diritto penale*, *cit.*, p. 118.
54. SIMON, J., *Governing through Crime*, Oxford, Oxford University Press, 2007. La expresión de la *ley y orden* que permitió la configuración del estado liberal al que se refirió Hobbes en el Leviatán, se ha empleado no tanto para defender la existencia de un Estado al servicio de sus ciudadanos, sino para ejercer la función del Estado precisamente contra los ciudadanos, un modelo de control de éstos, que no de garantía de aquéllos.
55. GARLAND, D., *The Culture of Control, cit.*, p. 127.
56. El sentido y significado de Estado atópico vino casando con el Estado minimizado, residual pero Estado a la postre que no desparece pero que queda claramente "deubicado" o "deslocalizado" (sin lugar), significado que tiene el término griego *atopia.* A él se refiere WILLKE, H., *Atopia. Studien zur atopischen Gesellschaft*, Suhrkamp

sujetos, a instituciones públicas y privadas, nacionales e internacionales, y a la sociedad civil. Este retrato social generó un descontento social y ciudadano, que ha propulsado la aceptación del control a cambio de la pérdida de libertades, a cambio de más y más seguridad, que, de alguna manera, ha favorecido esta mutación en la Justicia penal, en la intromisión en la esfera jurídica-privada y en la conversión de una sociedad de garantías por una sociedad del control.

2.º– Esta "manera" de investigar no solo afecta a quien investiga, sino también a quien es objeto de investigación, de manera que asistimos a una expansión subjetiva de la investigación a terceros que ni son sospechosos ni son imputados ni guardan relación con los hechos delictivos objeto de la investigación. Las nuevas diligencias de investigación lo permiten (art. 588 ter c de la LECRIM).

3.º– Obviamente, todo ello viene completado con los sistemas técnicos y tecnológicos cada vez más sofisticados que permiten el actuar *ex ante*, desde la fortaleza que ofrece la denominada vigilancia preventiva policial, que no puede practicarse de forma indiscriminada salvo que concurran motivos de seguridad del Estado, defensa nacional, seguridad pública, prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, o situaciones extremas similares. Y que van a reforzar, igualmente, las intervenciones *ex post*, si bien con cambios en las maneras y en los resultados de la investigación. Por ejemplo, es posible el empleo de la vigilancia dinámica, a través de cámaras colocadas en determinados lugares, consiguiendo tecnológicamente una vigilancia visual, o incluso acústica, que tiene lugar a ciertas distancias[57], mucho más eficiente que la vigilancia policial personal. Y, por otro lado, a título de ejemplo, tras la incorporación por la LO 5/1999, de 13 de enero, de la vigilancia policial a través del "agente encubierto" (art. 282 bis LECRIM), la LO 13/2015, de 5 de octubre adaptó las figuras existentes a la realidad digital, mediante la creación del denominado "agente encubierto informático", regulado en el art. 282 bis 6, II LECRIM, facultándole intervenciones en canales electrónicos de comunicación cerrada. Además, hemos asistido a una paulatina incorporación desde 2015 de medios técnicos y tecnológicos que avalan cambios en la vigilancia predictiva con

Taschenbuch Wissenschaft, 2001, quien construye el concepto desde su consideración de la "deconstrucción de la utopía", pp. 7 a 62.

57. GÓMEZ COLOMER, J. L., "El aumento del intervencionismo público en la investigación del delito. Una reflexión al hilo del acto de investigación criminal de registro remoto de equipos informáticos (coloquialmente llamado 'gusano informático')", en la obra colectiva *Estudio Probatorio y otros Estudios procesales. Liber Amicorum Vicente Gimeno Sendra,* Ediciones Jurídicas castillo de Luna, 2020.

consecuencias en el proceso, entre ellos la posible grabación de la imagen en espacio público sin necesidad de autorización judicial (una suerte de *Big Brother* tecnológico), la autorización de intervención y registro de las comunicaciones de cualquier clase que se lleve a cabo, vía teléfono o a través de cualquier otro sistema de comunicación telemática, lógica o virtual (WhatsApp, email, etc.), entre otras. Todos ellos, incorporados a la LECRIM, tiene como fin dar cobertura a su empleo por la policía en la persecución de los hechos delictivos y muy concretamente en la lucha contra determinada delincuencia sofisticada, compleja o incluso la ciberdelincuencia.

Las herramientas algorítmicas que se van incorporando para desplegar la investigación y obtener resultados se multiplican en la mayor parte de los países, ofreciendo apoyos al juez en la toma de decisiones derivadas de la investigación. A ellas nos referimos *infra.*

4.º– Efecto consecuencia de cuanto hemos expuesto es que los resultados en la investigación policial realizada a través de estos medios van a alcanzar valor probatorio, obviamente bajo las condiciones legalmente establecidas y discriminando los casos en que lo aportado al proceso se haya obtenido con vulneración de derechos fundamentales, impidiéndose que surtan efectos probatorios.

En conclusión, la realidad predictiva y algorítmica es incuestionable, como también lo es el hecho de que el mal uso de estos medios puede traer consecuencias negativas. Vivimos en la era de la fascinación algorítmica, lo que puede propulsar la asunción de la fiabilidad absoluta. Los modelos algorítmicos se basan en datos, y esos datos pueden servir o pueden aniquilar, pueden asistir o pueden laminar, pero es importante saber que son medios al servicio de la humanidad, no la humanidad al servicio de ellos. Que estos sistemas están transformando los cuerpos policiales, y aun lo harán más, es indiscutible; lo importante es trabajar para perfeccionarlos, para conocerlos, para usarlos siempre con el control humano que será quien tomará las decisiones pertinentes. En este camino, por tanto, no solo hace falta perfeccionar los modelos existentes, sino también conocerlos, evaluarlos, utilizarlos, pero con el convencimiento de que pueden ser un gran sostén al desempeño de la función policial, no sustitutos de las decisiones humanas.

3. EL EMPLEO DE LOS MODELOS BIOMÉTRICOS

Junto a las herramientas algorítmicas y computacionales empleadas *ex ante* o *ex post* en la investigación, han ido progresivamente ganando espacio en algunas regiones del planeta los sistemas biométricos. Son plurales

y heterogéneos y su funcionalidad en la actualidad es indiscutible (controles laborales, instrumentos de lucha contra fraude, acceso a dispositivos individuales, etc.). Existen los sistemas de identificación basados en el análisis de sus huellas dactilares, geometría de la mano, retina o iris del ojo, imagen facial, la oreja (otograma), los movimientos, etc., procediendo a su registro para poder desarrollar posteriormente su identificación. Su objetivo es identificar (reconocimiento) o autenticar (verificación) a las personas a partir de algunas características fisiológicas o morfológicas[58].

De entre los múltiples medios biométricos el más cuestionable es el del reconocimiento facial, que permite reconocer a una persona por los rasgos de su cara, empleando algoritmos, a través de "búsqueda de la apariencia". La amplia experiencia en China, Japón, Corea del Sur, Singapur, EEUU, etc., es larga. En Europa, pese a su indudable, aunque muy restringido empleo, sigue manteniéndose una prohibición del reconocimiento facial y el uso de otros datos biométricos sin el consentimiento de las personas, de ahí que la usabilidad de los mismos tiene que venir condicionada al cumplimiento de su específica función. Merece destacarse el Informe elaborado por la Comisión de Libertades civiles, Justicia y Asuntos de Interior (LIBE) del Parlamento, siendo refrendado por éste en octubre de 2021, en virtud del cual se solicita a la Comisión que implemente, mediante medios legislativos, no legislativos y procedimientos de infracción, la prohibición de cualquier procesamiento de datos biométricos incluidas las imágenes faciales con fines policiales, que conduzcan a una vigilancia masiva en espacios de acceso público. Existe un rechazo al *Big Brother* planetario o una suerte de panóptico benthiano digital, controlado por Estados o multinacionales tecnológicas, exponente de modelos totalitarios de control[59], evitando un control intenso y permanente de lugares o espacios que afecta directamente derechos fundamentales y puede provocar decisiones lesivas a la ciudadanía fruto de falencias en el diseño y funcionamiento de los sistemas[60].

IV. SISTEMAS ALGORÍTMICOS EN LA PRUEBA PENAL E INFLUENCIA EN LA DECISIÓN JUDICIAL

La irrupción en la esfera penal de los sistemas algorítmicos y computacionales, tanto en la prevención policial *ex ante* como en la investigación

58. BOULGOURIS, N. V. *et. al.*, *Biometrics, Theory, Methods, and Applications*, IEEE and WILEY, Estados Unidos, 2010.

59. HAN, B-CH., *En el enjambre*, *cit.*, pp. 108-109.

60. ETXEBARRÍA GURIDI, J. F., "Inteligencia Artificial aplicada a la videovigilancia: tecnologías de reconocimiento facial", en BARONA VILAR, S., (ed.), *Justicia algorítmica y Neuroderecho*, Valencia, Tirant lo Blanch, 2021, p. 448.

criminal *ex post* trae consecuencias también en el proceso penal y, muy especialmente, tiene una enorme influencia en la prueba y en la toma de decisiones judiciales, sea tanto en las que se adoptan a lo largo de la investigación, como las que se dictan en el juicio oral y muy especialmente en la resolución que pone fin al proceso. Con ello es innegable que estamos ante una serie de instrumentos que inciden en la función que desempeñan los jueces en el proceso penal, a saber, en la *Judge Craft*[61], esto es, tanto en la *Judicial Decision* como en su proceso de elaboración. Es más, comienzan a emergen herramientas algorítmicas con una eficacia innegable también en la fase de ejecución penal y muy especialmente en cumplimiento de condena en establecimiento penitenciario.

1. ALGORITMIZACIÓN DE LAS FUENTES DE PRUEBA

En primer lugar, resulta interesante observar cómo la incorporación algorítmica está suponiendo una posible conversión de la naturaleza de las fuentes de prueba, de manera que estamos asistiendo a una suerte de algoritmización de éstas. Este fenómeno lo podemos encontrar:

1°) En aquellas herramientas algorítmicas que, amén de almacenar datos, los seleccionan y configuran un documento específico[62]. Esta técnica permite, en consecuencia, crear el documento para incorporarla al proceso como prueba documental.

2°) Existen asimismo herramientas computacionales que ejecutan informes-auditorías que pueden aportarse al proceso con valor probatorio documental-pericial. Lo característico en este caso es que van acompañadas de una valoración de resultados y de posibles riesgos. De hecho, en algunos supuestos estas valoraciones se presentan con algunas propuestas para evitar, por ejemplo, riesgos de que una persona jurídica pueda incurrir en una posible responsabilidad penal.

3°) Existen numerosas herramientas predictivas de riesgos, que ofrecen un buen complemento y/o una suerte de asesoramiento a la hora de dictar sentencias o de adoptar medidas cautelares u otras decisiones. Aunque se presentan con valor instrumental, son en muchos casos soporte de las resoluciones judiciales, convirtiéndose en decisivas. Algunos ejemplos:

61. Un desarrollo *ad extensum,* BARONA VILAR, S., *Algoritmización del derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice,* Valencia, Tirant lo Blanch, 2021, citado.

62. FIGUEROLA, C.; ALONSO BERROCAL, J. L.; ZAZO RODRÍGUEZ, A. F.; RODRÍGUEZ, E., "Algunas técnicas de Clasificación Automática de Documentos", en *Cuadernos de Documentación Multimedia, Vol. 15,* 2004, pp. 3-12.

ADVOCATE es una herramienta que permite evaluar la idoneidad y/o fiabilidad de un testigo, de manera que permite valorar la prueba testifical con elementos interpretativos derivados de la aplicación de esta herramienta; COMPAS, en su momento permitió arrojar resultados algorítmicos acerca de la posible reincidencia delictiva, condicionando el sentido de la decisión judicial, fuere cautelar o fuere la decisión final del proceso; VioGÉN permite evaluar el riesgo de reincidencia de los victimarios en caso de violencia de género; la herramienta canadiense ASSYST[63] se ofrecía a ayudar a los jueces a aplicar las directrices en la sentencia, si bien al final lo que la herramienta provocaba era una suerte de aplicación automática de la condena; o LIST, desarrollado en la University of British Columbia, proporciona información relevante al juez, que no pretende determinar el contenido de la resolución, sino facilitarla. Se han criticado ambas al considerar que ninguna de las dos es capaz de asimilar en cada caso la complejidad real del supuesto y del razonamiento a seguir en la sentencia[64].

4°) Es más, amén de estos instrumentos algorítmicos, debe considerarse igualmente la posibilidad de emplear los modelos biométricos para obtener datos que se incorporan como fuente de prueba en el proceso, convirtiéndose ineludiblemente en sustento probatorio.

2. UTOPÍA O DISTOPÍA EN TORNO AL EMPLEO DE LAS HERRAMIENTAS ALGORÍTMICAS EN LA PRUEBA PENAL

La fascinación utópica por estas herramientas permite concentrar esfuerzos en reforzar el perfeccionamiento de las mismas para favorecer cada vez más la automatización funcional en el hábitat de la justicia penal. Hemos ido exponiendo *supra* manifestaciones de la justicia algorítmica y consecuencias derivadas de su aplicación. Cierto, son herramientas que asisten a los operadores jurídicos en la toma de decisiones (sean abogados, jueces, fiscales, policías, etc.) y pueden mostrarse como la esperanza de ofrecer más y mejor en menos tiempo. Ahora bien, no pueden presentarse como la perfecta solución frente a las personas, dado que, si bien ciertamente las personas no son infalibles –y no lo dudamos–, las máquinas tampoco lo son, fundamentalmente porque "se limitan a reproducir lo que nosotros

63. Se trata de un programa *Sentencing Guideline Calculator* al que se refieren SIMÓN, E.; GAES, G., "ASSYST – computer support for guideline sentencing", en *Second International Conference on Artificial Intelligence and Law (ICAIL-89*). Vancouver, ACM Press, pp. 195-200.
64. SCHILD, U. J., "Criminal Sentencing and Intelligent Decision Support", en *Artificial Intelligence and Law* 6, 1998, p. 159.

hacemos y pensamos"[65], son simuladoras del pensamiento humano, pero ni piensan, ni sienten, ni dudan, ni contextualizan. Generan, por ende, el dilema de sí nos hallamos ante una utopía o una distopía ante el fascinante empleo de los algoritmos en el ámbito probatorio del proceso penal.

Una de las cuestiones que suscita debate es la denominada falsa neutralidad de los modelos algorítmicos. Los algoritmos no son neutros, ni infalibles y su aplicación, en numerosos casos en diversos ámbitos de la vida, ha mostrado el lado oscuro, a saber, la desigualdad social, por sexos, por ideología, por edad, por nacionalidad o lugar del domicilio, por etnia, etc. Esa falsa neutralidad de los algoritmos puede incidir en la tutela de la ciudadanía y más directamente en sede probatoria, generando en algunos casos un distópico desequilibrio de los elementos esenciales en la prueba. De este modo, se pone en duda y se cuestiona cómo garantizar los principios y las reglas de un proceso con todas las garantías, cuando su desarrollo se ha soportado sobre la aplicación de modelo algorítmicos incisivos en la toma de decisiones.

PRIMERO.– Con un carácter general y esencial en el ámbito procesal, emerge la duda acerca de cómo garantizar el debido proceso, especialmente el derecho de defensa y la contradicción. Esta premisa se anuda a la dificultad de rebatir una decisión judicial que se haya podido fundar en los resultados de un modelo algorítmico predictivo de riesgo, dado que concurre una suerte de "infalibilidad" de estos sistemas. Se habla de las denominadas cajas negras de las máquinas, aun cuando cabría oponer a esta idea que también los humanos actúan con sus propias cajas negras. En cualquier caso, frente a los posibles sesgos que pueden concurrir en estas herramientas y a las múltiples dificultades que puede comportar rebatir sus contenidos, hay voces en la doctrina procesal favorables a considerar excluida como prueba los resultados que se aportan al proceso por la aplicación de estos sistemas, cuando es la única base probatoria de la sentencia condenatoria, lo que puede, a su vez, generar impunidad en ciertos casos. La dificultad está en alcanzar un equilibrio que permita su usabilidad con condiciones, a sabiendas de la utilidad probatoria que pueden reportar, empero siendo conscientes de su falibilidad.

SEGUNDO.– Obviamente lo expuesto con carácter general, en un sistema procesal garantista, genera dudas y frustraciones, todo y que, a la vez, inspira a los más eficientistas. No obstante, la aplicación de herramientas algorítmicas está suponiendo la necesidad de replantearse algunas cuestiones que, directa o indirectamente, alteran los postulados

65. PASCUAL, M. G., "Cuando el algoritmo se equivoca", en *El País Semanal,* 27 de junio de 2021, p. 36.

probatorios y muy específicamente la presunción de inocencia, entendida en sus tres vertientes, a saber: a) Como derecho fundamental de status de inocente del sujeto sospechoso, investigado o encausado; el sistema algorítmico invierte en ciertos casos el status de partida, favoreciendo una suerte de presunción de culpabilidad; b) Demostrar la inocencia afecta a la regla probatoria derivada de la presunción de inocencia, dado que la carga de probar la culpabilidad, precisamente a consecuencia de la utilidad del sistema algorítmico, se desplazaría de las partes acusadoras, que deben probar la totalidad de los elementos constitutivos del delito, tanto de carácter objetivo como subjetivo, hacia el acusado, que quedaría al descubierto ante los datos arrojados por la fórmula predictiva[66]; c) Y, en tercer lugar, la aplicación de estos sistemas allana la valoración de la prueba, superponiéndose al "*in dubio pro reo*", en cuanto el sistema algorítmico pueda convencer directamente al juzgador sobre la culpabilidad, más allá de toda posible duda razonable.

TERCERO.– Finalmente, la consecuencia de cuanto hemos expuesto es precisamente que todo lo anterior va a incidir en la motivación de la sentencia, referida a la valoración de la prueba y a las razones por las que se dicta la sentencia (razones, en todo caso, transparentes y visibles). Afecta, en consecuencia, a la argumentación jurídica de la sentencia, que exige dar razones de la decisión. En este sentido, el Informe "Artificial Intelligence and Fundamental Rights" presentado por la *European Union Agency for Fundamental Rights* en el año 2020, exige justificar adecuadamente los criterios y procesos mediante los cuales se adoptan decisiones basadas en algoritmos, esto es, debe contar con la correspondiente motivación, con la dación de razones, con los argumentos que justifiquen la decisión tomada a la luz de la prueba practicada.

3. ALGORITMIZACIÓN DE LA *JUDGE CRAFT.* EL CAMINO SILENTE HACIA LA JUSTICIA HÍBRIDA Y LA ROBOTIZACIÓN JUDICIAL

El oficio de ser juez (*Judge* Craft) tiene un elemento nuclear en la toma de decisiones. Para realizar esa función, allende conocer el derecho, los

66. Cuestión diversa es la de plantear a quién corresponde la prueba de los hechos y las circunstancias que conforman atenuantes y eximentes, que, según doctrina ya consolidada de la Sala 2.ª TS y del TC, en términos generales, la carga de probar eximentes y atenuantes corresponde a quien las alega, a saber, a la defensa del acusado. Puede verse DE HOYOS SANCHO, M., "La presunción de inocencia en el Anteproyecto de Ley de Enjuiciamiento Criminal de noviembre de 2020. Algunas valoraciones y propuestas con ánimo constructivo", en *Revista Aranzadi de Derecho y Proceso penal 63, julio-septiembre 2021,* p. 168.

jueces piensan jurídicamente y deciden en cada caso concreto dando respuesta a la tutela judicial efectiva. La teoría es sencilla, si bien la puesta en práctica exige el manejo de herramientas que van desde conocer la norma, hasta interpretarla, adaptarla y, por supuesto, razonar la decisión (argumentar o dar razones), a través de la motivación. El juez no es un autómata, lo que plantea el dilema de si se pueden automatizar las decisiones judiciales.

Como punto de partida, es indudable que en la actualidad los jueces comienzan a emplear herramientas colaborativas o asistenciales que le facilitan la tarea judicial (extracción y análisis de documentos, predicción de riesgos, evaluación de testigos y de su fiabilidad, reconstrucción de hechos, búsqueda de indicios a partir de otros hechos similares, etc., algunas de las cuales han sido citadas *supra*). En ellas no se sustituye al juez, sino que éste se sirve de ellas en cuanto le colaboran para decidir. Repárese que en algunos países anglosajones se han presentado algunos softwares que permiten incluso formular hipótesis sobre cómo llegaron a suceder los hechos, con propuestas exculpatorias o inculpatorias. La variedad y heterogeneidad de estas herramientas, amén de su funcionalidad, es grande, siendo que en unos casos son informativas, otras, colaborativas y hasta otras, propositivas de la función de "ser juez", incidiendo de forma automatizada en la *Judge Craft*.

El camino hacia la automatización de la decisión es lo que suscita polémica, si bien comienza a presentirse como una realidad, si no generalizada, si para algunas cuestiones y en determinados ámbitos. Es el dilema de la búsqueda de la sustitución del ser humano por la máquina y la pérdida de humanidad de las decisiones judiciales. Se trata de incorporar, a la postre, sistemas computacionales "¿capaces?" de realizar el oficio del juez, de sustituir al juez humano en las decisiones propias de la función jurisdiccional, propiciando la aparición de los "juez-robot"[67].

Esta evolución en sede judicial no es sino la consecuencia de la realidad que vivimos, la respuesta a ese "mundo feliz de los algoritmos perfectos" a que se refiere Markus GABRIEL[68], consecuencia de una delegación de nuestras decisiones esenciales en programas informáticos. La ponderación entre lo más sencillo y la capacidad decisional humana exige un espacio de interpretación, modulación y conformación que nos corresponde como humanidad. De este modo, depende de nosotros mismos el

67. BARONA VILAR, S., "Una justicia 'digital' y 'algorítmica' para una sociedad en estado de mudanza", en la obra colectiva BARONA VILAR, S., *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, *cit.*, p. 46.

68. GABRIEL, M., *El sentido del pensamiento*, *cit.*, p. 262.

que sepamos controlar a la máquina y no ella a nosotros, máxime cuando tras la máquina hay humanos, esto es, siempre habrá quienes hayan implementado implícita o explícitamente su pensamiento, sus parámetros de actuación, etc., en la actividad maquínica, por lo que el resultado algorítmico "debería" pasar el filtro posterior humano, con el fin de seguir garantizando los derechos y valores que los modelos democráticos fueron reconociendo y respetando.

Asumida esta necesidad de considerar, en todo caso, que la mente humana es mente inteligente y filtro final de las máquinas, no puede discutirse que la búsqueda de la automatización de la decisión judicial es ya una realidad. En algunos países se pretende alcanzarla y extenderla a asuntos en los que las decisiones se reiteran o repiten, al darse las mismas circunstancias y condiciones; en otros, se incorporan "a cuenta gotas", y con el debido control de su aplicación. Estos sistemas de automatización plena de la decisión implican la entrega de todo el itinerario decisorio al sistema de inteligencia artificial. Y esto es lo que se considera como robotización judicial, emergiendo una suerte de "jueces-robots", máquinas, sistemas operativos que realizan la tarea de decidir en el marco de la solicitud de tutela judicial efectiva. Esta robotización judicial suscita algunas dudas.

Por un lado, el principal dilema es si puede considerarse que las máquinas piensan como juristas. La respuesta es que las máquinas no piensan, no son inteligentes, sino estadísticas[69], trabajan con una masa de datos que le aportan información para realizar su función; carecen de memoria perceptiva, de sensación de tiempo, de recuerdos, de sensaciones ante éstos, creatividad, etc.. Pensar no es leer letras, no es alimentarse de información y traducirla, integrarla, extraer lo esencial respecto de un caso, que puede ser parte integrante de ese desarrollo intelectual que puede llevar a tomar decisiones por pensar. La máquina puede desarrollar funciones que hasta el momento realizábamos como humanos, y hacerlo a una velocidad inusitada, eficientísimamente, supliendo la carencia de la función humana, pero la máquina no ha podido, al menos hasta el momento, *provocar un discurso interior en el que se plasma la continuidad de la consciencia como memoria*[70]. Al trasladarlo a la función judicial, ésta exige conocimiento de las normas aplicables al caso y de la jurisprudencia, así como la capacidad de interpretarlo, de contextualizarlo también, lo que comporta emociones, percepciones, intuiciones, o lo que es lo mismo, las sensibilidades subjetivas. Y en la función judicial también surge, en no pocos casos, las dudas;

69. CARDON, D., *Con qué sueñan los algoritmos*, *cit.*, p. 78.
70. LLEDÓ, E., *El silencio de la escritura*, Barcelona, Espasa, 2011. p. 151.

la duda en este mundo que vivimos, acelerado, instantáneo, líquido, se ve como flaqueza o debilidad; nos gusta dar sensación de seguridad y no instalarnos en la duda, si bien dudar es fruto del intelecto, en cuanto supone la obligatoriedad de pensar más y no decidir al instante.

Por otro, se habla de la neutralidad de los algoritmos, lo que ya fue referido *supra,* reafirmándonos en los numerosos exponentes de sesgos algorítmicos que no siempre ni necesariamente han sido inoculados por sus diseñadores, sino que son asimilados por herramientas algorítmicas por conductas y parámetros sociales.

Negar la presencia de los modelos algorítmicos en el desempeño de la *Judge Craft* es absurdo. Existen ya plataformas que permiten asumir la función de solventar conflictos en ciertas áreas de conflictividad –probablemente más cercanas a la disponibilidad de las partes, aunque no solo– a través de fórmulas propositivas (puede pensarse en los numerosos *on line dispute resolution* algorítmicos (que los hay), u otras plataformas que en modelos más avanzados y menos garantistas han desarrollado. Los algoritmos han llegado al mundo de la Justicia para quedarse, y los avances nos enfilan directamente hacia la configuración de tres modelos superpuestos: a) Por un lado, aquellos en los que solo los jueces humanos intervienen; b) Por otro, aquellos en que los jueces humanos se apoyan en sistemas tecnológicos (instrumentales) y algorítmicos (funcionales) para la toma de decisiones (siempre con la posibilidad de separarse de propuestas, resultados algorítmicos. Serían modelos híbridos o mejorados de integración (jueces humanos+); y c) Finalmente, aquellos que sustituyen al ser humano por la máquina tanto en la gestión como en la *Judicial Decision*, una suerte de "robotización judicial", justicia automatizada, que ofrecen modelos computacionales de justicia, con capacidad "imitativa"(¿) del ser humano[71], que abren una gran interconexión colaborativa entre humanos y máquinas.

En suma, la Justicia asiste a un gran dilema. Hay que evitar el desequilibrio, las desigualdades, la brecha digital, la aminoración de garantías, la conversión de Justicia en el frío dato estadístico-matemático, que pervierta el modelo de Justicia humano; un modelo con falencias pero que ha venido construyéndose desde el respeto a los derechos y garantías. Si la algoritmización de la Justicia llega y se consolida debe ser para mejora del sistema (eficiente) y de las personas (garantista). Las posibilidades de "usar" las máquinas para mejorar el mundo y la Humanidad son claras. Tenemos la oportunidad de mejorar el mundo, no de perjudicarlo, un mundo en el que la tecnología sirva a la Humanidad y no al revés. ¿Qué podemos hacer los juristas?

71. TURING, A. M., "Computing Machinery and Intelligence", *Mind,* 1950, 49, p. 433.

1. Establecer mecanismos de control (compliance) de los sistemas algorítmicos o de inteligencia artificial, invalidando aquellos que puedan incurrir en sesgos.
2. Asegurar en todo caso que estos sistemas preserven el derecho a la protección de datos personales.
3. Incidir en lo que la doctrina viene denominando la inteligencia artificial explicada.
4. Configurar sistemas de control de funcionamiento: auditorías del sistema de forma periódica.
5. Garantizar la acción humana en estas supervisiones.
6. Favorecer la incorporación de los juristas en el diseño de las inteligencias artificiales.
7. Capacitar a los operadores jurídicos sobre estos sistemas, su usabilidad, sin perder la capacidad de asombro, de crítica y de interpretación del ser humano, en suma, el espíritu y el alma del ser imperfecto pensante.

Capítulo 5

Problemas legales del juez robot desde una perspectiva procesal y orgánica[1]

Juan-Luis Gómez Colomer

Catedrático de Derecho Procesal
Universidad Jaime I de Castellón

1. Texto escrito de la conferencia que pronuncié en Ponta Delgada (Isla de San Miguel, Azores) el día 13 de junio de 2022, gracias al Proyecto de Investigación "La mejora del acceso a la Justicia de la ciudadanía a través de una judicatura más cercana" (JusProx, Código: AICO 2021/272), financiado por la Generalitat Valenciana, Conselleria de Educación, Investigación y Cultura. Convocatoria 2021 de subvenciones del Programa para la Promoción de la Investigación científica, el desarrollo tecnológico y la innovación en la Comunitat Valenciana. Grupos consolidables, cuya investigadora principal es la Profra. Dra. Andrea Planchadell Gargallo.

Este capítulo forma parte de un libro sobre el Juez-Robot que estoy elaborando en estos momentos, cuyas líneas generales sobre el tema concreto de la creación de ese instrumento de Inteligencia Artificial consistente en una máquina de juzgar avanzo parcialmente ahora. Las fuentes bibliográficas extranjeras (alemanas y anglosajonas) pude consultarlas presencialmente en el *Institut für Strafrecht und Strafprozessrecht Abteilung 3: Deutsches und Ausländisches Strafrecht und Strafprozessrecht* de la *Rechtswissenschaftliche Fakultät* (*Albert-Ludwigs-Universität* de *Freiburg im Breisgau*, Alemania), dirigido por el Prof. Dr. Dr.h.c. Walter Perron, a quien agradezco profundamente su extraordinaria acogida y constante apoyo. También pude consultar mucha bibliografía en el *Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht* (antiguo *Max-Plank-Institut für ausländisches und internationales Stafrecht*), sito también en *Freiburg im Breisgau*. Mi agradecimiento a sus directores Prof. Dr. Ralf Poscher y Profra. Dra. Tatjana Hörnle, por aceptarme y permitir mi acceso, igualmente presencial, en estos tiempos de pandemia tan preocupantes. El acceso a la bibliografía italiana fue posible gracias a mi aceptación como investigador en el *Centro Interdisciplinare per l'Intelligenza Artificiale* y en el *Dipartimento di Scienze Giuridiche «Antonio Cicu»*, ambos de la *Università degli Studi di Bologna* (Italia). Mi agradecimiento a los Profs. Dres. Giovanni Sartor y Renzo Orlandi por su excelente acogida y apoyo. Ello fue posible gracias a la concesión de una beca de la Generalitat Valenciana – Programa BEST/2021 (julio a septiembre de 2021), a otra beca de la *Alexander von Humboldt-Stiftung* (*Wiedereinladung*, de octubre a diciembre de 2021), y a una tercera beca, finalmente, del Ministerio de Ciencia, Innovación y Universidades – Programa Salvador de Madariaga (julio a diciembre de 2022), instituciones todas ellas a las que igualmente quiero manifestar expresamente mi más profundo agradecimiento.

I. A MODO DE INTRODUCCIÓN

Una visión científica por no expertos del mundo de la Inteligencia Artificial[2], que empieza a despuntar en los años 50 del siglo pasado, pero que en realidad solamente a partir de finales del siglo XX se la ve pujar con fuerza en el mundo que nos rodea, se está abriendo paso para iluminar sobre aspectos concretos muy problemáticos de nuestra vida actual. Esa visión científica es jurídica, y afecta a la cuestión general de comprensión del fenómeno de la IA e intento de regulación legal de la misma, debido a que con su enorme desarrollo, empiezan a verse también, si no se han visto ya, los enormes peligros que encierra este nuevo mundo[3].

Es cierto que interesan otras visiones también, como la filosófica, en especial, la ética, la económica o incluso la perspectiva desde las ciencias de la salud. Pero son ajenas a nuestros intereses ahora. A nosotros lo que nos preocupa es la visión jurídica que tiene lugar desde el punto de vista procesal, y de todas las posibles cuestiones dentro de esa visión, de momento sólo una, en verdad, me llama poderosamente la atención. El problema que quiero abordar aquí, detectándolo, analizándolo, observando lo existente y proponiendo soluciones a los problemas planteados, dentro de la limitada extensión que un escrito de estas características me permite, es el de la viabilidad del Juez-Robot, específicamente si jurídicamente es posible su implantación en nuestro sistema judicial. Creo que es, sin duda, uno de los puntos estrella en estos momentos.

Pero es necesario antes comprender con carácter general el tema, siquiera sea en sus trazos más significativos[4]. Para lograrlo, es útil repasar las informaciones accesibles a la ciudadanía, de manera que sepamos exactamente cuál es el estado de la cuestión en estos momentos.

En este sentido, lo primero que hay que decir es que se habla mucho en los medios de información sobre IA, pero se constata que quienes han escrito en los *mass media* sobre inteligencia artificial y sus aplicaciones en la Justicia (organización, tribunales, procesos civiles y penales),

2. A partir de ahora, abreviada IA.
3. He advertido sobre ello en GÓMEZ COLOMER, J. L., *Ética, robots y proceso: sobre los límites en el uso de la inteligencia artificial*, en VELÁSQUEZ VELÁSQUEZ, F. / AMBOS, K. / LONDOÑO BERRÍO, H.-L. (Coord.) (2022), "Toda una vida por la vida. Libro Homenaje al defensor de los derechos humanos Jesús María Valle Jaramillo", Ed. Tirant lo Blanch – CEDPAL, Valencia, pp. 101 y ss., en donde comento la normativización ética que se cree conveniente asumir para evitar los evidentes riesgos y peligros que conlleva la IA.
4. No pretendo una cita exhaustiva de bibliografía, porque como se verá me voy a centrar en el Juez-Robot. Me limitaré a la escasa doctrina que en el tema tratado aporta al menos algo de interés.

específicamente los pocos que se han atrevido a hablar en concreto del juez-robot, no son cualquier ciudadano, son abogados, informáticos o periodistas especializados que se han adentrado en este mundo informando al público brevemente sobre diversos contenidos relacionados con la IA. Podemos decir que esta información transmite a toda la sociedad lo que una pequeña parte de ella piensa.

Ordenando las ideas expresadas acerca de estos temas, podemos resumir lo siguiente[5]:

1°) En general, todas las informaciones parten de considerar la introducción de la IA en el mundo de la Justicia como algo imparable, inevitable y positivo. Primero, porque el mundo del Derecho no puede ser ajeno a la enorme evolución tecnológica y considerable progreso científico que se manifiestan en otros mundos, como el de la Medicina, la Economía, la Ingeniería o la propia Administración, en los que la IA ocupa un papel cada vez más relevante[6]; y segundo, porque se constata, también paulatinamente, que la IA mejora aspectos de la Justicia sobre los que existe una gran preocupación social, como por ejemplo la rapidez de tramitación y resolución de los conflictos, un aspecto que lleva décadas enquistado provocando un caótico atasco judicial con dilaciones indebidas inasumibles. Esto es muy significativo, porque por culpa de la extrema lentitud de la Justicia una buena parte de la ciudadanía ha dejado de tener fe en ella, por ello, la aplicación de la IA para resolver este gran problema la hace muy atractiva.

2°) Toda la información habla de las ventajas e inconvenientes de la aplicación de la IA en la Justicia, en cualquiera de sus ramas, pero en donde más incidencia tiene es en la práctica ante los tribunales penales, por ser la más problemática.

3°) Las ventajas que se destacan son, principalmente, la enorme ayuda que implica para la descongestión judicial acabada de mencionar, porque los asuntos se resuelven rápidamente, la gran utilidad que significa para el juez manejar correctamente los datos y evitar que se pierda en montañas de papeles, y la nada menospreciable satisfacción de facilitar resoluciones justas e iguales en casos que son o idénticos o muy parecidos, lo que proporciona una gran seguridad jurídica.

5. Tampoco voy a citar ni a autores ni a medios concretos de información (prensa, TV o radio). Lo que aquí expreso se puede constatar fácilmente utilizando cualquier potente buscador en internet y haciendo la pregunta adecuada.

6. Por ejemplo, sobre la automatización de la administración alemana, procedimientos y decisiones, con base en la IA, v. MARTINI, M. / NINK, D. (2017), *Wenn Maschinen entscheiden… –vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz*, Neue Zeitschrift für Verwaltungsrecht– Extra In Zusammenarbeit mit der Neuen Juristischen Wochenschrift, núm. 10, pp. 1 y ss.

4°) Los inconvenientes son también claros, pues se reconoce principalmente que no es posible aplicar los avances en todos los campos del proceso, ni en todas las materias. Por ejemplo, en la línea problemática indicada, no lo ven apropiado para el proceso penal, aunque las aplicaciones se orientan principalmente a las predicciones (a tratar más adelante) para la adopción de medidas cautelares penales de naturaleza personal; tampoco lo consideran procedente para asuntos civiles de familia, en los que la decisión humana se entiende hoy como imprescindible ante la cantidad de problemas entrelazados que existen, la mayoría de los cuales requieren una sensibilidad y una emoción de la que carecen las "máquinas".

5°) En el ámbito de la Justicia civil y penal, también en los órdenes contencioso-administrativo y laboral, incluso en el militar, hay varios puntos sobre los que se quiere trasmitir a la sociedad alguna reflexión ulterior:

a) El primero hace referencia a la enorme utilidad de la aplicación de la IA en materia de predicciones judiciales, destacando dos aspectos:

1.– Un primer ámbito, aunque los campos pueden ser muchos, se centra sobre todo en los programas que hasta ahora se han construido y que mayor importancia tienen, Así por ejemplo, se suele citar mucho el programa COMPAS, diseñado en California en el año 1998, para predecir si un imputado o acusado por determinados delitos tiene un riesgo elevado de fugarse si se decreta su libertad provisional, con el peligro de reiteración delictiva que ello supone, hasta la espera del juicio, o si no lo tiene, de manera que con la ayuda de la predicción el juez pueda tomar una decisión más adecuada a la realidad del caso y de la persona que podría haber cometido el delito o los delitos que lo han provocado. Con relación a él se cita el *caso Loomis*, en 2013, que creó un precedente judicial en el estado de Wisconsin, Estados Unidos[7]. Pero hay muchos programas más, como PredPol, Precobs, Xlaw, Hart, Vaak, Cortica, o el español Eurocop, diseñado por mi universidad[8].

7. Véanse GRECO, L. (2020), *Poder de julgar sem responsabilidade de julgador: A impossibilidade jurídica do juiz-robô*, Ed. Marcial Pons, São Paulo, pp. 28 y 29; ARMENTA DEU, T (2021), *Derivas de la Justicia. Tutela de los derechos y solución de controversias en tiempos de cambios*, Ed. Marcial Pons, Madrid, pp. 262 y ss.; MIRANDA BONILLA, H. (2021), *Algoritmos y derechos humanos*, Revista de la Facultad de Derecho de México, tomo LXXI, núm. 280, pp. 720 y 721; MARTÍNEZ ZORRILLA, D. (2019), *El juez artificial: ¿próxima parada?*, Oikonomics, núm. 12, pp. 5 y ss.; y MIGUEL BERIAIN, I. de (2018), *Does the use of risk assessments in sentences respect the right to due process? A critical analysis of de Wisconsin v. Loomis ruling*, Law, Probability and Risk, núm. 1 (17), pp. 45 y ss.

8. Este programa pretende aumentar la capacidad predictiva, preventiva y operativa de la Policía, especialmente la Policía Local, de momento. Para lograrlo se creó mediante acuerdo entre la Universidad Jaume I de Castellón, el Ayuntamiento de Castellón y

2.– Un segundo ámbito de predicción que se está utilizando consiste en estudiar las sentencias dictadas por un juez, o por cada juez de un tribunal, o por el conjunto del tribunal, agrupando asuntos relativamente iguales durante un período de tiempo. Este análisis predictivo ayuda a los abogados en sus estrategias para intentar vencer la probable oposición psicológica de los jueces a sus intereses con relación a sus clientes, o para orientar mejor la argumentación hacia una victoria en el caso. Un programa desarrollado en 2016 por la Universidad de Londres, la Universidad de Sheffield y la Universidad de Pennsylvania para el estudio de casi 600 casos del Tribunal Europeo de Derechos Humanos, para ver si un algoritmo podía predecir el fallo con base en esos precedentes, llegó al sorprendente resultado de coincidir la predicción con la realidad posterior en casi el 80% de los casos[9]. No es el único estudio predictivo hecho[10].

b) El segundo se refiere a la posibilidad de que una máquina pueda juzgar. La enorme evolución tecnológica en esta materia está llevando más allá de las predicciones y se adentra en el delicado tema de las resoluciones judiciales, en definitiva, en estudiar si es posible que una computadora inteligente pueda decidir cualquier asunto litigioso civil o cualquier delito penal.

La idea central que preside este avance es, obsérvese que, en forma recurrente, pues hablamos casi siempre de lo mismo, aligerar el enorme colapso de los tribunales en todos los países democráticos, de manera que el ciudadano sienta de verdad que su derecho a la tutela judicial efectiva y a un proceso sin dilaciones indebidas sea respetado y amparado por el estado, el único ente que debe organizar el sistema judicial en una democracia.

Pero no es tan fácil, primero porque el avance tecnológico no ha llegado tan lejos, y segundo, porque, y en esto coinciden todos, nadie cree en

---

su Policía Local la "Cátedra Eurocop", con el fin de ayudar a resolver las necesidades que tienen los Cuerpos y Fuerzas de Seguridad, posibilitando que cuenten con las más avanzadas herramientas tecnológicas para predecir y prevenir delitos, infracciones, faltas, actos incívicos, etc. No es un programa ajeno a ciertas sensibilidades sociales que ven este tipo de usos atentatorio contra los derechos de los ciudadanos, v. https://www.lavanguardia.com/tecnologia/20190318/461013536935/inteligencia-artifical-vigilancia-predictiva-policia.html; y https://www.elsaltodiario.com/tecnologia/estado-policial-espanol-2.0-empresas-privadas-eurocop-vigilar-ciudadanos.

9. *Vide* ALETRAS, N. / TSARAPATSANIS, D. / PREOŢIUC-PIETRO, D. / LAMPOS, V. (2016), Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective, PeerJ Computer Science 2:e93, pp. 1 y ss.

10. Para la Corte Suprema de los Estados Unidos, v. RUGER, TH. / KIM, P. T. / MARTIN, A.D. / QUINN, K. M. (2004), *The Supreme Court Forecasting Project: Legal and Political Science. Approaches to Supreme Court Decision-Making*, Columbia Law Review, vol. 104, pp. 1150 y ss.

serio, al menos hoy en día, que desaparezca para siempre el juez humano de la vida judicial.

6°) Llegamos con estas reflexiones al juez-robot, sobre el que se ha escrito también, pero poco, quizás porque nadie cree, insistimos, al menos de momento, en que pueda ser realidad un día.

Pero dos países ya lo han empezado a implementar[11], y de ello se da cumplida cuenta en la escasa prensa que ha tratado el tema:

a) En Estonia, uno de los países más avanzados del mundo en esta materia, existe desde el año 2000 el juez-robot, que resuelve pequeñas reclamaciones civiles de cuantía hasta 7.000 €.

b) En China existen desde 2019 los llamados "Tribunales de Internet", o juzgados *online*, con competencias en litigios sobre comercio electrónico, pagos virtuales, transacciones en la nube y conflictos en materia de propiedad intelectual.

Los procesos se desarrollan de una manera ultrarrápida. Las partes únicamente proporcionan los hechos y las pruebas que tengan y la máquina mediante un sistema de algoritmos (basados en un complejísimo cálculo estadístico), dicta sentencia.

En ninguno de los dos países, sin embargo, la IA se ha apoderado totalmente del proceso. En primer lugar, sólo actúan en procesos civiles, y, en segundo lugar, proponen la decisión a un juez, quien debe revisar al procedimiento y ratificarla o no. Los recursos, de caber, se tramitan ante jueces "humanos".

En China han dado un paso más y han creado una máquina que actúa de Fiscal, encargado de acusar en algunos pocos delitos, generalmente de escasa dificultad probatoria, según los pocos datos que hasta este momento conocemos. El Fiscal-Robot está en pruebas en la gran urbe china de Shanghái. Es capaz de formular escritos de acusación contra sospechosos con base exclusivamente en una descripción verbal, con una precisión de hasta el 97% de acierto. De momento ha sido capaz de "comprender" ocho delitos: Fraude con tarjetas de crédito, juegos de azar, conducción imprudente, asalto intencional, obstrucción a un oficial, robo, fraude e incluso disidencia política.

7°) Finalmente, la ciudadanía es puesta al corriente de dos cuestiones negativas que el uso de la IA en el campo del Derecho Procesal implica: Se denuncian ciertos problemas éticos con la utilización de los programas

11. CÁRDENAS KRENZ, R. (2021), *¿Jueces robots? Inteligencia artificial y Derecho*, Revista Justicia & Derecho, Universidad Autónoma de Chile, vol. 4, núm.2, pp. 3 y 4.

de predicción, y se advierte sobre la posible colisión del uso de estas altísimas tecnologías con las constituciones democráticas y algunos de los derechos humanos (constitucionales) que reconocen.

a) El problema ético surge principalmente con relación a los programas de predicción porque los algoritmos, generalmente creados por empresas privadas, no se someten a información pública, es decir, nadie sabe cuál es su contenido, y no hay manera legal de obligar a la empresa a que lo haga público porque los resultados de su trabajo, el producto final, están protegidos por sus derechos de propiedad intelectual. Esto ha provocado en varios asuntos de gran trascendencia impugnaciones por parte de la defensa, cuando su cliente ha resultado perjudicado por la predicción, porque no se podía defender frente a un algoritmo "secreto".

Otra cuestión, no menor, ha sido que al no conocerse con qué criterios actúa el algoritmo, ni quién lo ha elaborado, no se puede saber si realmente la información que contiene es objetiva, imparcial, igualitaria y ajustada a la ley. De hecho, se ha demostrado que en algunos casos estos programas tenían sesgos claramente orientados a favor de la mayoría (*v.gr.*, de los ricos), e incluso prejuicios en favor de los blancos cuando los acusados eran negros, o en contra de personas que tenían alguna característica diferenciada que les perjudicaba, como la pobreza, el desarraigo, los antecedentes penales, etc. (*caso Loomis*, cit.).

b) El segundo tema es jurídico y atañe a la posible violación de determinados derechos constitucionales por el uso de estos programas de predicción, y también de resolución en el caso del juez-robot.

En líneas generales, se informa de los posibles derechos fundamentales afectados: Por ejemplo:

1.– Posible violación del principio de igualdad por los sesgos y prejuicios de determinados algoritmos causantes de discriminación.

2.– También puede quedar en entredicho el derecho de defensa, ya que no sabemos cómo "razona" la máquina.

3. El derecho al recurso, puesto que la máquina no motiva y por tanto la parte perjudicada no sabe por qué ha sido condenado.

4.– El derecho a un proceso equitativo o derecho al juicio justo (*Due Process of Law*, nuestro derecho al proceso con todas las garantías) puede quedar igualmente perjudicado, porque carece de sentido tanto hablar de competencia territorial, como hablar de audiencias y, por tanto, de los principios de oralidad e inmediación, entre otras muchas instituciones procesales que devienen superfluas o irrelevantes.

5.– El uso de la IA en temas de Justicia puede conllevar negativamente también, ante la enorme cantidad de datos que necesitan los programas hasta ahora creados para predecir o resolver, el aprovechamiento por parte de estados, entes o empresas poco escrupulosas de los mismos, para realizar paralelamente sobre la población una vigilancia masiva y total de su vida personal, profesional y social, sus costumbres, sus preferencias, sus pasiones, sus virtudes, sus gustos, sus logros, sus defectos, sus miserias, etc., lo que implicaría un control total que ni siquiera Orwell pudo llegar a imaginar. Derechos como la intimidad, la inviolabilidad del domicilio, el secreto de las comunicaciones, o el derecho a la protección de datos, estarían totalmente a disposición de esas personas jurídicas para un uso torticero público (o privado) de los resultados obtenidos como consecuencia de la búsqueda de información.

Para terminar con este repaso a la información que recibe la sociedad sobre la IA, destaco uno de los aspectos cruciales del sistema, a saber, el de la responsabilidad. ¿Quién se hará cargo de los posibles daños y perjuicios de una predicción errónea o de un fallo equivocado, ambos adoptados por una máquina de juzgar? Debe decirse que se ha pensado ya en el tema de la responsabilidad y que se han tomado en cuenta las Recomendaciones del Parlamento Europeo que afectan a una posible futura regulación de los robots[12], pero estamos empezando, por tanto, hay mucho que analizar.

En resumen, siendo ello así, dado que la IA sigue imparablemente su curso, no va a haber más remedio que cambiar muchas cosas para que las grandes estructuras, formadas por principios por los que mucha gente ha llegado a dar su vida a lo largo de la Historia, no se tambaleen y se destruyan definitivamente. Ello incluye, especialmente, toda la materia de los derechos fundamentales propios de un estado de derecho, los que conforman una democracia verdadera.

Todo ello gira en torno al Juez-Robot. A este interesante tema dedicamos las palabras siguientes, que conforman el núcleo central de esta contribución.

12. Informe de la Comisión de Asuntos Jurídicos del Parlamento Europeo con Recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, de 27 de enero de 2017 (A8-0005/2017), que se puede consultar en https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html; y Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica [2015/2103(INL)], que se puede consultar en https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html.

II. EL JUEZ-ROBOT

1. EN GENERAL

En primer lugar, me pregunto qué es el Juez-Robot. Es una máquina, obviamente, desde el punto de vista físico, y ello parece indubitado. Pero jurídicamente, ¿qué es? La respuesta ya no es tan clara.

Si atendemos a nuestra regulación básica, es decir, a nuestro Código Civil, observamos que el Juez-Robot no puede entrar en ninguna de las clasificaciones oportunas de forma irrefutable. El robot no es una persona física o natural (arts. 29 y 30 CC), pues ni es concebido, ni nacido, ni tiene vida autónoma; no es una persona jurídica (art. 35 CC), si bien al menos es algo artificial, una ficción, distinto a la persona natural, creado legalmente en forma independiente de sus miembros para cumplir determinados fines que las personas físicas por sí mismas no pueden o tienen muy difícil lograr; no es un animal, porque no es un ser vivo dotado de sensibilidad (art. 333 bis CC)[13], ni es un fruto (art. 355 CC), porque el robot no es un producto derivado de un bien industrial, sino una construcción artificial; ni tampoco es, finalmente, una cosa, o al menos no es sólo una cosa (art. 333 CC)[14], porque un bien mueble sí es, ya que es una cosa sin vida (propia autónoma) que es transportable y susceptible de apropiación (art. 335 CC).

Por tanto, en principio el robot, y, en consecuencia, el juez-robot, no es susceptible de ser encuadrado en ninguna de las categorías que distinguen jurídicamente a las personas de los animales, de los bienes y de las cosas. Parece algo distinto, no sólo por su novedad, sino también por su configuración y funcionalidad.

La moderna doctrina que estudia este tema formula varias propuestas. Un sector quiere que se considere a los robots como cosa (un bien mueble, que sería la cosa electrónica o el bien electrónico), otro que se cree una figura nueva, que sería la de la persona electrónica; otro en fin que se mantengan las cosas como están.

La discusión es relevante en varios sentidos. Los dos más importantes, que nos afectan directamente, serían por un lado la necesidad de aprobar un estatuto jurídico del robot, en el que se decidiría jurídicamente cuál es la naturaleza jurídica del robot y se fijarían las funciones que puede cumplir y las que no puede cumplir, lo que sería especialmente apropiado

13. Modificado por la Ley 17/2021, de 15 de diciembre de 2021, v. inmediatamente.
14. Modificado igualmente por la Ley 17/2021, de 15 de diciembre de 2021, v. inmediatamente.

para los robots diseñados para actuar como jueces; y de otro lado, si se toma la decisión de que es una persona nueva (la persona electrónica) o una cosa nueva (el bien electrónico), podríamos fijar las bases del espinoso tema de la responsabilidad en que puede incurrir la máquina, el juez-robot cuando, como consecuencia de la realización de sus funciones, produzca un daño evaluable económicamente a personas y cosas.

Pues bien, planteada así la cuestión, la opción que se está abriendo paso es la de crear la categoría de "persona electrónica", otorgando personalidad jurídica propia al robot. Ésa sería su naturaleza jurídica, dotándola de un estatuto jurídico propio, sólo que habría que reconocerla antes en España legalmente como categoría jurídica propia en la clasificación de las personas. Es la posición sostenida por la Unión Europea[15]:

> "f) crear a largo plazo una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan causar, y posiblemente aplicar la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente".

Y también la preferida de la doctrina que ha tratado el tema, no sin serias críticas[16]. Añado una cuestión que sin duda habrá que resolver: Si se reconoce a las máquinas inteligentes su naturaleza de persona electrónica y, en consecuencia, se procede a regular su responsabilidad, ¿tendrá también que reconocer la norma algunos derechos a los robots? Obsérvese que, si se le reconoce esta naturaleza, se crea un sujeto jurídico, como ahora con los animales ocurre en España específicamente[17], lo que significa que no es un absurdo plantearse el tema de sus derechos, que sólo el ser humano podrá crear, regular, hacer valer y defender, es decir, que no implicará la creación de un sistema jurídico autónomo, sino complementado por el que sirve a la persona, pero que en definitiva será propio para los robots[18].

---

15. *Vide* la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho Civil sobre robótica, cit. ap. 59, f). También VALENTE, L. A. (2019), *La persona electrónica*, Revista Anales de la Facultad de Ciencias Jurídicas y Sociales. Universidad Nacional de La Plata, núm. 49, pp. 1-30.
16. Véanse SANTOS GONZÁLEZ, M. J. (2017), *Regulación legal de la robótica y la inteligencia artificial: Retos de futuro*, Revista Jurídica de la Universidad de León, núm.4, p. 43; y NAVAS NAVARRO, S. (2017). *Derecho e inteligencia artificial desde el diseño. Aproximaciones. Inteligencia artificial*, en NAVAS NAVARRO, S. (Dir.) "Inteligencia artificial. Tecnología. Derecho", Ed. Tirant lo Blanch, Valencia, pp. 53 y ss.
17. Ley 17/2021, de 15 de diciembre, de modificación del Código Civil, la Ley Hipotecaria y la Ley de Enjuiciamiento Civil, sobre el régimen jurídico de los animales.
18. Derechos que se basarán en las conocidas tres leyes de la robótica de ASIMOV, a saber: 1.ª) Un robot no puede dañar a un ser humano o, por inacción, permitir que

2. LA LEGITIMIDAD DEMOCRÁTICA DEL JUEZ-ROBOT

Toda la organización judicial española está construida por nuestra Constitución en torno al concepto de legitimidad democrática. Significa que el Poder Judicial es uno de los tres poderes del estado, correspondiendo a los jueces por decisión del pueblo, el único que detenta la soberanía, la función de juzgar. Técnicamente significa que la potestad jurisdiccional se atribuye a las personas que reúnen los requisitos legalmente establecidos para ser jueces y juezas, en el país concreto en que la norma se tenga que aplicar.

Claro, ninguna norma ni constitucional ni ordinaria, por impensable en el momento de su redacción (en donde a lo sumo se podrían haber planteado los constituyentes si podría decidir el conflicto una persona jurídica, como sí lo hacen en el arbitraje), dice que los jueces son personas físicas o seres vivos, pero así se interpreta en España, en Alemania y en Italia, con base en el art. 117.1 CE ("La justicia… se administra… por Jueces y Magistrados…"), en el art. 92.1 de la Ley Fundamental de Bonn o *Grundgesetz* – GG ("El Poder Judicial es confiado a los jueces"), y en el art. 102, I de la *Costituzione* italiana – CI ("La función jurisdiccional la desempeñan magistrados"), respectivamente. La jurisprudencia, escasa por su obviedad, que ha tenido que pronunciarse sobre el tema, da por hecho que el juez al que se refiere la constitución es un ser humano, lo que excluye a las personas jurídicas como jueces y, ahora, ha de excluir también a la máquina inteligente[19].

Esta legitimidad democrática derivada de la soberanía popular fijada por la constitución operaría directamente sobre los principios de independencia e imparcialidad judicial, únicamente predicables de seres humanos jueces y, por ello, constituirían el núcleo esencial del fundamento en una democracia de su Poder Judicial.

Hasta aquí todo parece claro, pero no es sin embargo fácil de comprender la legitimidad democrática del Poder Judicial, porque no se trata sólo de explicar que los actos del poder político y del poder legislativo deben

---

un ser humano sufra daños; 2.ª) Un robot debe obedecer todas las órdenes que le den los seres humanos, excepto cuando tales órdenes entren en conflicto con la Primera Ley; y 3.ª) Un robot debe proteger su propia existencia, siempre que dicha protección no entre en conflicto con la Primera o Segunda Ley. Detalles sobre ello en GAEDE, K. (2019), *Künstliche Intelligenz – Rechte und Strafen für Roboter?*, Ed. Nomos, Baden Baden, pp. 37 y 38; y WALLACH, W. / ALLEN, C. (2009), *Moral Machines. Teaching Robots Right from Wrong*, Ed. Oxford University Press, New York, pp. 3 y 4.

19. Para Alemania, v. NINK, D. (2021), *Justiz und Algorythmen: über die Schwächen menschlicher Entscheidungsfindung und die Möglichkeiten neuer Technologien in der Rechtsprechung*, Ed. Duncker & Humblot, Berlin, cit., pp. 262 a 265.

encontrar fundamento en la propia voluntad del pueblo, de la ciudadanía, ya que los actos del poder judicial requieren de algo distinto, al no ser los jueces elegidos políticamente cada cierto tiempo, con participación directa del pueblo. Ese condicionante, y no es el único que prevén las constituciones pues hay muchas instituciones en las que la participación del pueblo no es directa, es la autorización que una ley democráticamente aprobada concede a otro poder del estado para organizar el Poder Judicial de determinada manera. No significa ello que no haya control del pueblo a través, por ejemplo, del Parlamento. Significa sólo que, por su esencia, la institución se organiza de otra manera, pero siempre democráticamente. Por tanto, si la ley ha sido aprobada por los ciudadanos libremente elegidos en votaciones libres por la ciudadanía, la ley es legítima desde el punto de vista democrático, y si esa ley afecta al poder judicial del país, el poder judicial de ese país goza de legitimación democrática.

El fundamento constitucional de estas afirmaciones sería el art. 1.2 CE: "La soberanía nacional reside en el pueblo español, del que emanan los poderes del Estado"; el art. 20.2 GG: "Todo poder del Estado emana del pueblo. Este poder es ejercido por el pueblo mediante elecciones y votaciones y por intermedio de órganos especiales de los poderes legislativo, ejecutivo y judicial"; y el art. 1, segunda frase CI: "La soberanía pertenece al pueblo, que la ejercitará en las formas y dentro de los límites de la Constitución".

Esto es sin duda alguna inaplicable al Juez-Robot. ¿Dónde está la intervención del pueblo, directa o indirecta en la fabricación y uso del algoritmo que permita juzgar y decidir conflictos? Ni siquiera podríamos hablar de una legitimación indirecta al aprobarse una ley que regulase el tema por un parlamento democrático, primero porque no existe, al menos todavía, y segundo porque si fuera el único impedimento, podríamos pensar en una posibilidad real de establecimiento, pero ya llevamos unos cuantos inconvenientes insuperables, y todavía nos quedan más, de manera que se puede afirmar que el Juez-Robot carece de legitimidad democrática en estos momentos. Es un razonamiento irrefutable: Si una máquina no puede ser juez en sentido constitucional, carece de legitimación democrática al no formar parte del Poder Judicial[20].

Cualquier intento de que juzgue una máquina se encuentra, por tanto, con el escollo insalvable de carecer de legitimidad democrática para ello, al menos, mientras esas constituciones democráticas no se reformen y lo admitan expresamente, por no ser el Juez-Robot una persona física, un ser vivo, en suma.

20. Lo razona con detenimiento NINK, D. (2021), *Justiz und Algorythmen*…, cit., pp. 323 a 330.

3. LA CONSTRUCCIÓN Y PROGRAMACIÓN DE LA MÁQUINA DE JUZGAR

La evolución de la IA ha llevado a pensar si es posible construir un ordenador que pueda decidir un litigio civil o una causa penal respondiendo de forma clara y contundente a las preguntas que se le formulen y tomando una decisión incontestable, es decir, yendo más allá del puro almacenamiento y tratamiento de datos e información, en suma, si es posible construir una máquina de juzgar equivalente al ser humano.

Todo nació con la Jurimetría a principios de los años 60 del siglo pasado[21]. Se trataba de "calcular" el Derecho. Se comenzó por estudiar la predicción de sentencias y el comportamiento de los jueces, para lo que la colaboración de la psicología fue decisiva. También ayudó mucho la mejora de la investigación documental, de manera tal que empezaron a estudiarse las sentencias judiciales partiendo de su vocabulario.

Se construyó así una máquina de informar como primer paso para llegar a una máquina de juzgar. El hecho que, desde la cibernética, la informática y la jurimetría se haya llegado a esta situación, no quiere decir sin embargo que no podamos preguntarnos si se justifica su existencia, es decir, si es necesaria su creación[22].

Desde luego, hay que decir ante todo que no se ha llegado todavía a crear una máquina que juzgue de verdad, aunque China y Estonia están en ello, como hemos mencionado al principio. China incluso, además del Juez-Robot, ha creado el Fiscal-Robot. El Juez-Robot, si llega, está todavía muy lejos, por lo que parece que de momento no tengamos que temer que nos pueda juzgar una máquina. Además, recuerdo también, que esos ejemplos de China (tribunal de internet y fiscal electrónico) y Estonia (juez-robot) son engañosos, porque la decisión final la toma un juez humano (en Estonia al menos la apelación es humana).

Pero su justificación es otra cosa, porque se ha comprobado que las máquinas de juzgar, en su formato actual, están cumpliendo un papel

21. BOURCIER, D. (2003), *Inteligencia artificial y Derecho*, Ed. UOC, Barcelona, p. 18.
22. BOURCIER, D. (2003), *Inteligencia artificial y Derecho*, loc. cit.; GUZMÁN FLUJA, V. (2017), *Sobre la aplicación de la inteligencia artificial en la solución de conflictos (Reflexiones acerca de una transformación tan apasionante como compleja)*, en BARONA VILAR, S. (ed.) "La justicia civil y penal en la era global", Ed. Tirant lo Blanch, Valencia, pp. 69, 79 y 97; NIEVA FENOLL, J. (2018), *Inteligencia artificial y proceso judicial*, Ed. Marcial Pons, Madrid, p. 99; PÉREZ ESTRADA, J. (2019), *El uso de algoritmos en el proceso penal, y el derecho a un proceso con todas las garantías*, en BARONA VILAR, S. (ed.), "Claves de la Justicia Penal", Ed. Tirant lo Blanch, Valencia, pp. 237 y 247.

importante en determinados aspectos que implican tener que tomar decisiones judiciales, como, por ejemplo, citados anteriormente, la prisión preventiva, la fiabilidad de un testigo o el peligro de reincidencia.

La máquina de juzgar está proporcionando al juez, que es quien decide si impone la medida cautelar de prisión preventiva a un investigado, los datos necesarios para decidir si cree o no a un testigo, o si niega la libertad condicional a un preso por existir peligro de reincidencia, ofreciendo datos suficientes para hacerlo, es decir, se está comportando todavía como una máquina de informar, como una asistente en la toma de decisiones.

Igualmente está resultando muy útil en los juicios más frecuentes en la práctica, tanto civiles, como penales, también para toma de decisiones, puesto que, aunque formalmente la resolución la adopta, y motiva, un juez, la solución la da la máquina. En lo civil son de citar los procesos monitorios de cuantías pequeñas o medianas sin oposición del deudor, mientras que en el proceso penal podemos poner como ejemplo válido los llamados juicios penales de tráfico por delitos contra la seguridad vial (alcoholemias v.gr.), muy sencillos y generalmente con prueba de cargo irrefutable.

¿Cuál es el problema entonces? El problema es la confiabilidad de su información, porque si el juez no hace caso de las respuestas que da la máquina, para qué la ha consultado. Se produce así la falacia de que el juez sólo hace que ratificar lo que la máquina ha informado, no en la condena o absolución, ciertamente, pero sí en cuestiones y momentos que pueden influir decisivamente más tarde en una u otra. ¿De qué grado de independencia disfruta el juez o tribunal en estos casos?[23]

Tres temas más concretos me preocupan ahora, todos con difícil solución. Primero y positivamente, la importante ayuda que se espera del Juez-Robot en el funcionamiento de la Justicia; segundo, y negativamente, el engaño que se produce al considerar su papel irrelevante en el contexto general. Finalmente, el sempiterno problema del costo económico.

23. Véanse BATTELLI, E. (2021), *La decisión robótica: Algoritmos, interpretación y justicia predictiva*, Revista de Derecho Privado (Colombia), núm. 40, pp. 45 y ss.; QUATTROCOLO, S. (2018), *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, La legislazione penale, en http://www.lalegislazionepenale.eu/wp-content/uploads/2019/02/Carta-etica-LP-impaginato.pdf.; y UBERTIS, G. (2020), *Intelligenza artificiale, giustizia penale, controllo umano significativo*, Sistema Penale, 11 de noviembre, accesible en https://www.sistemapenale.it/it/articolo/ubertis-intelligenza-artificiale-giustizia-penale-controllo-umano-significativo, pp. 1 y ss.

3.1. El problema de la enorme sobrecarga judicial en la Justicia local

La venta política del Juez-Robot es segura y dará muchos beneficios. Se afirma por todos aquéllos que han tratado el tema de la IA que, en el mundo jurídico y en particular en el judicial, es de inestimable ayuda para agilizar los procesos, facilitar el desarrollo procedimental, eliminar trámites innecesarios, reducir plazos y simplificar la prueba. En suma, es de enorme utilidad para descongestionar a nuestros sobrecargados tribunales de Justicia y así, eliminando dicha sobrecarga, contribuir a una pronta Justicia, más rápida, más eficaz, más justa, en definitiva.

El problema de la sobrecarga judicial, del atasco permanente de los juzgados y tribunales es prácticamente universal, especialmente en las democracias occidentales. Cierto que algunos países la sufren más que otros, pero ninguno está satisfecho con este tema.

Pensar en una máquina de juzgar no es una meta en sí mismo, pero sí es la consecuencia y aprovechamiento de una evolución, lo que hace al problema y a su resolución más identificable y, por tanto, de mejor comprensión. Nadie pensó cuando empezó el desarrollo de la IA en crear una máquina de juzgar. Como hemos destacado, se pensó en proporcionar instrumentos de ayuda para organizar bases de datos confiables y más tarde en desarrollar tecnología que permitiera predecir determinadas conductas de influencia en la sentencia o patrones deducidos de sentencias ya dictadas. La meta no era la de juzgar electrónicamente, sino ayudar para un mejor desarrollo del proceso. La evolución llevó a aprovechar todos los avances de la IA y así se pensó en un Juez-Robot.

Por tanto, hoy existe acuerdo general en considerar que la introducción de la máquina de juzgar contribuirá indubitadamente a reducir, en determinados ámbitos de manera drástica, la sobrecarga judicial[24]. No sólo es un tema jurídico, también lo es moral, aunque su importancia, de hecho, radica en ser en nuestras sociedades principalmente un tema constitucional, porque afecta al derecho de acceso a la Justicia: ¿Qué es preferible, que un ciudadano tarde 10 años en obtener Justicia, que *de facto* es una injusticia porque ante esa realidad esa persona muy probablemente huya de la Justica y renuncie a ella, o permitir que una máquina la imparta en cuestión de minutos?[25] Es la visión positiva del problema.

---

24. Un dato periodístico informaba en 2019 que en España la IA ahorraría a los jueces una cuarta parte de su trabajo, v. VozPópuli en https://www.vozpopuli.com/economia_y_finanzas/robots-ahorrarian-cuarta-parte-trabajo-jueces-espanoles_0_1260174449.html–.
25. SUSSKIND, R. (2020), *Tribunales online y la Justicia del futuro*, Ed. La Ley-Wolters Kluwer, Madrid, p. 336.

3.2. La falacia de pensar en los asuntos pequeños, irrelevantes o sencillos

Pero estos avances tienen también una visión negativa, consistente en partir de un engaño difícil de detectar como tal. Me explicaré: Hasta ahora, la venta del producto "máquina de juzgar" o "Juez-Robot", se hace indicando primero que está en fase de pruebas, lo que es lógico, y segundo, aplicado sólo a asuntos pequeños, irrelevantes o sencillos.

Todo empieza con la afirmación de que la intervención de la máquina de juzgar consiste, previo acuerdo de las partes, en dictar una resolución fuera del ámbito extrajudicial, por ejemplo, en el arbitraje, en la conciliación o en la mediación, siempre en materia de Derecho privado y tratándose de derechos subjetivos disponibles, en asuntos de pequeña cuantía, por ejemplo, la reclamación de una pequeña deuda de 100€, o de fácil solución al no necesitar prueba o ser esta de muy fácil obtención, por ejemplo, un juicio monitorio sin oposición del deudor, antes citado, o muy repetitivos, como reclamaciones en materia hipotecaria. En lo penal se trataría de aplicarlo a casos en los que existe conformidad con la pena o a los delitos leves, que en ningún caso están castigados con penas privativas de libertad (juicios por delitos de tráfico, también citados *supra*).

La falacia, el engaño, está en el enfoque. Porque si tiene éxito el Juez-Robot en estos casos, se intentará extender y ampliar a otros no tan sencillos, con el argumento irrefutable de que ha funcionado y sería por tanto una irresponsabilidad no seguir luchando contra la sobrecarga judicial restante.

Pero el enfoque correcto no es ése, sino a qué precio constitucional estamos eliminando la sobrecarga judicial. Este tema no es propio del Juez-Robot, de hecho, es bastante antiguo, porque en el fondo es el mismo debate que se produjo cuando se empezaron a introducir en procesos penales de la Europa continental determinadas "ventajas" anglosajonas ancladas en el principio de oportunidad, como las alternativas a la persecución o las negociaciones sobre la declaración de culpabilidad, o incluso la propia justicia transaccional.

El punto central por tanto es si estamos dispuestos a negar principios esenciales de la constitución democrática por la que tantos seres humanos han luchado, muchos incluso han dado sus vidas, renunciando a principios que jamás deberían desaparecer ni de nuestras leyes ni de nuestra práctica, a cambio de aligerar la Justicia civil o penal y conseguir juicios más rápidos. Ésa es la cuestión.

En mi opinión, de momento el Juez-Robot vulneraría el estado democrático de derecho, la independencia judicial, la imparcialidad judicial y

el principio del juez legal. Vulneraría otros más, como podremos observar más adelante, pero ahí están cuatro sin los que la Revolución Francesa habría sido una rutinaria pelea de barrio.

Mi respuesta por tanto es negativa. A ese precio no quiero acabar con la sobrecarga judicial. Hay que dar alas a la imaginación y buscar otras vías de solución.

3.3. El costo no es el problema

Puede pensarse que la introducción de la Justicia digital conllevaría costos enormes para el estado que, en épocas de crisis (pero siempre estamos en crisis), no puede asumir. Para el poder político es más fácil reducir la planta y demarcación judiciales, con la supresión de plantilla que implica, que aumentarla.

Pero también se puede pensar que la introducción de la Justicia robotizada conllevaría reducción de costes porque, por esto mismo, implicaría reducción de plantilla.

Ambas cuestiones son relativas[26]. Mientras no se hagan estudios rigurosos sobre el gasto público que implicaría la introducción de la Justicia robótica en el sistema judicial, cualquier opinión, además de subjetiva, es puramente especulativa. Una cosa es que se rechace su introducción si se acredita que el costo es desorbitado y otra cosa es que se rechace porque se intuye no barata.

En cualquier caso, debe primar el derecho constitucional de acceso a la Justicia del ciudadano y, siendo deseable obviamente que la introducción del Juez-Robot implique el menor coste posible, el argumento económico no puede ser decisivo para adoptar una decisión a favor o en contra del mismo. Se trata de eliminar cuantas más injusticias mejor y de mejorar la Justicia[27].

III. LOS DAÑOS COLATERALES

El reconocimiento legal del Juez-Robot produciría además muchos daños colaterales irreparables. Estos daños colaterales, la mayoría, no

26. Véanse las reflexiones al respecto para Colombia, un país con relevantes dificultades económicas y gran congestión judicial, de RINCÓN CÁRDENAS, E. / MARTÍNEZ MOLANO, V. (2021), *Un estudio sobre la posibilidad de aplicar la inteligencia artificial en las decisiones judiciales*, Rev. direito GV 17 (1) Brazil, también en https://www.scielo.br/j/rdgv/a/vZDXYYPRrcwgsgJDWQf97QG/abstract/?lang=es, pp. 8 a 12.

27. Véase SUSSKIND, R. (2020), *Tribunales online y la Justicia del futuro*, cit., pp. 214 y 215.

todos, tienen que ver directamente con la independencia y con la imparcialidad (las predicciones, los presupuestos procesales del órgano jurisdiccional, la práctica y valoración de la prueba y la responsabilidad), y nos llevan a formularnos necesariamente una pregunta que debemos hacernos en nuestra investigación y que, podríamos decir, afecta a toda la constelación procesal, o si se prefiere, es su piedra filosofal: ¿Vulneran dichos daños, destrozándolo, el principio del debido proceso legal, llamado en España el derecho al proceso con todas las garantías, o en Europa el derecho al proceso equitativo o justo?

Si por lo visto parece que la respuesta puede ser positiva, nuestra obligación como juristas es estudiar la realidad y sus causas, ver la manera de resolver los problemas que se plantean y formular las propuestas de solución legal que nos parezcan más aceptables.

Enumero ahora, intuitiva y brevemente, los siguientes daños colaterales:

1. DESAPARICIÓN DE LA EQUIDAD

Ya no sería posible resolver litigios no con base en legislación, sino con base en lo que el juez crea más justo, dando a cada uno lo que merezca. Dado que la equidad está en la base del Derecho Romano, y de ahí ha pasado a todos los derechos continentales (con poca influencia en el Derecho Procesal Civil español y ninguna en el Derecho Procesal Penal, la verdad, pero sí en el arbitraje), y también y especialmente al anglosajón, su supresión obligaría a cambiar a pesar de ello algunos aspectos esenciales del sistema, porque una máquina no puede saber lo que es la equidad.

2. USO TORTICERO DE PREDICCIONES

Ya existen programas informáticos, como hemos dicho, que se utilizan para predecir posibilidades de éxito de demandas y querellas en función de datos e informaciones relativos a los hechos, a las decisiones previas de un juzgado o tribunal, o a las características personales y profesionales de los jueces y magistrados. Como siempre se puede ir más allá, quién asegura que este conocimiento predictivo no se pueda utilizar malintencionadamente para evitar o favorecer que los asuntos sean conocidos por jueces "preseleccionados". Desde luego, se violaría el principio del juez legal (art. 24.2 CE). Pero también, y esto es muy grave, se haría inútil la función de la jurisprudencia desde la entrada en vigor de la máquina, así como la adaptación de la norma a la realidad

histórica en la que se tiene que aplicar, porque siempre se resolvería conforme a datos e informaciones ya existentes, es decir, siempre se resolvería conforme al pasado.

3. RECONSIDERACIÓN RADICAL DE LOS PRESUPUESTOS PROCESALES

Así es, los presupuestos procesales como hoy los entendemos carecerían de sentido. Indudablemente, la jurisdicción, la competencia genérica, y los criterios objetivo, funcional y territorial no podrían ni regularse ni exigirse como hoy hacen la LOPJ, la LEC y la LECRIM. Una única máquina los controlaría todos, sita Dios sabe dónde (la competencia territorial sería irrelevante). El mantenimiento de los presupuestos procesales de las partes, capacidad legitimación y postulación, sería necesario, pero su concurrencia o no se decidiría en décimas de segundo por la máquina de juzgar, no haciendo ninguna falta audiencia saneadora alguna porque la máquina diría inmediatamente dónde está el fallo y qué debe hacerse. En cuanto a los actos procesales, la concurrencia de los presupuestos generales y concretos que afectan a cada acto se controlaría automática e inmediatamente.

4. PÉRDIDA DE SENTIDO DE MUCHOS ACTOS PROCESALES

Aspectos que hoy nos parecen esenciales y que consideramos con razón una conquista de Estado de Derecho, carecerían absolutamente de relevancia. No tendrían sentido las audiencias o vistas interlocutorias, ni el juicio oral, porque el principio de oralidad habría pasado a mejor vida.

5. PRÁCTICA INVISIBLE DE LA PRUEBA

Al no tener que explicar las razones probatorias, es decir, al no tener que valorar la prueba, ¿para qué practicarla? Una máquina lo haría por el juez, si a eso se le puede llamar práctica. Por otra parte, las nuevas teorías sobre los indicios pasarían rápidamente a la historia procesal, porque con la automatización en el tratamiento de datos y de la información perderían el sentido modulador que hoy tienen, lo que podría llevar a sentencias muy injustas[28].

28. GÓMEZ COLOMER, J. L. (2021), *El indicio de cargo y la presunción judicial de culpabilidad en el proceso penal*, Ed. Tirant lo Blanch, Valencia, pp. 27 a 30.

6. EL PRINCIPIO DE ORALIDAD, INNECESARIO

Una de las luchas jurídicas más importantes de la Historia, conocer cómo trabajan los jueces y controlar su aplicación de la ley, únicamente posible a través de la inmediación y la publicidad, principios que se derivan del tronco común llamado principio de oralidad, el principio clave del moderno procedimiento procesal, sea civil, sea penal, dejará de tener sentido. Volveremos al pasado, a no ser que se establezcan mecanismos de control que permitan llegar a efectos similares, lo cual en estos momentos no alcanzo a ver con claridad.

Muchos mandatos constitucionales, como nuestro art. 120.3 CE, serán irrelevantes. El algoritmo decidirá en secreto y, en realidad, sin procedimiento alguno, al menos conceptualmente comparable a lo que hoy entendemos por procedimiento judicial.

Tenemos que estar preparados para ello, pues se trata de aceptar que renunciamos a una conquista democrática, cuyos factores positivos se han acreditado indubitadamente en la práctica, que al ser humano ha costado siglos de ganar.

7. IRREMEDIABLE DESAPARICIÓN DEL JURADO

El mundo anglosajón, especialmente los Estados Unidos de América, es sin duda el que más está investigando en materia de IA y, en particular, en la creación de una máquina de juzgar lo más perfecta posible. En lo jurídico, es el mundo también más juradista que existe. ¿No se han parado a pensar allende los mares que la instauración del Juez-Robot acaba con el Jurado?

Es evidente que no lo contemplan de este modo, porque son conscientes de que, de ser así, necesitarían una reforma constitucional, imposible de aprobar en estos momentos en los Estados Unidos por razones políticas. Lo afrontan pragmáticamente fijándose sobre todo en casos civiles en los que el Jurado no forma parte del tribunal (la inmensa mayoría de todos ellos), y en los penales en temas en los que la constitución del Jurado no es posible, por ejemplo, para dictar la orden de prisión provisional. De esta manera soslayan el problema y se convencen de que el Juez-Robot y el Jurado no se cruzan en sus caminos.

Pero que nadie se llame a engaño. Si se generalizara un día el Juez-Robot, la constitución del Jurado (actualmente en el 5% de los casos delictivos que han dado lugar a la apertura de una causa penal), sería innecesaria absolutamente y, por tanto, la máquina habría acabado con él.

8. NUEVA PLANTA Y DEMARCACIÓN DEBIDAS A UNA REORGANIZACIÓN DE JUZGADOS Y TRIBUNALES

Qué duda cabe, finalmente, que si se introduce el Juez-Robot, una nueva configuración orgánica de los juzgados y tribunales españoles será necesaria, afectando a su planta y demarcación.

De entrada, debería bastar con un robot centralizado para tratar todos los asuntos. No me imagino a las alturas de desarrollo de la IA ya en estos momentos, un robot en cada Audiencia Provincial o TSJ. Esto significa que el criterio de atribución de la competencia territorial desaparece por completo.

Pero organizar el recurso de apelación no será fácil, porque entonces el único criterio seguro va a ser el de la competencia territorial. Si el Robot decidió en primera instancia en la nube un conflicto surgido en San Sebastián, la apelación debe ser competencia de un juzgado de San Sebastián o de la Audiencia Provincial de San Sebastián. Lo mismo en cuanto al *forum comissi delicti*. Cometido el delito en Morella, el Robot en la nube decidirá en primera instancia lo procedente, pero la apelación será competencia de los juzgados y tribunales de Castellón.

No entro, conscientemente, en los complejos problemas que se producirán en cuanto al tratamiento de fondo de los motivos de los recursos, por ejemplo, en infracción procesal o en casación (y también en una apelación paracasacional), ni tampoco en el callejón sin salida que puede plantearse en su caso ante un posible proceso de revisión o de anulación. Porque, si la decisión del robot no es motivada, ¿servirán de algo los recursos?

IV. CUESTIONES ORGANIZATIVAS IRRESOLUBLES QUE DEBEN RESOLVERSE

Para finalizar, debo abordar desde el punto de vista interno, por tanto, exclusivamente español, algunas cuestiones de organización que hoy son, sencillamente imposibles de resolver, pero que no habrá más remedio que abordar y solucionar.

Llamo la atención del lector porque puede parecer que lo que trato a continuación es ridículo, incluso motivador de risas o, más gravemente, de mofas. Pero nada más alejado de mi intención. Si estamos hablando de un juez, aunque sea una máquina, habrá que incardinarlo en el mundo judicial. Esto deben entenderlo los expertos en IA, por muy absurda que les pueda parecer la cuestión (o por muy simple), ya que existen reglas,

muchas de ellas del máximo nivel, que impiden que ellos (los informáticos) pueden cambiar el mundo a su antojo.

Es por tanto necesario preguntarse, e intentar resolver, varias cuestiones:

1. ¿ESTARÁ EL JUEZ-ROBOT BAJO LA TUTELA DEL CONSEJO GENERAL DEL PODER JUDICIAL?

Es evidente que el Juez-Robot es una máquina, por tanto, la organización de los jueces que son máquinas, hecha obviamente por el ser humano, debe contemplar dónde se ubican y de quién dependen. En España la única posibilidad sería, con todas las reformas legales que ello implicaría, crear una sección específica para los robots en el seno del Consejo General del Poder Judicial.

Una sección creada con idéntico fin en el Ministerio de Justicia rompería el equilibrio constitucional entre los tres poderes del estado, si finalmente la máquina de juzgar, juzgara. Mientras asesorara o hiciese una propuesta pre-procesal no pasaría nada irresoluble, ni siquiera grave, pero si tomara decisiones, aunque hubiesen sido previamente consensuadas por las partes, con nuestra Constitución en la mano no tendrían cabida política en el Gobierno, sino que deberían estar incardinados en el órgano que tutela y protege el funcionamiento correcto de los órganos judiciales, el Consejo General del Poder Judicial.

Hoy por hoy resultan inimaginables todas las consecuencias orgánico-procesales que ello conllevaría, porque por mucho que se intentara asimilar el régimen organizativo de los jueces humanos al de las máquinas, en el fondo nada cuadraría y todo tendría que ser innovado, y, por tanto, muy distinto. Pretender regular la planta y demarcación judiciales, el régimen de ingreso y ascenso, la provisión de plazas, la propia organización de los Jueces-Robot, la constitución de los juzgados y tribunales de IA, sus órganos de gobierno interno, la inspección de tribunales, el nombramiento y posesión, honores y tratamientos, los derechos y obligaciones de los Jueces-Robot, las sustituciones, las vacaciones, etc., etc., resulta hoy por hoy impensable. Decidir tajantemente, por el contrario, que nada de ello puede ser aplicable a los Jueces-Robot, suena a solución demasiado fácil y, por tanto, probablemente errónea, porque en el desarrollo de las normas orgánico-procesales hay muchos principios implicados, algunos de ellos de naturaleza constitucional, que afectan a las partes en conflicto y no sólo a la organización de los tribunales, como el principio de la independencia judicial, que necesariamente deben ser abordados.

Habrá que decidir muchas cuestiones, nada simpáticas o que den risa. Se me ocurren las siguientes: Cuántos Jueces-Robot habrá, dónde se instalarán, quién será su operador directo si no es el Letrado de la Administración de Justicia, qué sistema de homologación de la máquina será el válido, cada cuánto deberán revisarse las máquinas, qué hacer en caso de avería o sustitución sin haberse decidido el conflicto, de cuántos años de vida activa gozarán, cómo se coordinarán entre sí si hay varios, cómo se garantizarán el principio de contradicción y el principio de publicidad en las notificaciones procesales cuyo origen sea el Juez-Robot, qué sistemas de control se activarán para garantizar en todo momento su correcto funcionamiento, etc.

2. ¿QUÉ PARTICIPACIÓN TENDRÁN LAS COMUNIDADES AUTÓNOMAS?

No es un tema nimio. En España las Comunidades Autónomas no poseen un Poder Judicial propio, a diferencia de los otros poderes del estado, que sí los tienen (el legislativo y el ejecutivo). Esto ha llevado a muchas tensiones, aunque el diseño constitucional se aprobara mediante referéndum de resultado incontestable en 1978[29]. Decidir acertadamente sobre ellas no era nada fácil, al final tuvo que ser la Justicia y no la Política quien delimitara los campos de actuación.

En efecto, Fruto importante de la discusión fue imaginar una distinción entre "núcleo esencial del Poder Judicial", en el que sólo el Estado puede intervenir mediante ley orgánica, y "administración de la administración de Justicia", en la que las Comunidades Autónomas pueden tener participación en el Poder Judicial del estado, a veces incluso sin necesidad de ley alguna. Esta distinción, un tanto forzada, establecida por nuestro Tribunal Constitucional hace ya muchos años[30], implica en la realidad que la intervención de las comunidades autónomas en el Poder Judicial del estado es mínima, centrada, salvo en aquellos aspectos fijados constitucionalmente como la proposición de la capitalidad de los partidos judiciales (art. 152.1, II CE y art. 35.6 LOPJ), en aportación de recursos materiales y personales no incardinados en el Consejo General del Poder Judicial para que los juzgados como organización administrativa puedan funcionar mejor. Pero

29. Véase GÓMEZ COLOMER, J. L. (2012), *Independencia judicial y diseño político del Estado*, en GÓMEZ COLOMER, J. L. / BARONA VILAR, S. / CALDERÓN CUADRADO, P. (coord.), "El Derecho Procesal español del siglo XX a golpe de tango. Juan Montero Aroca. Liber Amicorum, en homenaje y para celebrar su LXX cumpleaños", Ed. Tirant lo Blanch, Valencia, pp. 346 a 358.

30. Véanse las SS TC 56/1990, de 29 de marzo (FJ 1, B), y 62/1990, de 30 de marzo (FJ 1, B).

no tienen ni una sola participación en temas de impartición de Justicia, es decir, de ejercicio de la función jurisdiccional (juzgar y hacer ejecutar lo juzgado, art. 117.3 CE), porque éste es el núcleo esencial.

¿Qué papel quedaría reservado a las Comunidades Autónomas si se creara el Juez-Robot? Porque la experiencia y los datos históricos, basados en hechos reales, demuestran que las Comunidades Autónomas van a querer ocupar espacios de poder allá en donde existan en detrimento de los del estado, lo que significa que, si estas cuestiones no se regulan bien, tendremos jueces-robot catalanes, vascos, gallegos, navarros, valencianos, etc.

Al ser su naturaleza no humana, la doctrina del núcleo esencial debe revisarse, porque con la Constitución en la mano, las comunidades autónomas tendrán derecho legítimo a participar en este poder bajo el que se incardina el Juez-Robot, ya que se trata de inversiones, de dinero, de recursos materiales, en definitiva. Dicho de otra forma, si no se previenen con tiempo estas cuestiones, hoy por hoy la Comunidad Autónoma tiene derecho, si no lo hace todo ello por sí misma, a contratar al programador, a encargar la elaboración del algoritmo, a elegir al fabricante de la máquina, a proveer para que se ponga en funcionamiento, a rodearla de los instrumentos necesarios para que funcione correctamente y a ofrecer respuestas a las partes en conflicto. También puede el estado, pero no está expresamente excluido que no puedan las comunidades autónomas, porque ni la Constitución ni las sentencias del Tribunal Constitucional citadas les son, ante la nueva situación, de aplicación.

Habrá que llegar por tanto a acuerdos políticos del más alto nivel, solución preferida a tener que esperar a ver qué decide al respecto, una vez más, nuestro Tribunal Constitucional.

3. ¿SERÁ NECESARIO UN ESTATUTO JURÍDICO DEL JUEZ-ROBOT?

No tengo ninguna duda que habrá que regular, al menos, los mínimos de organización y funcionamiento de los jueces artificiales, si la opción de futuro es que puedan tomar decisiones judiciales vinculantes para las partes.

Este tema está relacionado con el abordado en primer lugar (tutela del Juez-Robot por el Consejo General del Poder Judicial) y surge, porque el art. 122.1 CE obliga a que los jueces y tribunales que no conforman órganos jurisdiccionales especiales salvados por la propia CE, tengan un estatuto jurídico propio.

En este sentido, habrá que fijar preliminarmente quién los gobierna, sin duda un ser humano o grupo de seres humanos, y cómo los gobiernan. Los primeros pueden ser una pequeña comisión formada por vocales del propio Consejo General del Poder Judicial a cuya cabeza estaría, obviamente, el presidente. Pero cómo va a gobernar esa comisión ya no es tan claro, porque al tratarse de máquinas las disposiciones de la Ley Orgánica del Poder Judicial resultan inaplicables en su gran mayoría. Por eso sería necesario que esa comisión fuese mixta, es decir, formada por miembros del Consejo General del Poder Judicial y por expertos en IA (informáticos, estadísticos, programadores, empresarios del sector, etc.).

Lo relevante en estos momentos es que, si finalmente se pensara en Jueces-Robot que decidiesen conflictos, sería necesario elaborar una serie de normas que regulasen su organización y funcionamiento grupal e individual, de manera que en mi opinión la obligación de redactar un estatuto jurídico para los mismos sería insoslayable.

Dicho estatuto jurídico debería contemplar los siguientes aspectos:

1.º) Qué máquinas pueden concurrir a un procedimiento público de homologación como Jueces-Robot;

2.º) Qué requisitos técnicos deben concurrir para su homologación por el Consejo General del Poder Judicial;

3.º) ¿Qué sistema de homologación sería el más adecuado y como operaría el procedimiento de homologación?

4.º) ¿Quién formará parte de la comisión técnica, que podría ser distinta de la ya aludida, que habrá que crear para asesorar al Consejo General del Poder Judicial en esta materia en concreto, sin perjuicio de otras funciones?

5.º) ¿Cómo se configurará la estructura orgánica de los Jueces-Robot? ¿Habrá sólo una máquina de capacidad gigante en la capital del estado, o una de capacidad más reducida en la capital de cada comunidad autónoma, o una de capacidad más adaptada en la capital de cada provincia., etc.?

6.º) ¿Cómo se coordinarán esas máquinas entre sí, si fuera necesario, por ejemplo, para evitar litispendencias o cosas juzgadas, o para favorecer acumulación de pretensiones o de procesos?

7.º) ¿Habrá que salvaguardar el principio de inamovilidad judicial, no sea que a alguien se le ocurra cambiar la máquina de lugar (y quizás con ello de competencias), a su gusto?

8.º) ¿Cómo garantizaremos su independencia concretamente, el tema clave?

9.º) ¿Cómo fijaremos en concreto la exigencia de responsabilidad a la máquina judicial que cause daños?

Habría obviamente, muchas más cuestiones a tratar. Es posible que un ingeniero informático, o un experto en IA considere ridículas, permítasenos la insistencia, estas preguntas, e incluso que se mofe de la ignorancia de quien escribe estas líneas. Pero los presupuestos de jurisdicción, de competencia genérica y los criterios de atribución de la competencia que afectan a los órganos jurisdiccionales, están fijados en nuestra Constitución (art. 117.3), y prescindir de ellos sólo porque estamos trabajando con máquinas y no con personas, no es legalmente posible sin una reforma legal amplia, que incluye la de la propia Constitución española.

Puede ser que ese mismo bienintencionado ingeniero informático o experto en IA crea que la cuestión puede resolverse de un plumazo, diciendo que hay que cambiar todo el sistema porque el vigente no sirve para nada. Tampoco es posible legalmente una solución tan simple, porque ello significaría un abandono conceptual de la división de poderes reflejada en nuestra Constitución, dado que el Poder Judicial ya no sería enteramente un poder político confiado por el pueblo, la ciudadanía, a seres humanos.

4. ¿QUÉ SITUACIÓN JURÍDICA TENDRÁN LAS EMPRESAS QUE PRODUCEN LOS ALGORITMOS?

En principio la idea básica de control, al ser una máquina, reside en los requisitos técnicos que deben concurrir para su construcción y homologación previa a su puesta en funcionamiento. Antes lo hemos apuntado. Esto está estrechamente vinculado con la fabricación de los algoritmos y de las máquinas de juzgar, es decir, con las empresas, públicas, privadas, o semipúblicas, que hagan de ello su actividad central, incluido su negocio.

Esto nos lleva, dicho en forma absolutamente pacífica, a una zona de alto riesgo, porque cuando un poder del estado, los jueces y magistrados, necesitan de expertos técnicos para explicar lo que ha sucedido, sucede o va a suceder, no tienen todo el control, porque escapa a su saber explicar los porqués. Aunque legalmente se opere con la ficción de que los jueces pueden controlar el proceso lógico de decisión del experto y valorar la consistencia de las conclusiones a los que ha llegado el mismo, aquí la situación es totalmente distinta, porque se trata de construir una máquina

que, nutrida por un algoritmo, teniendo en cuenta que ni la máquina ni el algoritmo son conocidos por los jueces y magistrados, decida un litigio, o ayude al juez a decidirlo.

Es evidente, por tanto, que el juez no puede explicar, por su formación, a no ser que sea ingeniero informático también, cosa rara en nuestro país, o experto acreditado en IA, tampoco frecuente, cómo se ha construido el Juez-Robot, ni cómo trabaja, ni cómo llega a la decisión que ha tomado. Y es dudoso que ello sirva de algo, por el principio que impide aportar el conocimiento privado del juez al conflicto. No sabe, en suma, nada del Juez-Robot. Está como juez en manos de la empresa fabricante de la máquina y, si no es la misma, también de la empresa elaboradora del algoritmo.

Por ello deben fijarse normas claras sobre esas empresas, que nos digan, no a nivel español, sino al menos, a nivel de la Unión Europea (y de Estados Unidos, Rusia y China), qué situación jurídica les alcanza. Debe regularse con detalle, qué empresas pueden construir el Juez Robot y pueden elaborar los algoritmos, qué requisitos deben concurrir para su autorización, que requisitos específicos respecto a las máquinas de juzgar y qué requisitos respecto a los algoritmos (normas de transparencia), el régimen específico de derechos de propiedad intelectual, de manera que no sea un coto cerrado de información inaccesible para el poder judicial y para las partes.

También debe regularse el régimen de responsabilidad jurídica de estas empresas, civil (extracontractual por el producto), y penal, en su caso.

Finalmente, el *status* jurídico de la empresa debe obligar a una cláusula muy estricta de confidencialidad sobre los asuntos llevados y resueltos, pues a nadie escapa que la información procesal en determinados casos delicados o muy notorios socialmente, puede ser muy valiosa, y al estar en manos de empresas privadas, ya no es fácilmente controlable.

5. ¿DEBERÁ EL CONSEJO GENERAL DEL PODER JUDICIAL CONTROLAR A LOS PROGRAMADORES?

Tratándose del Juez-Robot, lo más importante está en manos de personas ajenas al Poder Judicial, los programadores. ¿Cómo se les va a controlar? No veo otra manera de controlarlos más que por el Consejo General del Poder Judicial. Un control por el Ministerio de Justicia sería inmediatamente tildado de político y, por tanto, perjudicial para los nuevos sistemas de resolución de conflictos basados en la IA.

Pero ello deberá hacerse por ley orgánica y articulando un estatuto propio de los programadores (v. inmediatamente). En principio la idea básica de control, al tratarse de personas, reside en los requisitos personales y profesionales que deben concurrir en los candidatos para su aceptación. No es difícil establecer unos requisitos razonables, por ejemplo, ser mayor de edad, tener un título universitario que acredite los conocimientos exigidos o experiencia acreditada que los avale.

Pero otros requisitos, que deberían ser apropiados, no pueden serlo, como la ajenidad a la causa, la independencia profesional o la confidencialidad. Quien programa y maneja la máquina puede estar relacionado con la causa y no saberse nunca; puede tener un prejuicio o sesgo claramente atentatorio a la independencia judicial y no saberse nunca; y conocido por el público un dato interno del proceso que nunca debía haberse sabido, cómo probar que ha sido él quien lo ha filtrado. ¿Qué hacer entonces? ¿Qué parámetros deberá manejar el Consejo General del Poder Judicial para que ello no suceda? Cuanto más cercana al Poder Judicial sea la figura del programador, más probabilidades de control existirán, pero crear un cuerpo de funcionarios programadores no parece una buena solución en principio, porque las empresas privadas se opondrán, sin duda alguna, a perder el control sobre los mismos y sus "secretos".

La forma del control es problemática, porque la amenaza de sanción disciplinaria frente a incumplimientos o actos irregulares respecto a personas que no son funcionarios públicos, podría ser ilegal, incluso inconstitucional. Habrá que pensar en otras vías. El despido por la empresa podría servir, si el programador pertenece a la empresa que ha construido la máquina, ha elaborado el algoritmo o se encarga de su mantenimiento, pero no es tan fácil y habrá que reformar muchas leyes laborales. Además, puede ser notoriamente insuficiente a la vista del daño causado, si hay salidas profesionales para esas personas fuera de control.

Me inclino por pensar en una vía propia, sin perjuicio de que normas de otras instituciones puedan ser parcialmente aplicables, como la propia responsabilidad disciplinaria de los funcionarios en lo relativo a las infracciones y sus clases (muy graves, graves y leves).

6. ¿SERÁ NECESARIO UN ESTATUTO JURÍDICO DEL PROGRAMADOR?

No hace falta seguir más allá en estos temas orgánicos para entrever los graves problemas que el funcionamiento de la máquina de juzgar puede

conllevar. Pero queda uno, quizás el más importante en estos momentos, que debemos considerar.

En efecto, el algoritmo, en tanto en cuanto es una herramienta que proporciona una solución utilizando información, debe ser introducido en el ordenador por una persona. Esa persona es denominada "programador". Aunque puede ser ayudado por juristas y, por tanto, por jueces, no es un juez. El juez no sabe ni tiene por qué saber de informática a esos niveles. Es un informático, seguramente con titulación universitaria y altamente cualificado, con ampliación acreditada de estudios en magníficos institutos extranjeros de investigación, pero puede que sea un hábil técnico autodidacta que tan sólo hace su trabajo perfectamente.

Las preguntas que me vienen al pensamiento son entonces:

1.– ¿Qué grado de capacitación debe tener el programador? No hay nada regulado al respecto y, por tanto, no se requiere ninguna homologación profesional, al menos de momento.

2.– ¿Quién decide qué programador en concreto debe intervenir en la máquina de juzgar? Nadie lo sabe, por el momento. Hoy son decisiones sobre el terreno.

3.– ¿Quién decide qué criterios deben utilizarse para la selección del programador? Hay que responder lo mismo, son decisiones sobre la marcha, que no están estandarizadas.

4.– ¿Debe formar parte el programador de un organismo de control, independiente del Poder Ejecutivo, que proteja a los ciudadanos y a los propios programadores?

5.– ¿En el momento concreto de establecer el algoritmo, ¿quién controla que el programador no transmita a la máquina sus emociones, sentimientos, fortalezas, debilidades, pasiones, virtudes, defectos, etc., todo el subjetivismo de la persona que acabe contaminando y sesgando la decisión?

6.– ¿Habrá jerarquía de programadores, con sus clases, ascensos, etc.?

En suma, ¿será necesario un estatuto jurídico del programador para resolver todas estas cuestiones? Para mí, sin duda alguna, porque, una vez decidido quién va a ser el programador y cómo va a actuar, debería existir un estatuto jurídico del mismo que estableciese sus derechos y deberes, sus obligaciones y responsabilidades, incluida la regulación de un sistema objetivo de selección.

V. CONCLUSIONES

A estas alturas, creo que puede llegarse a dos conclusiones claras, siempre en el mundo del interrogante:

1.ª) ¿Estamos a las puertas de una nueva Justicia? Los temas aquí apuntados brevemente me hacen preguntarme si una nueva Justicia, no sólo por la forma de impartirse y por quien se imparte, va a venir entre nosotros para quedarse. Intuyo que sí, que una nueva Justicia está formándose en el mundo.

Es obvio que, ante el imparable progreso de la IA, un día u otro tendremos en Europa y, por tanto, también en España al Juez-Robot. Habrá que resolver muchos problemas orgánicos y funcionales, pero lo tendremos.

¿Significará ello que habrá que distinguir entre una Justicia humana y una Justicia robótica?

¿Significará ello que el órgano supremo de gobierno de los jueces, el Consejo General del Poder Judicial, carecerá de sentido, tal y como hoy lo entendemos?

¿Significará ello que habrá que reformar necesariamente la Constitución para que los principios humanos que rigen hoy la única Justicia que conocemos no perjudiquen el desarrollo de la IA, derogando o entendiendo de manera muy distinta la organización, la marca y la demarcación judiciales, suprimiendo los principios objetivos y subjetivos del Poder Judicial?

2.ª) Si así fuera, he de decir que un procesalista creyente en el Estado de Derecho no puede permitir que se socaven ni la independencia judicial ni la imparcialidad judicial desde ninguna perspectiva, ni dejar sin respuesta cualquier ataque a ambos principios.

El Juez-Robot provoca con ocasión de su actividad varias vulneraciones muy relevantes de derechos fundamentales, que pueden acabar significando el hundimiento del proceso como ahora lo conocemos:

A) La independencia judicial está en peligro, incluso aunque admitamos que la existencia del mismo no impide la sumisión a la ley, a una ley democráticamente aprobada. Pero la cuestión no es ésa, o ello por sí sólo no tranquiliza demasiado, si se tiene en cuenta que:

1.– No hay control judicial alguno sobre la figura del programador. Ni está regulado su ingreso en cuerpo alguno, ni su selección, ni los derechos, deberes ni responsabilidades, porque carece de un estatuto jurídico.

2.– No existe tampoco un órgano equivalente al Consejo General del Poder Judicial que pueda garantizar la independencia del programador, y parece ridículo pretender adscribir a éste a aquel órgano constitucional, aunque sí podría serlo al Ministerio de Justicia, lo que no aconsejaríamos por las razones aducidas *supra*.

3.– El programador se convierte en una autoridad, pública o privada, externa al juez, que influye en sus decisiones.

4.– El programador, ni tampoco el juez que se apoye en sus conocimientos, no está sujeto a responsabilidad civil o penal alguna.

B) La imparcialidad judicial sufre probablemente los mayores embates, porque la ajenidad no se puede predicar de un programador en el mismo sentido que del juez, y además habría que demostrarla. También debe añadirse que:

1.– El Juez-Robot carece de emociones, con lo cual hablar de principio subjetivo orgánico no tiene sentido, ya que no hay subjetividad posible en una máquina por muy inteligente que sea.

2.– Es imposible que el Juez-Robot se pueda abstener o que se le pueda recusar, lo que es aplicable también al programador.

3.– No es posible eludir las características personales del programador, quien consciente o inconscientemente, introduce sus propias inclinaciones, gustos, prejuicios, etc., al configurar los algoritmos y ponerlos a disposición de la máquina inteligente. Existe el peligro de que trate de proporcionar una información sesgada, contraria directamente a la exigible imparcialidad del decisor.

Por ello afirmo que en las circunstancias actuales la existencia de un Juez-Robot sentenciador no debería ser admisible ni en nuestro proceso civil ni en nuestro proceso penal. No vale la pena. Podría pensarse que en determinados casos sí podría ser admisible, previo acuerdo entre las partes de someterse a él y de renunciar al recurso, pero únicamente en el ámbito del proceso civil y fuera de la Jurisdicción, es decir, configurándose como alternativa (ADR).

Piénsese además en el profundo cambio que implicaría legalmente admitir el Juez-Robot. El problema es que se sigue estudiando y se sigue avanzando en este tema a pasos agigantados, lo que nos obliga como procesalistas a estar preparados, poner de manifiesto sus problemas legales e intentar darles solución. No estoy contra la IA, sólo estoy contra la Justicia robótica decisora. No me convence, ni me gusta y no le veo además ninguna ventaja y sí muchos inconvenientes.

Capítulo 6

Deepfakes, conteúdo gerado por inteligência artificial e verdade processual

Pedro Miguel Freitas[1]

Doutor em Direito. Professor da Escola do Porto da Faculdade de Direito Universidade Católica Portuguesa

I. INTRODUÇÃO

A procura da verdade histórica no decurso de um processo judicial, em particular o penal, é um caminho especialmente tortuoso e repleto de dificuldades. Desde logo, as colocadas pelas limitações intrínsecas à cognição humana dos factos que constituem o objeto do processo, que se somam às que resultam da circunstância de o decisor judicial não ter, em regra, contactado diretamente com a situação que deve julgar. Porque o decisor judicial não presenciou a comissão ou omissão da conduta penalmente relevante, o contacto com os factos ocorre de forma mediata, por intermédio de documentos ou testemunhos, por exemplo. Contacto esse que, mesmo que fosse direto, não é impermeável, antes pelo contrário, à subjetividade da perceção humana e ao circunstancialismo objetivo do decurso da situação apreciada.

Naturalmente que o princípio da imediação não resolve este problema. Tem o seu âmbito de aplicação confinado ao processo penal em si, não retrocedendo, por razões claras para todos, até ao momento da consumação típica do crime. A sua influência faz-se sentir, isso sim, na fase de julgamento. O motivo?

1. O presente texto serviu de suporte a uma comunicação oral apresentada na Conferência Ibero-Atlântica sobre Justiça Penal e Novas Tecnologias, que teve lugar nos Açores, em 13 de junho de 2022. Optou-se por manter o registo simples e tendencialmente coloquial do texto de apresentação.

Antes de mais, é preciso atender à natureza deste princípio. Alcandorando-se em princípio fundamental do processo penal, o seu conteúdo nutre-se das linhas caracterizadoras do direito processual penal positivado[2] e ao mesmo tempo serve de critério para integração de lacunas desse mesmo direito positivo. Assim, o princípio da imediação cinge-se ao tempo do processo penal e, dentro deste, essencialmente à audiência de julgamento.

Quanto ao seu conteúdo, convém relembrar que, tal como os princípios da publicidade e o da oralidade, é um princípio que se relaciona com a forma dos atos processuais e implica que "a decisão jurisdicional só [possa] (…) ser proferida por quem tenha assistido à produção das provas e à discussão da causa pela acusação e pela defesa" e que se deva "dar preferência aos meios de prova que se encontrem em relação mais directa com os factos probandos (*v.g.* preferência das testemunhas presenciais às de «ouvir dizer», dos documentos originais às suas cópias, etc.)"[3].

A imediação "torna possível, na apreciação das provas, a formação de um juízo insubstituível sobre a credibilidade da prova; das razões que se podem observar, no exame directo da prova, para acreditar, ou não acreditar, na mesma" (Ac. STJ de 06/02/2008, processo n.º 07P4374).

Mesmo assim configurado, o princípio da imediação não resolve definitivamente o problema da aproximação –pois não é mais do que isso– à verdade histórica ou ontológica. A imediação processual mais não é que um contato direto e pessoal entre o juiz e os meios de prova[4], uma espécie de aproximação mediada ao facto ilícito típico, que não se confunde com a imediação pré-processual ou extraprocessual associada a uma exposição presencial ao mesmo.

II. INTELIGÊNCIA ARTIFICIAL E DIREITO PENAL

Esta aproximação enfrenta agora um outro desafio colocado pelas novas tecnologias. Os avanços sentidos no campo da inteligência artificial, nomeadamente em *machine learning*, têm sido revolucionários, ao mesmo tempo que demonstrativos de uma potencialidade que promete transformar profundamente o rumo da civilização humana. Enquanto isso, ao Direito, enquanto instrumento regulatório, é-lhe pedido que normativize esta realidade, marcando a fronteira do lícito e do ilícito, do desejável e do indesejável, do risco permitido e do proibido.

2. SILVA, Germano Marques, *Curso de Processo Penal*, vol. 1, 6.ª ed., Verbo, 2010, p. 64.
3. SILVA, Germano Marques, *Curso de Processo Penal*, vol. 1, 6.ª ed., Verbo, 2010, p. 105.
4. SILVA, Germano Marques, *Direito Processual Penal Português, Do Procedimento (Marcha do Processo)*, vol. 3, Universidade Católica Editora, 2015, p. 212.

Mas desta vez não se trata somente de incorporar no *corpus iuris* algo que lhe é estranho e externo.

Tomemos como exemplo o direito penal em sentido amplo. A emergência e desenvolvimento de técnicas de inteligência artificial tem contribuído para a criação de novos modos de preenchimento típico de comportamentos que convencionamos dizer que são pertencentes à criminalidade tradicional (p. ex. difamação) e fazem-nos refletir sobre a eventual necessidade de identificação de bens jurídico-penais até aqui inexistentes na tessitura jurídico-criminal como resposta aos mais recentes ensejos comunitários no sentido da proteção de estados, objetos ou bens de relevância individual ou coletiva. Dito de outro modo, o condão transformativo da inteligência artificial sente-se e sentir-se-á cada vez mais intensamente nos mais ínfimos aspetos da nossa vida, incluindo, por maioria de razão, aqueles com que o direito penal substantivo terá de lidar, ou por via da neocriminalização ou pela acomodação de modos de execução inauditos, se não mesmo pelo reequacionamento das suas categorias dogmáticas e princípios norteadores.

Atenta a sua simbiótica relação com o direito penal substantivo, ao processo penal é exigido idêntico esforço de reflexão e eventual adaptação a uma nova realidade. Neste domínio, que se cruza com o anterior, não são incomuns os estudos acerca do impacto jusfundamental de ferramentas algorítmicas de suporte à decisão judicial. Em particular, como o seu funcionamento, tendencialmente opaco e permeável a vieses societais, mina o direito a um julgamento justo e impossibilita o exercício efetivo de garantias de defesa como o direito ao recurso. Outro dos direitos fundamentais potencialmente afetado pelo uso de IA é o direito à privacidade. A crescente presença de equipamentos inteligentes (*smart devices*), p. ex. colunas inteligentes, que vão registando e conservando o que é dito ao seu redor origina situações em que a "AI in some cases can actually assume the role of a witness, providing crucial evidence in an investigation or lawsuit"[5], no sentido da condenação ou da absolvição. Tudo isto com consequências a nível probatório. Uma outra questão, sobre a qual nos dedicaremos um pouco mais, é a da criação ou manipulação de fotos, vídeos e áudio com recurso a inteligência artificial e seu impacto no processo penal.

III. *DEEPFAKES* E O DIREITO PROBATÓRIO

A manipulação de imagens (estáticas ou em movimento) e áudio não é um fenómeno exclusivo do século XXI. O seu aparecimento

5. BARFIELD, Woodrow e Ugo Pagallo, *Advanced Introduction to Law and Artificial Intelligence*, Elgar, 2020, p. 51.

entrelaça-se com a história da gravação do áudio, fotografia ou vídeo[6], inclusivamente quando o formato digital ainda não existia. Aliás, muito antes sequer do advento do Photoshop e pouco tempo após a invenção da fotografia, Hippolyte Bayard criou aquela que é considerada a primeira fotografia falsa, intitulada "Noyé" (1840), um autorretrato de Boyard supostamente afogado após suicídio, como forma de protesto contra a falta de reconhecimento público do seu trabalho na invenção da fotografia[7]. Nesse mesmo século XIX surgiram as fotografias espíritas onde se empregava uma técnica de dupla exposição com a qual se sobrepunham várias imagens numa só fotografia e que supostamente revelariam fantasmas.

Desde então, a manipulação de fotografias foi-se tornando trivial. Apesar da sua falibilidade, a fotografia foi sendo admitida enquanto meio de prova sujeito à livre apreciação do julgador. No Reino Unido, por exemplo, material fotográfico como prova incriminatória do arguido é admissível em quatro hipóteses ([2003] 1 Cr APP Rep 21):

"(i) quando a imagem fotográfica for suficientemente nítida, o júri pode compará-la com o arguido sentado no banco dos réus;

(ii) quando uma testemunha conhece o arguido suficientemente bem para reconhecê-lo como o infrator retratado na imagem fotográfica, ele pode depor sobre isso; e isso pode acontecer mesmo que a imagem fotográfica não esteja mais disponível para o júri;

(iii) quando uma testemunha que não conhece o arguido passa muito tempo a ver e a analisar imagens fotográficas do local, adquirindo assim conhecimentos especiais que o júri não possui, pode fornecer prova de identificação com base na comparação entre essas imagens e uma fotografia razoavelmente contemporânea do arguido, desde que as imagens e a fotografia estejam à disposição do júri;

(iv) um especialista devidamente qualificado com habilidades de mapeamento facial pode fornecer provas de identificação com base numa comparação entre imagens da cena (aperfeiçoadas ou não e uma fotografia razoavelmente contemporânea do arguido, desde que as imagens e a fotografia estejam disponíveis para o júri".

Poder-se-á perguntar o que traz de novo a inteligência artificial. O que há de diferente na criação e manipulação de imagens e áudio por

6. KIETZMANN, Jan, Linda W. Lee, Ian P. McCarthy, Tim C. Kietzmann, "Deepfakes: Trick or treat?", in *Business Horizons*, volume 63, número 2, 2020, p. 145.
7. WHEELER, Thomas H., *Phototruth or Photofiction?: Ethics and Media Imagery in the Digital Age*, Routledge, 2002, p. 15.

intermédio da inteligência artificial? Sumariamente: a credibilidade e a acessibilidade[8].

O desenvolvimento de técnicas de *machine learning* e inteligência artificial aplicadas à alteração e modificação de imagem e áudio permitiu que a criação de resultados praticamente indistinguíveis da realidade, sobretudo na área da fotografia, se tornasse perfeitamente acessível mesmo para quem não tenha profundos conhecimentos técnicos. Algo similar existia já na área do cinema –efeitos especiais e visuais–, mas requerem mão-de-obra especializada e intensiva, bem como hardware e software adequados.

A credibilidade inerentemente atribuída a algo que vemos ou ouvimos é precisamente o vetor explorado por quem se serve destas novas técnicas. Pense-se, por exemplo, no fabrico de um vídeo em que certo indivíduo aparece a pontapear outrem, tendo isto servido para corroborar a acusação.

Este novo fenómeno é denominado *deepfake*. Nas palavras de der Sloot e Wagensveld, um *deepfake* é "conteúdo (vídeo, áudio ou outro) que é total ou parcialmente fabricado ou conteúdo existente (vídeo, áudio ou outro) que tenha sido manipulado"[9].

De um ponto de vista tecnológico, a criação de *deepfakes* faz-se, em regra, com Redes Adversárias Generativas (*Generative Adversarial Networks* –GAN). Estas redes são uma espécie de algoritmo generativo que consiste na implementação de dois modelos computacionais que competem entre si: um gerador e um discriminador. A função do primeiro modelo é a de "criar exemplos que são o mais realistas possíveis para enganar o discriminador, enquanto o discriminador tenta distinguir os exemplos falsos gerados dos exemplos verdadeiros"[10]. Desta competição entre os dois modelos– tipicamente redes neuronais artificiais[11] –resulta uma aprendizagem automatizada útil para aplicações tão diversas quanto a manipulação e síntese de imagens, incluindo a criação de imagens de rostos ou objetos, a síntese de texturas, a deteção de objetos, geração de música e

8. KIETZMANN, Jan, Linda W. Lee, Ian P. McCarthy, Tim C. Kietzmann, "Deepfakes: Trick or treat?", in *Business Horizons*, volume 63, número 2, 2020, pp. 136-137.
9. SLOOT, Bart van der, Yvette Wagensveld, "Deepfakes: regulatory challenges for the synthetic society", in *Computer Law & Security Review*, volume 46, setembro 2022, p. 1.
10. GUI, Jie, Zhenan Sun, Yonggang Wen, Dacheng Tao, Jieping Ye, "A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications", in *arXiv*, 2020, p. 2.
11. GOODFELLOW, Ian, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, Yoshua Bengio, "Generative Adversarial Networks", in *arXiv*, 2014, p. 140.

vídeo, síntese de fala, processamento de linguagem natural e a descoberta de medicamentos[12], para citar apenas algumas das áreas que beneficiaram desta técnica, que é estudada deste 2014[13].

Ademais, é uma técnica que dispensa supervisão humana para atingir os objetivos propostos. Daí que se categorize como uma modalidade de "aprendizagem não supervisionada". Se se tratasse de uma "aprendizagem supervisionada", haveria um programador/utilizador humano que "ensinaria" o algoritmo a partir de um conjunto de dados. Ao algoritmo é "fornecido um conjunto de dados de pares de exemplos de entrada e de saída" e "aprendem a associar cada entrada a uma saída"[14], p. ex., associar uma foto de um cão a este tipo de animal e não a um gato.

Uma vez que a aprendizagem supervisionada é intrinsecamente dependente da intervenção humana e suas capacidades e limitações, assim como de um número considerável de dados, não raras vezes na ordem dos milhões, com a aprendizagem não supervisionada ultrapassam-se as referidas desvantagens[15].

Os *deepfakes* podem ser agrupados em cinco tipos[16]: substituição facial, reencenação facial, geração de rostos, síntese de fala e falsificações superficiais (*shallowfakes*). Com a substituição facial transfere-se a imagem da face de uma pessoa para a de outra pessoa. A reencenação facial consiste em usar a imagem de alguém e recriar movimentos faciais, incluindo os lábios. Uma possível utilidade deste tipo de *deepfakes* é a de simular que alguém está a concordar ou discordar de algo ou ainda que está a dizer algo que na realidade não está. Os *deepfakes* podem também corresponder a rostos de pessoas inexistentes. Nesta modalidade de *deepfakes*, são empregadas técnicas de inteligência artificial para gerar "fotografias" de rostos (p. ex. https://generated.photos/faces). Com a síntese de fala é

12. HONG, Yongjun, Uiwon Hwang, Jaeyoon Yoo, Sungroh Yoon, "How Generative Adversarial Networks and Their Variants Work: An Overview", in *arXiv,* 2019, pp. 1-2.
13. GUI, Jie, Zhenan Sun, Yonggang Wen, Dacheng Tao, Jieping Ye, "A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications", in *arXiv*, 2020, p. 1.
14. GOODFELLOW, Ian, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, Yoshua Bengio, "Generative Adversarial Networks", in *arXiv*, 2014, p. 139.
15. GOODFELLOW, Ian, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, Yoshua Bengio, "Generative Adversarial Networks", in *arXiv*, 2014, p. 139.
16. TREND MICRO RESEARCH, United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol's European Cybercrime Centre (EC3), *Malicious Uses and Abuses of Artificial Intelligence*, Trend Micro Research, 2020, pp. 53-54.

possível treinar algoritmos com a voz de alguém para, posteriormente, ser criada ou modificada uma comunicação oral. Finalmente, por falsificações superficiais entendem-se as falsificações de menor complexidade, em que são usadas "técnicas de edição rudimentar"[17].

Neste ano de 2022, foram disponibilizadas ao público em geral ferramentas de text-to-image (texto para imagem) que, beneficiando dos avanços do *deep learning*, permitem aos seus utilizadores fornecer uma descrição textual do resultado que procuram obter e o sistema de IA cria a imagem correspondente. Ou seja, ferramentas como o DALL-E 2 (https://openai.com/dall-e-2/), Stable Diffusion (https://stability.ai/) ou o Midjourney (https://www.midjourney.com/) são "sistema[s] de IA que conseguem criar imagens realistas e arte a partir de uma descrição em linguagem natural" (https://openai.com/dall-e-2/). Em termos sintéticos, trata-se de síntese text-to-image (texto para imagem). Estas ferramentas integram também funcionalidades como o *inpainting* (criação ou alteração de partes de uma imagem sintética ou real), *outpainting* (extensão de uma imagem previamente existente) e *image-to-image* (criação de uma imagem a partir de uma imagem e uma descrição textual previamente fornecidos pelo utilizador).

Diante deste estado de coisas e, sobretudo, do que está para vir, não será exagero afirmar-se que as "tecnologias digitais parecem minar a nossa confiança acerca da natureza autêntica, genuína e original do que vemos e ouvimos"[18]. Inclusive quando um julgador tem a tarefa de descortinar a verdade histórica a partir dos contributos probatórios que encontra ou que traz para os autos de um processo. Como alertam a Europol, as Nações Unidas e a Trend Micro, "o conteúdo audiovisual deepfake pode ser apresentado de forma maliciosa como prova «legítima» na tentativa de frustrar investigações criminais e processos judiciais, lançando dúvidas sobre as provas audiovisuais como uma categoria de provas. Isso criaria novos obstáculos legais para investigadores e advogados, além de prejudicar a credibilidade dos processos, incluindo as instituições e indivíduos que participam do mesmo processo. Até mesmo a administração ou o sistema de justiça podem ser questionados"[19].

17. TREND MICRO RESEARCH, United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol's European Cybercrime Centre (EC3), *Malicious Uses and Abuses of Artificial Intelligence*, Trend Micro Research, 2020, p. 54.
18. FLORIDI, Luciano, "Artificial Intelligence, Deepfakes and a Future of Ectypes", in *Philosophy & Technology*, volume 31, 2018, p. 320.
19. TREND MICRO RESEARCH, United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol's European Cybercrime Centre (EC3), *Malicious Uses and Abuses of Artificial Intelligence*, Trend Micro Research, 2020, p. 61.

Uma resposta adequada aos riscos criados pelos *deepfakes* é necessariamente multidisciplinar: "(…) [o] que o digital quebra ele também pode reparar, não muito diferente da luta interminável entre vírus e antivírus. No nosso caso, para além de educarmos as pessoas, adquirir novas sensibilidades e ter o enquadramento legal adequado"[20]. São essenciais a educação e a literacia digital das pessoas, de modo a que a acessibilidade às novas tecnologias seja acompanhada de uma atitude mais crítica e reflexiva acerca da informação que é consumida por seu intermédio. A preparação da comunidade em geral para a realidade da má utilização de *deepfakes* é importante, mas a tecnologia em si também pode ser útil para minorar este problema. Por exemplo, ferramentas automatizadas de deteção de *deepfakes* ou a verificação de origem de um conteúdo audiovisual com recurso a *blockchains*[21].

No que ao direito processual penal se refere, não restam dúvidas de que os *deepfakes* podem contaminar o acervo probatório e a decisão final do julgador. Relembre-se a hipótese acima referida de o assistente fabricar um vídeo em que é alegadamente agredido pelo arguido, ou imagine-se que são submetidas como provas vídeos ou fotos adulterados ou artificialmente criados. Atendendo ao quadro normativo português atual, sobressai desde logo o princípio da livre apreciação da prova. Previsto no artigo 127.º do Código de Processo Penal (CPP), estabelece que "a prova é apreciada segundo as regras da experiência e a livre convicção da entidade competente". Princípio esse que comporta uma dimensão positiva e uma dimensão negativa: "significa, negativamente, a ausência de critérios legais que predeterminem o valor da prova e, positivamente, que as entidades a quem caiba valorar a prova o façam de acordo com o dever de perseguir a realização da justiça e a descoberta da verdade material, numa apreciação que terá de ser sempre objetivável, motivável e, por conseguinte, suscetível de controlo"[22]. O juiz de julgamento, o juiz de instrução e o ministério público devem então valorar a prova não de forma predeterminada pela lei –a isto corresponderia o princípio da prova legal– mas de acordo com as regras de experiência e a sua livre convicção. Não é, todavia, um princípio sem exceções, como evidenciam p. ex. as regras em matéria de depoimento indireto (artigo 129.º do CPP) ou de vozes públicas e convicções pessoais (artigo 130.º do CPP). Vale, porém, sem especiais limitações para a apreciação de reproduções fotográficas, cinematográficas ou fonográficas.

20. FLORIDI, Luciano, "Artificial Intelligence, Deepfakes and a Future of Ectypes", in *Philosophy & Technology*, volume 31, 2018, p. 320.
21. TREND MICRO RESEARCH, United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol's European Cybercrime Centre (EC3), *Malicious Uses and Abuses of Artificial Intelligence*, Trend Micro Research, 2020, p. 62.
22. ANTUNES, Maria João, *Direito Processual Penal*, 2.ª edição, Almedina, 2018, p. 177.

Tendo como pano de fundo o princípio da livre apreciação da prova, impõe-se perguntar se o surgimento dos *deepfakes* demandam uma reavaliação dos atuais princípios norteadores do direito processual penal português e, concomitantemente, do direito positivo.

A manutenção do *status quo* normativo –de sujeição à livre apreciação da prova– encontra um inconveniente que é o do relativo, quando não mesmo generalizado, desconhecimento desta nova realidade. Como pode ser materializado jurídico-empiricamente o princípio da livre apreciação da prova nos dias atuais se a mundividência de quem procede à valoração for sustentada em pressupostos datados, próprios de quem equivoca passado, presente e futuro, e desconhece a atualidade dos perigos para a comunidade e para a administração da justiça em particular? Inexistindo uma robusta literacia digital que acompanhe o domínio da criação, interpretação e aplicação do direito, abrem-se as portas para um fenómeno de obsolescimento material do direito.

Uma via de encerramento das portas do sistema de justiça penal à sua instrumentalização pelos *deepfakes* passaria pela introdução de regras de admissibilidade de provas fotográficas, cinematográficas ou fonográficas com as quais se atribuiria um ónus de comprovação de autenticidade ao sujeito processual que as pretende juntar ao processo. Particularmente se se tratar do assistente ou do arguido. Desse modo, incumbiria ao sujeito processual juntar um relatório pericial atestando que, à luz dos conhecimentos tecnológicos atuais, não teria sido possível detetar indícios de que esse conteúdo fosse parcial ou totalmente artificial. A eventual crítica de parcialidade na redação do referido relatório técnico poderia ser ultrapassada com a atribuição deste encargo a um estabelecimento, laboratório ou serviço oficial, como acontece de resto com qualquer prova pericial nos termos do CPP atualmente em vigor (artigo 152.º).

A vantagem de uma solução assim configurada seria a de conferir maior confiança e tranquilidade à entidade que devesse valorar uma prova desta natureza. Embora pudesse constituir uma desvantagem naquelas situações em que a confiança e tranquilidade dessa entidade assentassem num falso negativo quanto à identificação do *deepfake*. Sairia exacerbado o potencial lesivo do *deepfake* agora que ultrapassado e ludibriado o crivo da prova pericial. Além de que se colocaria a questão de saber quem deveria arcar com as despesas inerentes à contratação de um perito. Recaindo, como seria expectável, sobre quem quisesse juntar ao processo a prova, não seria um desincentivo à sua utilização? Não estaríamos assim a caminhar para um processo desprovido de fotografias, vídeos e áudios enquanto material probatório? Ou mesmo a cavar um

fosso probatório entre sujeitos processuais consoante a sua capacidade financeira?

Provavelmente a resposta mais direta e imediata aos *deepfakes* passaria pela produção de prova pericial nos termos do artigo 151.º e ss. do CPP. Dada a complexidade técnica inerente ao juízo de atribuição de uma origem sintética a um conteúdo visual ou sonoro, o recurso à prova pericial é facilmente percecionado como uma solução evidente para estes casos. A intervenção de um perito justifica-se pela circunstância de serem precisos especiais conhecimentos técnicos que o jurista não dispõe. Por essa razão, temos a presunção de que o juízo técnico esteja subtraído à livre apreciação do julgador (artigo 163.º, n.º 1 do CPP). Todavia, a questão que se deve colocar é a seguinte: se a constatação da necessidade da perícia é um elemento constitutivo do despacho que a ordena, é expectável que o julgador admita a possibilidade de que o que vê com os seus olhos e ouve com os seus ouvidos não é real?

O juízo de ponderação acerca da necessidade da prova pericial não é verdadeiramente livre e esclarecido se desconhece os pressupostos (tecnológicos) que servem de fundamento ao requerimento. Atribuir a solução de um problema complexo a um especialista, pressupõe, em primeiro lugar e antes de mais, a identificação da complexidade do problema.

E este problema poderá assumir proporções especialmente graves quando o alvo destes conteúdos sintéticos ou artificiais seja uma pessoa particularmente indefesa, alguém incapaz de, por si mesmo, clamar por justiça perante uma prova que não corresponde à realidade.

IV. CONCLUSÃO

A inteligência artificial tem fomentado mudanças galopantes na nossa sociedade, relativamente às quais o direito não pode ficar indiferente. Ao direito é demandada uma resposta normativa, enquanto é, concomitantemente, cada vez mais afetado e transformado, no desenvolvimento das suas tarefas, pelos contributos produzidos no domínio da inteligência artificial.

O surgimento dos *deepfakes,* intrisicamente ligado a sistemas de inteligência artificial, é mais um (novo) desafio colocado ao direito penal, nomeadamente adjetivo, podendo inclusive originar uma reavaliação dos seus atuais princípios norteadores. De entre eles, merece particular atenção o da livre apreciação da prova. A questão é sobretudo a de saber se a mera existência de *deepfakes*, e risco associado de perda de confiança

na veracidade e autenticidade de factos penalmente relevantes exibidos em conteúdos audiovisuais, implicaria, *ab initio*, a subtração deste tipo de material probatório à livre apreciação do julgador.

Tendencialmente poder-se-á afirmar que a resposta deverá implicar uma maior utilização da prova pericial, desde que capaz de aferir, para além de qualquer dúvida significativa, a origem sintética ou não de um conteúdo audiovisual. No entanto, uma resposta mais holística não deve ignorar a importância da literacia digital, em particular daqueles que integram o sistema de justiça penal.

Capítulo 7

Justiça penal e inteligência artificial – uma justiça *fitness*?

Anabela Miranda Rodrigues

Professora Catedrática
Faculdade de Direito/Universidade de Coimbra

I. INTRODUÇÃO

É minha convicção que, neste momento, é responsabilidade nossa estarmos empenhados em procurar caminhos para melhorar a justiça penal. E que os desenvolvimentos tecnológicos que experienciamos são uma oportunidade que devemos saber aproveitar. Somos privilegiados por termos a liberdade de poder imaginar uma justiça que pode ser transformada pelo digital. E por termos o poder de o fazer.

Nesta abordagem ao tema da Inteligência Artificial (IA) e justiça penal, vou manter-me no plano epistemológico.

Em jeito de introdução, apresento quatro notas, que surgirão desenvolvidas ao longo do meu texto.

Assim, relembro que a viragem digital trouxe consigo duas condições para permitir que a justiça penal tivesse ao seu dispor instrumentos que lhe podem ser de grande utilidade em toda a espécie de processos de tomada de decisões[1]: dados –uma sua produção maciça e, além do mais, a título gratuito– e poder computacional de cálculo sem precedentes, num quadro de globalização de redes. Para além disso, admitiu-se que

1. Cf. MIRANDA RODRIGUES, Anabela, "Inteligência Artificial no Direito Penal – a Justiça Preditiva entre a Americanização e a Europeização", *A Inteligência Artificial no Direito Penal*, Coord. Anabela Miranda Rodrigues, Almedina, 2020, p. 11s; LASSÈGUE, Jean, "L'Intelligence Artificielle, Technologie de la Vision Numérique du Monde", *Les Cahiers de la Justice*, 2019/2 N.º 2, p. 205s (especialmente, p. 207s).

a noção de ser humano podia *desaparecer* do conceito de inteligência –a inteligência–, afinal, pode ser vista como um conceito objetivo, aplicável a outros comportamentos que não os humanos. Podem convocar-se os filósofos –desde *Aristóteles, Hobbes, Pascal, Leibnitz* ou *Descartes*, passando por *Hume*, até aos mais lídimos representantes do *Círculo de Viena*, como *Russel* ou *Wittgenstein*–, que de alguma maneira consideravam o cérebro humano comparável a uma máquina; a psicologia cognitiva e *William James*, defendendo que humanos e animais podem ser considerados máquinas que processam informação; ou os linguistas, como *B.F. Skinner* ou *Noam Chomsky*, com a sua sugestão de que a linguagem, com a sua estrutura sintática, é suficientemente formal para poder ser programada. Mas o impulso da matemática foi essencial, passando a ver a relação do agente inteligente com o mundo como uma relação matemática de tipo funcional. Raciocinar passa a ser relacionar informações recolhidas como "entrada" (*input*) para operar um "tratamento", produzindo informações como "saída" (*output*). O algoritmo desempenha aqui um papel fundamental, traduzindo-se num conjunto de instruções matemáticas a ser seguidas por uma ordem fixada, exatamente com a finalidade de fazer a passagem dos *inputs* para *outputs*.

A matemática forneceu à IA a formalização e os instrumentos de que ela necessitava nas áreas da computação, lógica e probabilidades. Estava criado o contexto ideal para o seu desenvolvimento. Pode ainda dizer-se que as suas realizações práticas são eticamente neutras – os mesmos instrumentos podem desencadear efeitos positivos ou negativos, consoante as finalidades que lhe são atribuídas, para o melhor ou para o pior.

Outro aspeto que é essencial ter presente é a objetividade que se aponta aos processos algorítmicos de decisão.

A objetividade que o algoritmo traz consigo –afastando aspetos subjetivos, suportados, designadamente, em preconceitos ou condições contingentes– pode ser uma vantagem, por suprimir, não só a arbitrariedade, mas ainda também a discricionariedade na decisão humana. Isto é (ou pode se, quase sempre…) uma vantagem indiscutível, quando estão em causa decisões em domínios técnicos e científicos: por exemplo, na condução de veículos, na aviação, em decisões médicas, em certos domínios jurídicos que envolvam a aplicação de normas meramente técnicas, etc. Mas, nas decisões jurídico-penais de um certo tipo –relativas, por exemplo, à imputação da culpa ou à determinação da pena pode e deve discutir-se a questão da discricionariedade da decisão judicial. Ou seja: o "poder" que o algoritmo deve retirar a um juiz é o da arbitrariedade– e ainda bem, dir-se-á. O risco é o de suprimir também a necessária discricionariedade

–implicada no sentido da aplicação do direito[2]– das decisões judiciais, onde entram, agora, o pensamento intuitivo ou valorações pessoais.

Um terceiro aspeto a apontar é o de que a IA é melhor do que a Inteligência *Humana*.

A IA alimenta-se de um maior conhecimento sobre o nosso cérebro, que as neurociências favoreceram, permitindo conhecer melhor o nosso processo de tomada de decisões. A IA compete com as redes neuronais e é melhor. Escreveu *Yuval Noah Harari*[3]: "Se as emoções e os desejos 'não passarem de algoritmos bioquímicos' e 'resultarem de um processo bioquímico', a IA pode 'ultrapassar o desempenho humano em muitas áreas profissionais, como emprestar dinheiro a estranhos, negociar um acordo comercial ou conduzir um veículo numa rua cheia de peões'. Além disso, a IA possui duas importantes capacidades não humanas: conetividade e aperfeiçoamento constantes. O que significa que a IA pode superar o desempenho humano".

Dito de outra maneira: a IA pode funcionar de modo bastante diferente e *inhumano*. Pensar que o desenvolvimento de artefactos artificiais inteligentes reside em "copiar" as formas de desempenho humano baseia-se, como *Richard Susskind* e *Daniel Susskind* alertaram, numa falácia e numa visão excessivamente centrada no ser humano da IA[4].

Acrescento ainda uma última nota.

No direito, e no direito penal, há ainda alguma confusão quanto à distinção entre automatização (*automation*) e IA[5].

Podemos considerar sistemas autónomos aqueles que são capazes de reagir ao ambiente sem a necessidade de intervenção humana –por isso, autónomos–, mas que são incapazes de escolher o curso da ação ou de criar uma solução nova para um problema –por isso, não são inteligentes–. Estes sistemas apenas apresentam uma resposta pré-programada, de acordo com o ambiente identificado por eles.

Com os desenvolvimentos matemáticos a que fizemos referência, os engenheiros estavam aptos a criar máquinas com redes de neurónios

2. Cf. *infra*, sob III., 1. e 1.1.
3. HARARI, Yuval Noah, *21 Lições para o Século XXI*, Edição Elsinore, 1.ª edição, 2018, p. 41s.
4. Cf. SUSSKIND, Richard/SUSSKIND, Daniel, *The Future of the Professions: How Technology Will Transform the Work of Human Experts*, Oxford University Press (2015); Updated Edition (2022), *passim.*
5. Um domínio prático onde esta distinção avulta é o da prevenção e luta contra o branqueamento de capitais. A este respeito, cf. MIRANDA RODRIGUES, Anabela, "*Compliance* inteligente e prevenção e luta contra o branqueamento", *A Inteligência Artificial e o Direito Penal*, Volume II, Coord. Anabela Miranda Rodrigues, Almedina (no prelo).

artificiais (ANN – *artificial neural networks*), não necessariamente idênticas mas inspirados nas redes neuronais biológicas, que "aprendem" a desempenhar tarefas. A finalidade da IA é criar sistemas computacionais com capacidade, entre outras, de *machine learning*, isto é, de se adaptarem a novas circunstâncias e detetarem e extrapolarem padrões. Isto significa que são capazes de aprender e de se aperfeiçoar automaticamente com a experiência, sem serem expressamente programados. Esta aplicação de IA centra-se no desenvolvimento de programas que podem aceder a dados e usá-los para aprender por si próprios. Neste sentido, podemos considerar a IA como *machine intelligence*, tendo a capacidade de perceber o ambiente através de *input* de dados e, com base neles, de escolher o curso da ação entre vários possíveis, com o objetivo de resolver problemas.

Acontece que a aproximação do direito à IA é ainda demasiado "conservadora", porque se reduz a uma relação de meio-fim – a *Legaltech* centra-se apenas na otimização de processos mediante a IA e descura o desenvolvimento da IA "profunda". Desta forma, quero significar que, normalmente, cai-se na tentação de utilizar o conceito de IA como um "conceito-chapéu", onde cabem vários sub-domínios como a robótica, a *machine learning* ou o processamento de linguagem natural. O erro consiste em considerar que existe "uma" IA e concentrarmo-nos só nas suas aplicações mais conhecidas ou comerciais, quer dizer, na *IA soft* ou *limitada* –a das aplicações móveis como a *Siri*– ou na *IA média*, como a dos veículos inteligentes ou dos juízes robôs do projeto *Velsberg*, aprovado na Estónia, para julgar casos bagatelares em matérias do âmbito contratual. Em qualquer caso, *IA fraca*. Ora, é preciso estar atento aos desenvolvimentos da IA mais "profunda" –a *IA forte*– que, no âmbito dos *Big Data* e da *Internet das Coisas* (*IoT*, na sigla inglesa), nos situa na "rota da singularidade"[6] – de sistemas que são, de alguma forma, conscientes[7].

Terei em consideração apenas a IA fraca. Combinando uma definição que toma em conta o seu desenho e a sua função, hoje contamos já com instrumentos que, em vez de realizarem tarefas seguindo regras explicitamente articuladas por programadores humanos –enormes árvores de decisão e fluxogramas, no que se pode considerar a "primeira vaga de IA"–, "aprendem" a partir de enormes bases de dados passados: é a "segunda vaga de IA"[8]. São sistemas que realizam tarefas –tão diferentes

6. Cf. CARO CARIA, Dino Carlos, "Compliance, Neurociencias e Inteligencia Artificial/Compliance, Neuroscience and Artificial Intelligence", *on line*, https://neuralink.com/2022, p. 633 s. (p. 635).
7. Cf. SUSSKIND, Richard, *Online Courts and the Future of Justice*, Oxford Universsity Press, 2019, p. 265.
8. Cf. SUSSKIND, Richard, *op.ult. cit.*, p. 264.

como resolver problemas, escrever música, reconhecer emoções ou colocar tijolos– e que se acreditava até há bem pouco tempo que exigia inteligência humana. Pode ir-se mais longe e abranger também "máquinas super-inteligentes", isto é, sistemas de IA que têm um desempenho bem além das capacidades correntes humanas. Em qualquer caso, estamos a referir-nos a *supervised machine learning* ou a *deep neural networks*, na terminologia apontada por *Richard Susskind*[9].

II. A IA APLICADA À ADMINISTRAÇÃO DA JUSIÇA PENAL

A revolução digital permitiu falar de justiça penal preditiva. Isto significa promover uma *nova* previsibilidade como suas principais caraterística e objetivo nos processos de tomada de decisões.

Se quisesse fazer uma aproximação a uma definição ampla de justiça preditiva[10], diria que está em causa o tratamento algorítmico de enormes quantidades de dados, para garantir às partes e aos decisores judiciários, designadamente aos juízes, previsões credíveis –muitas vezes quantificadas em termos percentuais– sobre o futuro. De um lado, favorece-se a possibilidade de completa digitalização das decisões dos tribunais e o acesso irrestrito a qualquer jurisprudência e utilização de *software* mais ou menos sofisticado para a sua análise, tendo em vista encontrar padrões de previsibilidade nas decisões judiciais; e, por outro lado, contribui-se para a crescente utilização de instrumentos de avaliação do risco (*risk assessment tools*) no processo de tomada de decisões nas várias fases do processo judicial.

A questão de uma definição de justiça preditiva acompanha a discussão sobre ela. Desde logo, difere sensivelmente consoante os atores em causa do sistema de justiça. Chega a referir-se como um conceito vazio de sentido e afirma-se que "não há nada a prever", lembrando que "não só 2 juízes diferentes podem tomar 2 decisões diferentes num mesmo caso, como também 1 só e mesmo juiz pode adotar decisões divergentes em casos que apresentam as mesmas caraterísticas"[11].

Entretanto, com as diferentes ferramentas hoje em dia disponíveis, do que se trata é de produzir informação estatística e probabilística, tendo em

9. Cf. SUSSKIND, Richard, *op. ult.cit., loc. cit.*

10. Sobre isto, com desenvolvimentos, MIRANDA RODRIGUES, Anabela, "Inteligência Artificial no Direito Penal – a Justiça Preditiva entre a Americanização e a Europeização", *A Inteligência Artificial no Direito Penal*, Coord. Anabela Miranda Rodrigues, Almedina, 2020, p. 17s e 24s; *vide*, também, DE JONG, Nathalie, "État des lieux des legaltech en France", *La Semaine Juridique* – Édition Générale. Supplément au N.º 44-45 – 28 Octobre 2019, LEXISNEXIS SA, p. 31s.

11. Cf. DE JONG, Nathalie, *op. cit.*, p. 34.

vista reduzir a álea judicial ou aumentar a previsibilidade das decisões. Dentre as possibilidades oferecidas, referem-se *outputs* quanto a probabilidades de sucesso relativamente ao resultado de um caso (hipótese de «ganhar» um processo); montante de uma indemnização ou *quantum* de uma pena; ou argumentos de direito mais pertinentes.

1. PREVISÃO DEDECISÕES DE LITÍGIOS EM TRIBUNAL

Vale a pena começar por referir que a *Legaltech*[12] tem conhecido um grande desenvolvimento, designadamente no setor da advocacia. Os advogados já dispõem hoje de sistemas de análise de dados para previsão das decisões judiciais, criados por empresas privadas. Utilizam técnicas de *Big Data* judicial, *machine learning*, algoritmos de semelhança e proximidade e técnicas de processamento de linguagem natural (PNL). Do que se trata é de "fazer falar" as decisões judiciais. O *software* seleciona e extrai os dados relevantes, principalmente das bases de dados judiciais, e processa-os, utilizando sistemas de IA para facilitar ao usuário a analítica jurisprudencial preditiva.

Na Europa, a França[13] é provavelmente o país onde o "negócio" da *Legaltech* está mais desenvolvido: o ecossistema francês da tecnologia jurídica contava, em 2019, com mais de 200 atores, não deixando de se fazer notar que, na atividade destes novos agentes, o setor da justiça *preditiva* –a análise preditiva de casos– representa apenas 3% do conjunto da sua atividade. Nesta área, a *Case Law Analytics*, uma *startup* francesa criada em 2017, é um exemplo de oferta de quantificação do risco que comportam as decisões judiciais através de uma plataforma equipada com IA. De qualquer modo, não deve deixar de se assinalar que, neste momento, em França, o debate é especialmente vivo em torno da análise preditiva de casos[14]. Na verdade, na sequência da aprovação da *Lei sobre a République numérique*, de 6 de outubro de 2016, tendo em vista garantir a maior transparência sobre o funcionamento dos tribunais, a Administração foi obrigada a disponibilizar *on line* todas as decisões judiciais tomadas em território francês – desde a 1.ª instância até ao Conseil d'État ou à Cour

12. Uma aproximação possível ao conceito de *Legaltech* diz respeito a empresas que utilizam as novas tecnologias para proporcionar soluções inovadoras, não só aos diversos profissionais do direito como também aos destinatários da justiça, pessoas físicas e coletivas.

13. Cf. DE JONG, Nathalie, "État des lieux des legaltech en France", *La Semaine Juridique* – Édition Générale. Supplément au N.º 44-45 – 28 Octobre 2019, LEXISNEXIS SA, p. 31 e 34.

14. Cf. RIVOLLIER, Vincent, "Diffuser le nom des magistrats ou quele Conception de la justice en France?", *La Semaine Juridique* –Édition Générale. Supplément au N.º 44-45– 28 Octobre 2019, LEXISNEXIS SA, p. 26s, especialmente, p.28 e 29.

de Cassation, em todas as matérias, civil, administrativa ou penal. Foi, assim, criado um imenso banco de dados *open data*, muito apelativo para as *startup*s francesas de *Legaltech*. Todavia, apesar desta disponibilização se manter, uma Lei de março de 2019 veio incriminar o tratamento de dados relativos à identificação de magistrados tendo como objetivo a previsão das suas decisões[15].

A Espanha é outro país que vale a pena referir a este propósito, onde existem vários sistemas, criados por empresas muito poderosas do setor jurídico: podem referir-se a *Jurimetria*, uma das aplicações pioneiras na aplicação da justiça preditiva ao Direito, cuja empresa titular é a *Wolters Kluver*; ou a *Tirant Analytics,* que, entre outras funcionalidades, conta com mapas conceituais para a representação gráfica de cada sentença, a possibilidade de busca por posição processual "a favor" ou "contra" ou por probabilidade de êxito de cada parte, ou permite ainda busca com uma visão global de todos os valores em jogo, por forma a descobrir novas vias, outros procedimentos, outras provas e dados ocultos.

Há, entretanto, uma grande diversidade de utilizadores de serviços (*legaltecher*) e uma multiplicação de serviços oferecidos. A este propósito, refere-se, do ponto de vista dos profissionais e do grande público, a *democratização do acesso à informação jurídica* –favorecida por empresas como a *Doctrine* ou a *Predictice,* em França, que organizam e tornam acessível informação jurídica–, mas vai-se para além disso. Por exemplo, nos Estados Unidos da América, o *Tech Index of the CodeX Center for Legal Informatics*, da Universidade de *Stanford*, em setembro de 2022, registava mais de 1.900 empresas de *legaltech*, em setores como *compliance*, automatização documental, plataformas de *e-learning* para ensino e formação jurídica, investigação criminal, *marketplaces* ou plataformas de encontro entre clientes e advogados, resolução de conflitos em linha, práticas de governança, ferramentas de *e-discovery* e de revisão de documentos.

15. A Loi n.º 2019-222 du 23 mars 2019 – art.33 (V), designada por Loi de programmation et de reforme pour la justice (LPJ), dispõe que: "Les données d'identité des magistrats et des membres du greffe ne peuvent faire objet d'une réutilisation ayant pour objet ou pour effet d'évaluer, dánalyser, de comparer ou *de prédire leurs pratiques professionnelles réelles iu supposés.* La violation de cette interdiction est punie avec des peines prévues aux articles 226-18, 226-24 et 226-31 du code penal, sans préjudice des mesures et sanctions prévues par la loi n.º 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés" (itálicos nossos). Pelo que diz respeito ao sancionamento, verifica-se, assim, que estão previstas a aplicação de uma pena de prisão de cinco anos e uma pena de multa de 300.000 euros. Deve assinalar-se, entretanto, a entrega ao Presidente da República Emmanuel Macron, em 8 de julho de 2022, do relatório "Rendre justice aux citoyens", elaborado por um comité independente, no âmbito dos trabalhos dos Estados Gerais sobre a Justiça lançados em 18 de outubro de 2018, e presidido pelo Vice-Presidente do Conseil d'État Jean-Marc Sauvé (*Rapport Sauvé*).

Acentua-se, entretanto, que, no âmbito mais clássico da automatização dos serviços, a *Legaltech* não oferece apenas soluções para a realização de tarefas repetitivas e demoradas que a emergência da justiça digital permitiu, com o objetivo de otimização do tratamento e do tempo e da atividade[16] – no primeiro caso, diminuindo o risco de erros e obtendo ganhos de eficácia; no segundo caso, deixando tempo às pessoas para se concentrarem no fundo das questões, trazendo valor acrescentado para a sua resolução. Com efeito, Na Alemanha, o projeto *ARGUMENTUM*[17] é demonstrativo das virtualidades da tecnologia ao nível da argumentação em juízo, que requer esforço intelectual específico e informação abundante –em face das limitações inerentes à capacidade humana para processar informação–, foi desenvolvido um protótipo de *software* para auxiliar na identificação automática, análise e seleção de estruturas de argumentos jurídicos. Ao nível da automatização, a *Legaltech* é, para além disso e ainda, em um setor cada vez mais competitivo como é, designadamente, o da advocacia –basta pensar no número crescente de advogados um pouco por todo lado–, uma ferramenta "de comunicação" e um meio de aumentar a sua visibilidade para captar clientes. Existem também sistemas que combinam IA com *Big Data* para oferecer uma seleção de advogados com as respetivas taxas de sucesso ou tempo médio de resolução de casos[18].

Compreende-se que os desenvolvimentos da *Legaltech* estejam na origem de uma discussão muito viva sobre o impacto que terão sobre as profissões

16. Aponta-se, por exemplo, o *Allen and Overy*, um dos maiores escritórios de **advocacia** do mundo com experiência no setor bancário e financeiro, que utiliza uma aplicação de IA, a *MarginMatrix*, para analisar a regulação financeira em mais de 30 jurisdições e para redigir milhares de contratos sobre derivados *over-the-counter*, um mercado de 30 triliões de dólares. E também encontramos referências a advogados-robô: um jovem de 19 anos, que nem sequer era estudante de Direito, conseguiu tramitar com sucesso 160.000 multas de trânsito em Nova Iorque, fazendo poupar aos seus "clientes" 4.000.000 USD…

17. O Projeto de humanidades digitais *ARGUMENTUM* visa explorar o potencial e os limites de métodos e técnicas da ciência da computação e da IA para aplicações inovadoras no domínio de humanidades digitais, especialmente para efeitos de argumentação. Sobre o Projeto *ARGUMENTUM*, cf. HOUY, C., P. FETTKE, P., LOOS, P., SPEISER, I., M. HERBERGER, M., GASS, A., e U. NORTMANN, U., "ARGUMENTUM – Towards computer-supported analysis, retrieval and synthesis of argumentation structures in humanities using the example of jurisprudence, presented at the KI-2012: Poster and Demo Track of the 35th German Conference on Artificial Intelligence (KI-12), Saarbrücken, Germany, 2012; sobre o conceito básico para a preparação e tratamento do *corpus* de decisões do Tribunal Constitucional Federal Alemão na base do *software* protótipo do *ARGUMENTUM*, HOUY, C., NIESEN, T., FETTKE, P., LOOS, P., "Towards Automated Identification and Analysis of Argumentation Structures in the Decision Corpus of the German Federal Constitutional Court", 6833_IEEE_DEST_2013_Houy_Niesen_Fettke_Loos.

18. Nos Estados Unidos da América, a PREMONITION A. I. constitui um bom exemplo de uma ferramenta deste tipo.

jurídicas, desde logo na advocacia. Se bem que, como se salientou, a sua atividade, um pouco por todo o lado, esteja mais concentrada em inovações relativas a soluções de gestão de informação, listagem de leis e de decisões ou redação de contratos "inteligentes" do que em algoritmos de justiça preditiva, as transformações podem ser mais profundas, projetando os seus efeitos para além das tarefas de rotina e afetando as atividades cognitivas e criativas[19]. Defende-se, todavia, que a IA vai empoderar os advogados –os bons advogados, sublinha-se–, permitindo-lhes ser mais produtivos e eficientes na realização das suas tarefas, a menor custo. Neste contexto, eles não serão substituídos por *legalbots*, se se "transformarem": o advogado do futuro, para além de saber direito e entender de tecnologia, deve desenvolver competências interpessoais (*soft skills*) que o tornarão insubstituível pela máquina, tais como liderança, criatividade, empatia, gestão e resolução de conflitos ou articulação de relações interpessoais. O exercício de profissões jurídicas como a advocacia não pode ser reduzido a uma "agência de informações" –o digital pode melhorar e tornar mais barato o acesso à justiça e isso é bem-vindo–; mas o direito abrange questões éticas e é uma experiência social e humana. Para além disso, o desafio está nos novos papéis para as profissões jurídicas ou mesmo de novas profissões jurídicas que as novas tecnologias implicam: a referência é, agora, aos analistas de riscos jurídicos, engenheiros de conhecimento jurídico (*legal knowledge*), arquitetos e gestores de contratos, gestores de projetos jurídicos (*legal project managers*) e os chamados híbridos, os profissionais que combinam conhecimentos jurídicos com informáticos, económicos e estatísticos.

Este panorama brevemente traçado esconde, no entanto, um perigo para que deve alertar-se[20]. O risco de que os modelos de *IA Legaltech* substituam os advogados existe para aqueles que permanecerem agarrados a um modelo tradicional de advocacia, em face das novas regras ditadas pela tecnologia ou, de outra perspetiva, para advogados juniores e assistentes de advogados, que, justamente, desempenham tarefas repetitivas e demoradas. Nestes casos, um robô, incluindo um advogado robô, fará provavelmente a sua aparição…

2. JUÍZES E UTILIZAÇÃO DE IA NOS PROCESSOS DE TOMADA DE DECISÕES

No âmbito da utilização de IA nos processos de tomada de decisões durante o processo, deve falar-se de *instrumentos de avaliação do risco*. Está

19. Assim, SUSSKIND, Richard, *Online Courts and the Future of Justice*, Oxford University Press, 2019, p. 273s.

20. Cf., nesta linha, GARAPON, *Dalloz Actualité*, Édition du 13 juillet 2022, *passim*.

em causa, com eles, a utilização de algoritmos que analisam um número muito elevado de dados relativos à pessoa envolvida no processo e ao seu passado e estabelecem padrões (*pattern*), com vista a obter uma *previsão sobre a sua perigosidade criminal.*

No momento[21], são ainda instrumentos mais difundidos em alguns ordenamentos de *common law*, designadamente nos Estados Unidos da América e no Reino Unido, e principalmente no âmbito da *parole*, mas também alargados a decisões de caução (*bail*) e de *sentencing*. Nos últimos anos, assistiu-se a uma explosão da utilização de instrumentos algorítmicos de avaliação do risco na justiça norte-americana. No âmbito da *sentencing*, o COMPASS é, provavelmente, o mais conhecido, através da sua utilização no que já se pode considerar como um *leading case* –o caso *Loomis*–[22]. O próprio *Model Penal Code*, revisto em 2017, exortou ao emprego de instrumentos atuariais (*actuarial instruments*) deste tipo.

Em contraposição a este quadro, na Europa continental é ainda rara a utilização de instrumentos preditivos. Isto deve-se, do meu ponto de vista, e desde logo, ao modelo de justiça penal posto em prática nos sistemas anglo-saxónicos, refletido, antes de mais nada, nas *finalidades da punição*: como é sabido, a reabilitação foi posta em causa sobretudo por uma lógica de eficácia e pelas *preocupações com a disparidade das penas aplicadas*; depois, relaciona-se com o tipo de processo penal ou, noutra formulação, a forma de fazer justiça penal: do lado americano, as fases de *sentencing* assumiram, no processo, uma importância crescente –para o que contribuiu também um sistema baseado cada vez mais na *guilty plea* e na *plea bargaining*, com *efeito burocratizante* na discussão do caso propriamente dito–, em comparação com os sistemas de justiça europeia continental, onde continua a manter destaque a fase de julgamento –de discussão da *questão da culpa*–, com intensa intervenção humana e menos possibilidade de introduzir instrumentos de predição.

Em última análise, amplifica o *gap* na utilização de instrumentos preditivos nos sistemas de *common law* e romano-germânicos o facto de a jurisprudência ser, ali, *horizontal*, levando-se o mais longe possível, nos EUA, designadamente, o princípio do "tratamento igual dos casos semelhantes"; e, nestes, ser *vertical*, apoiando-se no controlo exercido pelos tribunais superiores sobre a fundamentação das decisões dos tribunais inferiores.

21. Para mais desenvolvimentos sobre isto e o que se segue, cf. MIRANDA RODRIGUES, Anabela, "Inteligência Artificial no Direito Penal – a Justiça Preditiva entre a Americanização e a Europeização", *A Inteligência Artificial no Direito Penal*, Coord. Anabela Miranda Rodrigues, Almedina, 2020, p. 17s.

22. Cf. CARIA, Rui, "O caso *State v. Loomis* – a pessoa e a máquina na decisão judicial", *A Inteligência Artificial no Direito Penal*, Coord. Anabela Miranda Rodrigues, Almedina, 2020, p. 245s.

A menção já feita aos "juízes robôs" projetados na Estónia, utilizados para decidir casos bagatelares, são uma exceção no contexto europeu, e dizem respeito a decisões que podem ser *praticamente* automáticas, sem necessidade de intervenção humana. Poder-se-á comparar este domínio a outros domínios do direito, como o da elaboração de contratos: quando se trata de contratos em massa, sistemas autónomos podem processá-los de forma mais rápida e com falhas mínimas.

Para além deste caso, o panorama geral é o de os juízes não contarem com sistemas autónomos ou de IA na justiça preditiva. De assinalar[23], entretanto, no sistema jurídico espanhol, a utilização de um instrumento de predição do risco de violência –o RisCanvi–, utilizado pelos juízes apenas no sistema penitenciário catalão, designadamente para decidir sobre licenças de saída ou liberdade condicional.

III. RISCOS E LIMITES DAJUSTIÇA PREDITIVA APLICADA À JUSTIÇA PENAL

Aqui chegados, a questão já não é tanto ser a favor ou ser contra a justiça penal preditiva – ela *está* aí! O que se vem dizer é que ela não é –não tem de ser, nem deve ser– necessariamente, a que delega, na totalidade, a tomada de decisões em máquinas –além disso, em máquinas que são hoje *inteligentes*–, suprimindo a intervenção humana, como uma certa visão distópica sugere. Aponta-se, a este respeito, um modelo de colaboração entre as capacidades humanas e as vantagens de sistemas autónomos e de IA[24].

De qualquer forma, assume a maior importância ter em conta os **riscos** e traçar **limites** à nova justiça penal preditiva.

1. A QUESTÃO DO DETERMINISMO (OS RISCOS)

Na questão da justiça preditiva está implícita a questão do determinismo do direito. Há um *novo* determinismo nesta *nova* previsibilidade[25].

23. Sobre isto, *vide*, por todos, RIVERA BEIRAS, Iñaki, "Actuarialismo penitenciário. Su recepción en España", *Revista Crítica Penal y Poder*, n.º 9, Septiembre, 2015, p. 102s (p.118s).
24. Cf. CARO CARIA, Dino Carlos, "Compliance, Neurociencias e Inteligencia Artificial/Compliance, Neuroscience and Artificial Intelligence", *on line*, https://neuralink.com/2022, p. 639.
25. Cf. MIRANDA RODRIGUES, Anabela, "Inteligência Artificial no Direito Penal – a Justiça Preditiva entre a Americanização e a Europeização", *A Inteligência Artificial no Direito Penal*, Coord. Anabela Miranda Rodrigues, Almedina, 2020, p. 43s. A este respeito, é fundamental a obra de GARAPON, Antoine/LASSÈGUE, Jean, *Justice*

Para caraterizar a justiça digital é fundamental ter presente que o digital introduz, na análise da *Garapon* e *Lassègue*, uma "rutura radical com o direito", inaugurando uma nova semiogénese do direito que deixa de passar pela linguagem. Introduz, mais precisamente, uma *outra legalidade*, que procede de uma linguagem autónoma que depende muito pouco do direito a "legalidade digital", no cruzamento da legalidade jurídica com a legalidade científica e tecnológica. E demonstra, além disso, uma eficácia incrível, beneficiando de uma autoridade que entra em concorrência frontal com a legalidade, eficácia e autoridade do direito tal como o conhecemos. O que está em causa vai muito para além do que se poderia considerar como mais um movimento de "*law and …*", no caso sendo *law and mathematics*, e de o direito encontrar o seu critério de validade no exterior de si mesmo. É neste sentido que o digital traz a rutura –constrói um terceiro externo-interno–: interno, porque a *Legaltech* não pretende extrair qualquer informação substancial de fora do direito; externo, porque se trata de um terceiro algébrico e não mais simbólico.

A lei, então, que perde o monopólio da expressão da vontade soberana, deve ser transposta para programas. Ela tem, naturalmente, uma versão escrita numa linguagem jurídica; mas tem de ser codificada, transcrita para a linguagem digital para ser efetiva. Ela é ilegível, embora sendo operativa. É a ideia de *legal by design*. Tome-se o exemplo das *Regtech*[26], que se propõem colocar em ligação os sistemas de reguladores e entidades reguladas, de modo a que modificações regulatórias alterem automaticamente as lógicas dos regulados.

Com esta ascensão do digital, é uma *revolutio* do direito que se prefigura. Só que ela não é obra de juristas, mas de informáticos que não sabem direito. Esta ignorância permite-lhes estabelecer padrões que escapam à teorização dos juristas e não são assimiláveis a regras com força normativa, mas que constituem uma referência importante para os práticos. Isto significa, sobretudo para estes, a passagem da **interpretação** para a exploração de uma massa de informações heterogéneas; da atividade com regras para a identificação de regularidades; da utilização da lei geral e abstrata para as injunções situacionais e pessoais.

Digitale, Révolution graphique et rupture anthropologique, Puf, 2018, passim (p. 169s); vide, também, GARAPON, Antoine/LASSÈGUE, Jean, "Autour de *justice digitale*: reencontre avec Antoine Garapon et Jean Lassègue", Société de legislation compare "Tribonien", 2018/2 N.º 2, p. 84-89 (https://www.cairn.info/revue-tribonien-2018-2-page-84.htm).

26. A este respeito, cf. MIRANDA RODRIGUES, Anabela, "*Compliance* inteligente e prevenção e luta contra o branqueamento", *A Inteligência Artificial e o Direito Penal*, Volume II, Coord. Anabela Miranda Rodrigues, Almedina (no prelo).

1.1. Pelo lado do juiz

A interrogação a colocar diz respeito a saber como se vai justificar a permanência do ser humano, designadamente de juízes, no processo de tomada de decisões no processo penal, se os resultados das decisões tomadas por sistemas de IA podem reunir uma série de condições que as tornam mais objetivas e credíveis. Esta questão prende-se com o facto de que, como já se referiu, os juízes decidirem sobre a responsabilidade criminal individual de pessoas e com a determinação da pena a aplicar-lhes[27] e não sobre assuntos técnicos ou científicos. O que se pretende destacar é que à função judicial está ligada a dimensão de compreensão do caso concreto e das caraterísticas da pessoa a ser julgada e punida, que é o elemento que assegura a prudência da decisão e favorece a sua aceitação pelos destinatários e pela comunidade. E, neste sentido, a interpretação[28] é inerente ao exercício da função, em qualquer processo de decisão que envolva determinar a culpa e punir quem cometeu um facto criminoso.

O que desde já se adianta é que uma operação algorítmica retira à decisão judicial a dimensão *humana* e de *responsabilidade* que, como tal, envolve, e o *sentido jurídico*. A manutenção e mesmo a preservação de um indeterminismo não calculável é necessário à construção de um sentido jurídico. Este aspeto[29] "é indispensável à constituição do direito como forma simbólica", referem *Garapon* e *Lassègue*. Que acrescentam: "O direito não é redutível à soma das prescrições positivas, porque ele oferece também a capacidade de transformar estas prescrições positivas ao mesmo tempo que mantém o seu poder prescritivo". Ora –concluem os autores– "o cálculo preditivo fecha o direito e priva-o desta capacidade".

A questão pode ser formulada assim: porque é que a relação dos humanos com o mundo tem de se fazer de acordo com o modelo matemático de uma função, se ela é *existencial*?[30]

---

27. Não se equaciona aqui a questão de decisões judiciais sobre a responsabilidade criminal e a aplicação de penas a pessoas coletivas, que merece uma reflexão autónoma.
28. Neste sentido, especificamente para a função judicial de determinação da medida da pena, MIRANDA RODRIGUES, Anabela, *A determinação da medida da pena privativa de liberdade. Os critérios da culpa e da prevenção*, Coimbra Editora, 1995, p. 79s (especialmente, p. 93 e 94); *id*, "Medida da pena de prisão –desafios na era da inteligência artificial", Revista de Legislação e Jurisprudência, Ano 149, N.º 4021, Março-Abril, 2020, p. 258s; *id*, "A questão da pena e a decisão do juiz entre a dogmática e o algoritmo", *A Inteligência Artificial no Direito Penal*, Coord. Anabela Miranda Rodrigues, Almedina, 2020, p. 219s (especialmente, p. 238).
29. Cf. GARAPON, Antoine/LASSÈGUE, Jean, *Justice Digitale, Révolution graphique et rupture anthropologique*, Puf, 2018, p. 237.
30. Apela-se, agora, a STRECK, Lénio L., *O que é isto – decido conforme minha consciência?*, Livraria do Advogado Editora, Porto Alegre, 6.ª edição, 2017, *passim*; cf., também,

É o determinismo do direito, no âmbito penal, que lhe traz a previsibilidade ligada à utilização de sistemas de IA nos processos de tomada de decisões, que é preciso agora interpelar nas *novas* consequências que implica ao nível da sua aplicação.

Destaca-se[31] como a passagem da escrita alfabética para uma escrita *digital* projeta o discurso de uma decisão judicial "para fora do direito", produzindo uma alteração do seu sentido e colocando-a no domínio de uma "mitologia geral" de inteligência *artificial*. Os programas informáticos não são da mesma ordem que a construção coletiva (humana) de sentido. É o pensamento que, com a sua reflexividade e originalidade, ganha a especificidade *humana*. O sentido humano é plurivocal e vale tanto para a linguagem como para as condutas simbólicas (por exemplo, vestir-se de uma determinada forma em um certo contexto). Nada disto vale para o tratamento informático, num sistema de *inputs* e *outputs*, exatamente porque a informação supõe que o sentido está definido antes e mantém-se fixo e determinado durante a interação. É evidente que o tratamento da informação compensa de alguma maneira esta fixidez e determinação de sentido, através da colocação em memória de todos os sentidos já encontrados. Mas… o facto de se armazenar na íntegra um dicionário de português, por exemplo, nada nos diz como como vai evoluir o sentido das palavras no futuro, o que nenhum dicionário pode conter! É a diferença entre um torneio de Go, em que uma máquina bateu, em 2016, o grande mestre sul-coreano *Lee Se-dol*, e um sistema aberto como é a linguagem natural, em que, diferentemente do jogo, a ideia de regra estrita não é pertinente. É assim que o tratamento de dados se afasta deliberadamente do raciocínio jurídico, desencadeando a passagem "da causalidade jurídica para a correlação prática". Fala-se de uma *nova* normatividade preditiva que, diferentemente da normatividade jurídica, não estabelece ligações entre proposições através da escrita alfabética, mas através de uma "pura correlação matemática" que não se funda no que as pessoas *vivem* na interação social em que participam. O simples tratamento digital de dados codificados desapossa a "nova norma» das

STRECK, Lénio L., BERNST, Luisa G., GOMES, Jefferson de Carvalho, "Inteligência Artificial: Mesmos Problemas, mas na Versão Hi-Tech/Artificial Intelligence: Same Problems, but un Hi-Tech Version", *Constituição, Economia e Desenvolvimento: Revista da Academia Brasileira de Direito Constitucional*, Curitiba, ago./dez, 2021, vol. 13, n.25, p. 333s (p. 338). Sobre a relação humana com o mundo externo, que não permite a nossa apreensão deste através simplesmente do cálculo e exige "sentido físico", LASSÈGUE, Jean, "L'Intelligence Artificielle, Technologie de la Vision Numérique du Monde", *Les Cahiers de la Justice*, 2019/2 N.º 2, p. 211s.

31. Vide, para o que se segue, GARAPON, Antoine/ LASSÈGUE, Jean, *Justice Digitale, Révolution graphique et rupture anthropologique*, Puf, 2018, p. 219s; e LASSÈGUE, Jean, "L'Intelligence Artificielle, Technologie de la Vision Numérique du Monde", *Les Cahiers de la Justice*, 2019/2 N.º 2, p. 208s.

duas dimensões, "social e hermenêutica", que caraterizam a norma jurídica e lhe conferem tantos conteúdos quantos os diversos tipos de ligações que a escrita alfabética permite. Com a nova norma, a decisão judicial procede da massa de dados a favor de uma solução e não do sentido da norma jurídica, obtido com a sua seleção, hierarquização e integração no direito. O sentido da decisão judicial resulta –nas palavras de *Garapon* e *Lassègue*[32]– "quer do próprio texto da decisão, quer do seu tratamento pela instituição para o erigir em jurisprudência". É exatamente esta relação que "é desvendada pelos *Big Data*": agora, "*quantitas non auctoritas facit legit*". É a massa das correlações –e não o raciocínio jurídico ou a *auctoritas* dos princípios– que *faz* a decisão. Cada caso alimenta um imenso banco de dados que permite uma previsão cada vez mais fiável da atuação da instituição e uma antecipação cada vez mais fina das decisões.

Isto convida, assim, a repensar as condições do exercício da função judicial com autonomia[33], mesmo quando se entende que a decisão judicial não se torna totalmente automática. Tendo em conta a tendência humana para confiar nos resultados de um procedimento automatizado, a submissão do juiz à máquina e a devolução da decisão sobre a punição ao algoritmo são riscos que não devem ser ignorados. Trata-se do fenómeno conhecido por *enviesamento automático* (*automation bias*), que ocorre quando um decisor humano não toma em conta ou não procura informação contrária, em face de uma solução gerada por um computador[34]. Há já uma elaboração teórica sobre este problema, que mostra como, uma vez oferecida por um instrumento *high-tech* um resultado, é extremamente oneroso para o humano refutar aquele resultado e tomá-lo apenas como uma "recomendação". Normalmente, a pessoa que tem de decidir valora de uma forma mais positiva do que neutral a recomendação automática, apesar de estar alertada para que pode ser incorreta, imprecisa ou incompleta. Em Espanha, com a utilização do RisCanvi, assinala-se que apenas em 3,2% dos casos o juiz se afasta da decisão tomada pelo sistema.

Esta forma de "pressão" sobre o juiz é nova, não tanto ou não só na medida em que equivale, sob forma digital, à consciência coletiva –da instituição judiciária– presente na consciência do juiz quando decide o caso particular, mas enquanto funciona como um controlo de natureza diferente

32. *Op. ult. cit*., p. 226.

33. A referência pode entender-se como feita à independência do poder judicial, nesta nova dimensão.

34. Cf. CUMMINGS, M. L., "Automation bias in Intelligent Time Critical Decision Support Systems", https://arc.aiaa.org, 2012, p. 2; e FREMMAN, K., "Algorithmic injustice: how the Wisconsin Supreme Court failed to protect due process rights in state v. Loomis", North Carolina Journal of Law and Technology, Vol.18, Issue 5, 2016, p. 75-106 (https://scholarship.law.unc.edu/ncjolt/vol18/iss5/3).

do hierárquico –que tem no recurso para os tribunais superiores a sua expressão–, exercido diretamente sobre o medo de fazer ou ser diferente do juiz. Esta espécie de "normatividade secundária que se substitui à norma de direito" e em que se transforma a justiça preditiva impele ao conformismo. Esta pressão, que não é assumida pelo juiz, arrisca-se a distrair o juiz da sua própria experiência profissional e a impedi-lo de fazer valer a interpretação na decisão. O que mais teme este novo juiz é estar isolado, ser designado como a "ovelha tresmalhada" do sistema, desviar-se do "padrão dado pela máquina. A 'nova' pressão evoca o poder performativo do digital, enquanto «sistema de recomendações" que exerce nos juízes uma influência de cunho *especial*, apesar de não pretender fornecer-lhes "a" solução, como já se adiantou. Pode ser, ainda, "horizontal", "dissimulada" ou "espontânea", "inconsciente", enquanto lhes indica "o que cem colegas seus decidiriam em casos semelhantes". Esta pressão sobre os juízes coloca a justiça como *fairness* em contraponto com uma justiça como *fitness*[35].

A jurisprudência é um sistema de sabedoria coletiva *autocorretiva*. A lição contida na publicação da opinião dissidente colhida do *common law* incentiva a argumentação jurídica e ilustra bem como um julgamento é um raciocínio coletivo, com uma dinâmica que impede o juiz de se deixar formatar[36].

A questão vai para além da opacidade do algoritmo (*black box problem*) e das soluções que podem ser pensadas para se obter uma explicação de uma tomada de decisão. Num contexto técnico, basta uma linguagem matemática clara, que já permite auditorias algorítmicas ou a um supervisor entender *ex post* como é que o processo evoluiu dos *inputs* para os *outputs*. Que, para o direito –para os sentidos jurídicos– não é suficiente. A questão é ainda mais profunda e diz respeito ao próprio enviesamento algorítmico (*algorithmic bias*). O que –diz-se– pode ser corrigido. Então, a deixar ficar no ar a possibilidade de inventar o Algoritmo Mestre[37]…

35. Assim, GARAPON, Antoine/LASSÈGUE, Jean, *Justice Digitale, Révolution graphique et rupture anthropologique*, Puf, 2018, p. 316, que referem como a "nova" pressão sobre os juízes é reveladora de uma reorganização mais geral do controlo, que logra menos a forma de uma normalização direta e autoritária dos comportamentos e mais de uma pressão sobre o alinhamento das decisões e como este controlo é bem conhecido, em geral, da sociedade contemporânea, expressando-se pela lógica do binómio inclusão/exclusão, parte/pária (p. 282 e 283).
36. Cf., a este propósito, a solução do Código de Processo Penal Português (Artigos 367.º, n.º 1 e 372.º, n.º 2). Sobre isto, cf. GARAPON, Antoine, *Interview, Dalloz Actualité, Le quotidien du droit. Édition du 13 Juillet* 2022, https://www.daloz-actualite.fr/printmail/interview/antoine-garapon-numerique-est-un-remede-lenteur-de-justice.
37. A referência é, agora, ao bem conhecido cientista informático português Pedro Domingos e ao seu conhecido livro: *A Revolução do Algoritmo Mestre. Como a Aprendizagem Automática Está a Mudar o Mundo*, 1.ª edição, Lisboa, outubro de 2017.

Acontece que, numa tomada de decisão judicial, sobretudo de cariz penal, está em causa um processo que, para ser compreendido e aceite pelos seus destinatários imediatos e pela comunidade, exige o que os juristas designam por fundamentação, que *obriga* o juiz a demonstrar o raciocínio feito para alcançar a decisão e a indicar os motivos pelos quais *aquela é a melhor decisão para o caso* –em termos dworkianos, correta: não importa o que os juízes pensam sobre o direito, mas sim o ajuste (*fit*) e a justificação (*justification*) da interpretação que eles oferecem das práticas jurídicas em relação ao direito de uma comunidade política[38]–, não podendo, pois, tomar decisões com base unicamente em cálculos de sistemas de IA.

A questão tem a ver com o *método* utilizado no âmbito da IA e é explicada por *Jean Lassègue*[39]. Traduz-se numa relação entre o ambiente e os esquemas de ação, que a maior parte das vezes implica opções executadas de forma automatizada. Estes esquemas de ação, na medida em que são capazes de se repetir, apelam a diferentes modos de cálculo, quer se trate de programas quer de redes neuronais. Avulta, então, o lugar do observador na sua relação com o objetivo: num caso, o objetivo consiste em atualizar um conjunto de regras fixadas antecipadamente e redigidas depois sob a forma de programas –o que vale por dizer que é possível desenvolver uma atividade a partir de "estados internos" que não se deixam transformar pelo ambiente mas que reagem somente a partir dele; noutro caso, estão em causa esquemas de ação que se alimentam do ambiente que os transforma, sem que esta transformação seja integralmente descritível em regras fixadas antecipadamente– o que está em causa é observar do exterior a forma que toma a interação entre esquema de ação e ambiente, para tentar determinar o efeito de adaptação que essa interação mantém com o objetivo visado pelo esquema de ação. É aqui que surge a interpretação como uma exigência permanente, porque o que se considera como objetivo releva de um acoplamento de que não se conhece antecipadamente a forma, que não está fixada definitivamente em uma regra.

Nem a explicabilidade substitui a interpretação, nem a racionalidade que se exprime na decisão judicial prescinde da interpretação.

Isto tem a ver com o que *António Damásio* nos ensinou no *Erro de Descartes* e com o Caso *Eliot*[40] ou o filósofo e cientista *M. Brady*, no seu

38. DWORKIN, Ronald, *Levando os direitos a sério*, trad. Nelson Boeira, Martins Fontes, São Paulo, 2002, p. 127s.

39. LASSÈGUE, Jean, "L'Intelligence Artificielle, Technologie de la Vision Numérique du Monde", *Les Cahiers de la Justice*, 2019/2 N.º 2, p. 213s.

40. DAMÁSIO, António, *O Erro de Descartes. Emoção, razão e cérebro humano*, 1994.

Emotional Insight: the Epistemic Role of Emotional Experience[41]: as emoções, que têm raízes no *self* físico do ser humano, são uma componente essencial do raciocínio *e da decisão*. Sem emoções, uma pessoa pode raciocinar, mas não pode decidir. As emoções motivam-nos a encontrar razões, que, elas próprias, *não são* razões; mas são reflexivas: quando refletimos, as emoções podem alargar a perspetiva do agente, corrigir preconceitos e refinar o julgamento. Isto é *essencial para a decisão*, também judicial. Por seu turno, os destinatários estão mais dispostos a aceitar uma decisão se pensam que é *fair.* Por vezes, uma decisão tem de ser adaptada às partes por forma a permitir-lhes partilhar o seu próprio conteúdo. Isto é um aspeto fundamental da decisão, que o raciocínio dedutivo reproduzido por um sistema de IA não pode incluir.

Outro aspeto tem a ver com o processo de decisão do juiz[42]. Não precisamos de ir ao realismo jurídico nem ao seu renomado intérprete –o juiz norte-americano *Jerome Frank,* que dizia que a decisão judicial não é previsível, porque é o resultado de uma intuição e não de um raciocínio e que o juiz chega a uma decisão antes de a tentar motivar–, nem relembrar a sua fórmula caricatural –a justiça "*is what the judge ate for breakfast"*–, hoje desmistificada em vários estudos[43]. A *Ilusão de Ponzo* é suficiente para nos manter alerta perante a hipótese de arbitrariedade da decisão judicial e para nos conduzir na tentativa de perceber como é que é possível melhorar o processo de raciocínio humano. Que, entretanto, não se deixa aprisionar nas teorizações de cognitivistas ou em raciocínios dedutivos: ali, quando os sistemas intuitivos não são devidamente articulados com os sistemas analíticos; aqui, porque quando o juiz decide –*judgement in law*–, a dedução não pode ser tão rigorosa como a regra descrita na disposição, porque a efetiva aplicação da regra ao caso depende da interpretação da

41. BRADY, M., *Emotional Insight: The Epistemic Role of Emotional Experience,* Oxford, Oxford University press, 2014.

42. A este propósito, cf. THE JUDGE OF THE FUTURE: ARTIFICIAL INTELLIGENCE AND JUSTICE, Team Italy 2 – THEMIS 2019 Semifinal D – *Judicial Ethics and Professional Conduct*, *passim*.

43. Cf. DANZIGERA, Shai, LEVAVB, Jonathan and AVNAIM-PESSOA, Liora, "Extraneous factors in judicial decisions", Edited by Daniel Kahneman, Princeton University, Princeton, NJ, and approved February 25, 2011 (www.pnas.org/egi/doi/10.1073/pnas.1018033108), cujo estudo mostra que oprocesso de decisão humano em geral, e também o dos juízes, não é imune à influência de fatores externos irrelevantes: "the likelihood of a favorable ruling is greater at the very beginning of the work day or after a food break than later in the sequence of cases. (…) the likelihood of a ruling in favor of a prisoner spikes at the beginning of each session–the probability of a favorable ruling steadily declines from ≈0.65 to nearly zero and jumps back up to ≈0.65 after a break for a meal. (…) from the perspective of the prisoner, there is a clear advantage to appearing at the beginning of the session (i.e., either at the beginning of the day or immediately following the break)".

disposição. *Aristóteles* referiu-se já ao "silogismo imperfeito" o que requer a adição de vários objetos, necessários, mas que não foram assumidos nas premissas. Que não pode ser reproduzido pela IA. Um exemplo do que está em causa é o da ponderação entre direitos ou liberdades, que depende das particulares circunstâncias do caso que não podem ser reduzidas a uma dedução perfeita.

1.2. Pelo lado do delinquente

O determinismo da nova normatividade faz sentir os seus efeitos também pelo lado do delinquente.

Um aspeto pode equacionar-se como "o desaparecimento da lei" a que já nos referimos[44]. A escrita alfabética da lei operava uma mediação essencial e indispensável à realização de duas qualidades essenciais do direito: a sua generalidade e a igualdade face a todos. A revolução simbólica do digital alterou o equilíbrio desta relação entre o indivíduo e (o direito através d)a lei geral e abstrata e igual para todos. Reconhece-se[45] que o conceito de previsibilidade tem um significado especial no âmbito da moderna conceção de legalidade. A teoria da previsibilidade das normas penais parte de uma teoria liberal da lei penal e encontrou um farol na famosa crítica de *Bentham* aos juízes ingleses. A lei penal deve ser prévia, clara e certa para que as pessoas possam saber as consequências dos seus atos e autodeterminar-se de acordo com ela. Mas é preciso perguntar se esta função da lei é a mesma que é prometida, designadamente, pelos novos instrumentos de *mining* e análise de todas as decisões de uma jurisdição, procurando padrões de correspondência entre decisões e (modo de ser de) juízes, ou com a utilização de instrumentos de avaliação do risco. Desta forma, para além de se assinalar, como já se referiu, a alteração que implica a revolução digital da própria conceção de direito e uma "transformação interna da normatividade" e como o conhecimento preditivo é não só performativo como conservador[46], importa agora destacar como a justiça digital, paradoxalmente,

44. Assim, e no que que se segue, GARAPON, Antoine/LASSÈGUE, Jean, *Justice Digitale, Révolution graphique et rupture anthropologique*, Puf, 2018, p. 245s; também, MIRANDA RODRIGUES, Anabela, "Inteligência Artificial no Direito Penal – a Justiça Preditiva entre a Americanização e a Europeização", *A Inteligência Artificial no Direito Penal*, Coord. Anabela Miranda Rodrigues, Almedina, 2020, p. 46s.

45. Cf. QUATTROCOLO, Serena, "An introduction to AI and criminal justice in Europe", *Revista Brasileira de Direito Processual Penal*, Vol.5, N.º 03 – set./dez. 2019, p. 1541.

46. Neste sentido, GIALUZ, Mitja, "Quando la Giustizia Penale encontra l'Intelligenza Artificiale: Luci e Ombre dei *Risk assessment Tools* tra Stati Uniti ed Europa", *Diritto Penale Contemporaneo*, 2019, p. 21. No âmbito da política punitiva, sobre a alteração substancial que qui está implicada, em geral e sobretudo ao nível da determinação da medida concreta da pena de prisão, cf. MIRANDA RODRIGUES, Anabela,

acaba por conferir um maior peso ao passado em detrimento do futuro e corre o risco de bloquear qualquer tentativa de mudança do indivíduo. O delinquente – que está então adstrito a um futuro que depende de um cálculo sobre as suas possibilidades futuras determinadas em função de caraterísticas do seu passado identificadas e avaliadas por instrumentos de IA e que pode ter de passar um longo período na prisão em virtude de um mau *scoring* – perdeu a liberdade, aberta pela lei, de mobilização das suas capacidades internas de que ninguém conhece antecipadamente as potencialidades. O seu futuro está comprometido numa nova relação entre ele e os *big data*, que produz o oxímoro de uma lei *individual*. A capacidade de resposta do delinquente é supérflua, já que a solução para o seu comportamento futuro é encontrada numa previsão determinista saída de um cálculo. Esta é a sua lei, no sentido de que é a lei que vale –só– para ele. Longe da lei kantiana ou rousseauniana e do sujeito autónomo que se dá a si mesmo a sua lei, *ele é, ele mesmo, a sua lei*[47].

Da mesma forma que ficou comprometido o modo como os indivíduos são interpelados pela norma –deixaram de ser chamados para explorar as suas próprias capacidades e passaram a ficar "colados" a uma categoria pré-constituída–, também a norma jurídica perdeu, erradicada pela revolução digital, a plasticidade que lhe permite reelaborar-se pela interpretação – esse ir e vir entre a norma e o facto que cria a norma na sua aplicação. "A lei tornou-se muda"[48]. É aqui que se inscreve, ainda, a orientação seguida nos Estados Unidos no âmbito da justiça penal no sentido de uma *evidence based sentencing*, em que a punição deve desligar-se da gravidade do facto para passar a ser proporcionada ao risco que o indivíduo representa para a sociedade. Esta prática de uma "condenação baseada em dados", vai contra séculos de doutrina penal que se reclama de um *direito penal do facto*. O direito penal esforça-se por distinguir o facto praticado e censurável das motivações pessoais e do comportamento geral, anterior e posterior ao facto, do indivíduo, tomando-as em consideração na medida em que são suscetíveis de o esclarecer e apreender na sua totalidade. Mas isto significa tomar em conta a pessoa por detrás do facto, numa certa medida ainda também para lhe aplicar uma punição adequada, mas não o regresso a um direito penal de preconceitos e pré-juízos, que surge

"A questão da pena e a decisão do juiz – entre a dogmática e o algoritmo", *A Inteligência Artificial no Direito Penal*, Coord. Anabela Miranda Rodrigues, Almedina, 2020, p. 219s (especialmente, p. 220s e 230s., pontos 2. e 3., 3.1.).

47. Assim, GARAPON, Antoine/LASSÈGUE, Jean, *Justice Digitale, Révolution graphique et rupture anthropologique*, Puf, 2018, p. 259: o sujeito "secreta ele próprio a sua lei, pelo seu comportamento e pelo seu modo de vida. (…). Esta lei não foi coletivamente decidida (…), está inscrita no seu comportamento individual".

48. *Id, ibidem*, p. 255.

disfarçado pelo digital. Agora, é o perfil algorítmico –aquilo que o agente *é* algoritmicamente– que faz desaparecer o facto praticado e a interpretação é erradicada e substituída pelo determinismo. Uma dimensão que a justiça preditiva não pode tomar em consideração é a do *contexto tal como foi vivido* pelo delinquente que comete um crime, por oposição ao *contexto tal como os big data o pode formalizar*. Perspetiva-se o comportamento humano no enquadramento preditivo de um computador e de acordo com uma nova normatividade algorítmica –feita de padrões–, que pesa, não apenas a favor da renúncia à interpretação do julgar, como, além disso, da progressiva desvalorização do momento do julgamento, que persiste em permanecer caro aos sistemas de *civil law*.

Importa, mais uma vez, ter presente, com efeito, que o relevo que assume a previsibilidade e, por aqui, a aplicação de IA à justiça penal nos sistemas de *common* e *civil law* é diferente, sendo que é reconhecidamente menor o seu impacto na justiça penal dos sistemas romano-germânicos. Há vários aspetos fortemente enraizados nos sistemas europeus de *civil law* que lhe retiram espaço e enfraquecem esta caraterística de previsibilidade, como os atinentes à estrutura da carreira judiciária, com repercussões sobre o recrutamento de magistrados e os diferentes modelos de formação, a conferir ao poder judiciário caraterísticas específicas de autonomia e independência. Designadamente, com um corpo de juízes anónimos com competências (mais) técnico-jurídicas (do que políticas) a orientarem o seu processo de decisão em função do caso concreto *sub judice*. E em que o precedente, por contraposição ao sistema de *common law*, lhes é de menor valor a orientar a tomada de decisões. Mas não sem que, apesar da ausência de *stare decisis*, se detete um deslizar para exigências de fundamentação acrescidas em caso de decisões que fogem à regra ou menos à vontade dos juízes em se afastarem de decisões-regra.

2. A REGULAÇÃO (OS LIMITES) LIMITES)

De um ponto de vista jurídico, torna-se exigível que o critério da eficácia que se liga à utilização de IA na justiça penal seja perspetivado em função de outras variáveis. O aspeto da regulação é, então, particularmente importante. A minha geração tem particular responsabilidade a este respeito. Realmente, um *turning point* como o que tivemos o privilégio de viver, que significou a entrada na *infosfera* –esse espaço indistinto entre o *online* e o *offline*–, só acontece uma vez numa geração. É por isso que se nos impõe desenvolver o nosso *projeto humano* para a era digital[49].

49. Qual é o nosso "projeto humano" (*human project*) para a era digital? – era a interrogação já formulada em 2018 por *Luciano Floridi*: cf. FLORIDI, Luciano, "Soft Ethics

Os Estados Unidos estão na linha da frente na criação de um enquadramento legal para a IA –com a promulgação, em 1 de janeiro de 2021, da *US National AI Iniciative Act*[50]– e a União Europeia deu um passo importante com a *Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de Inteligência Artificial*, apresentada em 21 de abril de 2021[51]. Também a China marcou posição, com a aprovação, em março de 2022, de regulação –as *Internet Information Service Algorithmic Recommendation Management Provisions*–, embora limitada ao uso de algoritmos pelas empresas em sistemas de comunicação *on line*. A este respeito, direi, apenas –quaisquer considerações implicariam uma abordagem aprofundada, que não cabem no espaço disponível deste texto–, que o desafio não reside na inovação digital, mas sim na governança digital. É possível e desejável aplicar aqui o pensamento de Nietzsche, expresso na conhecida formulação "Was mich nicht umbringt macht mich staarker"[52]. Uma posição não excessivamente prescritiva e mais baseada no risco, por um lado, e centrada no ser humano, por outro lado[53], tem, além disso, virtualidades para promover um desenvolvimento da IA "eticamente sólido, juridicamente aceitável, socialmente equitativo e ambientalmente sustentável"[54].

Neste contexto, deve ter-se em atenção que a gestão e proteção de dados pessoais é uma pedra angular para limitar os riscos de um mundo digital em expansão. O edifício jurídico construído a este respeito pela União Europeia evidencia esta preocupação –designadamente, o Regulamento

and the Governance of the Digital", *Philosophy and Technology,* February 2018 https://www.researchgate.net/publication/32324854.

50. A *National AI Initiave Act* de 2020 (DIVISION E, SEC. 5001) entrou em vigor em1 de janeiro de 2021. Encontra-se, neste momento, em tramitação no Congresso a *Algorithmic Accountability Act*, apresentada em fevereiro de 2022.

51. COM(2021) 206 final, Bruxelas, 21.4.2021 (Proposta de Regulamento Inteligência Artificial). Sobre a Proposta de Regulamento, cf. FLORIDI, Luciano, "The European Legislation on AI: a Brief Analysis of its Philosophical Approach", *Philosophy & Technology* (2021) 34:215 ttps://doi.org/10.1007/s13347-021-00460-9.

52. Na seu livro *Götzen-Dämmerung oder Wie man mit dem Hammer philosophirt*, lançadoem 1889.

53. São estes os dois aspetos identificados pela União Europeia que devem orientar a intervenção reguladora no domínio da IA, contidos no *Livro Branco sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança*, Bruxelas, 19.2.2020 COM (2020) 65 final. Para mais desenvolvimentos, cf. MIRANDA RODRIGUES, Anabela, "Inteligência Artificial no Direito Penal – a Justiça Preditiva entre a Americanização e a Europeização", *A Inteligência Artificial no Direito Penal*, Coord. Anabela Miranda Rodrigues, Almedina, 2020, p. 38s.

54. Assim, FLORIDI, Luciano, "The European Legislation on AI: a Brief Analysis of its Philosophical Approach", *Philosophy & Technology* (2021) 34:215 ttps://doi.org/10.1007/s13347-021-00460-9, numa referência à Proposta de Regulamento de Inteligência Artificial) e que aqui generalizamos.

Geral da Proteção de Dados (RGPD)[55] e o Regulamento que estabeleceu a Autoridade Europeia para a Proteção de Dados[56]–, sendo de salientar, para o que agora nos interessa, no ordenamento jurídico português, que a Lei n.º 58/2019, de 8 de agosto, que assegura a execução do RGPD, é mais protetora das pessoas do que o RGPD[57], uma vez que *não prevê* que o consentimento do titular dos dados legitime a sua sujeição a uma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis. Assim[58], exceto quando são autorizadas por lei e desde que seja previsto o direito de o titular dos dados obter a intervenção humana do responsável pelo tratamento, *são proibidas* as decisões tomadas exclusivamente com base no tratamento automatizado, incluindo a definição de perfis. Devendo ainda acrescentar-se que o mesmo vale nos termos da lei que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais[59].

IV. A CONCLUIR

Não comungando eu de qualquer culto tecnófilo, julgo poder dizer que, por ora, quando se enumeram as realizações da IA e as suas finalidades, estamos relativamente equilibrados entre benefícios e malefícios.

Para o melhor, num universo alargado, temos de considerar a melhoria do acesso e da elaboração do conhecimento, o auxílio que representa nas deslocações no espaço ou no ar ou os progressos de que é credora no campo médico. No domínio estrito da administração da justiça, a redução de custos e da sua lentidão e atrasos, conjuntamente com a previsibilidade que oferece, sobretudo em casos simples, são vantagens que, além do mais, vão ao encontro das aspirações dos seus destinatários.

55. Regulamento (UE) 2016/679, de 27 de abril relativo à proteção de dados das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral da Proteção de Dados – RGPD).
56. Regulamento (UE) 2018/1725, de 23 de outubro relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados,
57. Cf. Artigo 22.º RGPD.
58. Cf. Artigo 11.º, n.º1, Lei n.º 58/2019, de 8 de agosto.
59. Lei 59/2019, de 8 de agosto, que transpõe a Diretiva 2016/680, de 27 de abril de 2016. Cf. Artigo 11.º, n.º 1: "São proibidas as decisões tomadas exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produzam efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa, exceto quando autorizadas por lei, desde que seja previsto o direito de o titular dos dados obter a intervenção humana do responsável pelo tratamento".

O digital pode ainda libertar a justiça em geral, e a penal em particular, do quadro espácio-temporal, ritual e heurístico do processo, dando lugar a uma nova *justiça aumentada*: pode proporcionar aos juízes o conhecimento da sua própria produção e aumentar a sua consciência sobre a sua própria prática, permitindo-lhes corrigir os seus vieses cognitivos e julgar-decidir melhor.

Para o pior, podem enumerar-se dificuldades contidas no que disse já especificamente para a justiça penal e que agora generalizo: os perfis estatísticos, através do cruzamento de dados; a manipulação de opiniões, através de perfis psicológicos em grande escala; a tendência a não ver o indivíduo senão como um exemplar estatístico de um tipo geral; ou a perda de controlo dos mercados financeiros, onde as ordens de compra e venda são executadas por máquinas, em prazos demasiado rápidos para serem seguidas ou contestadas por humanos. As referências a este respeito podem encontrar-se nos escândalos da *Cambridge Analytica* ou do *Facebook* ou nas derivas racistas, sexistas, de classe, ou ligadas à pobreza.

No início deste estudo, comecei por fazer notar como a noção de humano pode desaparecer do conceito de inteligência e tentei mostrar como isso acontece e como tal mudança –que implica uma nova forma da nossa relação com o mundo– nos é alheia como humanos.

No final, sugiro agora que a verdadeira alternativa que se coloca e sobre a qual temos de decidir, subjacente às finalidades dos artefactos de sistemas de IA que queremos criar e utilizar, é entre o *humano ser igual* à máquina ou o *humano ser diferente* da máquina – o que não é apenas uma questão técnica: é igualmente uma questão epistemológica.

Acrescento ainda: em última análise, é uma questão ética. Podemos entregar a realização da justiça penal a máquinas inteligentes, mas aquilo que temos de decidir é *se queremos* fazê-lo. E esta decisão é uma questão *ética* – uma opção nossa, eminentemente humana.

III

Cooperación judicial penal en la Unión Europea y digitalización

Capítulo 8

Órdenes europeas de retirada de contenidos terroristas en línea. [Análisis del nuevo instrumento introducido por el reglamento (UE) 2021/784][1]

Coral Arangüena Fanego

Catedrática de Derecho Procesal
Universidad de Valladolid

I. INTRODUCCIÓN. LA NECESIDAD DE COMBATIR LA DIFUSIÓN EN LÍNEA DE CONTENIDOS TERRORISTAS

Los actos terroristas constituyen una de las violaciones más graves de los valores universales de la dignidad humana, la libertad, la igualdad y la solidaridad, y el disfrute de los derechos humanos y de las libertades fundamentales, en los que se basa la Unión Europea. También representan uno de los ataques más graves contra la democracia y el Estado de Derecho, principios que son comunes a los Estados miembros y en los que se fundamenta la Unión. Se trata de una realidad que describe con estas precisas palabras el Considerando 2 de la Directiva (UE) 2017/541, relativa a la lucha contra el terrorismo[2].

1. Trabajo realizado en el marco del proyecto de investigación "Proceso Penal y Unión Europea. Aná-lisis y propuestas. PID2020-116848GB-I00" (Plan nacional I+D+i. Ministerio de Ciencia e Innovación).

2. Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO L 88 de 31.3.2017).

Las medidas que pueden adoptarse para combatirlo, muy variadas y cada vez más sofisticadas[3], gravitan sobre el delicado equilibrio que se ha de mantener entre dos intereses cruciales que ha de salvaguardar todo Estado democrático de Derecho: de un lado, la política de seguridad pública, encaminada a lograr la mejor prevención y represión de las conductas delictivas y, de otro, el debido respeto de los derechos y libertades de los ciudadanos[4]. En estas páginas nos ocuparemos de una de las más recientes que han comenzado a funcionar en la Unión Europea: las órdenes de retirada de contenidos terroristas en línea, introducidas por el Reglamento (UE) 2021/784, de 29 de abril de 2021, que ha entrado en vigor el 7 de junio de 2022[5].

La justificación de la creación de este nuevo mecanismo reside en la necesidad de atajar la propagación del mensaje terrorista, dada la facilidad con que se difunde en las redes. Advierte Velasco Núñez del crecimiento exponencial en los últimos años y en todo tipo de terrorismo de la elección de Internet como medio no sólo de informarse de objetivos, sino de reclutar acólitos y de planear ataques, habiéndose acuñado el término de la "yihad mediática" para el más mortífero que, desde diversos frentes y con carácter transnacional, sirve para la activación de métodos violentos[6]. Y añade Bustos Gisbert que el carácter global y descentralizado de Internet, sin un centro único de control, polifacético en las distintas formas de comunicación que permite, y donde reina la espontaneidad y el anonimato, han facilitado que Internet no sea sólo el reino del pluralismo (que lo es); sino que sea también el reino del radicalismo más brutal, agresivo e irrespetuoso de los más mínimos valores de convivencia. Un caldo

3. *Vid.* SANZ HERMIDA, A. "Garantismo y seguridad en el Estado de Derecho en la lucha (preventiva) contra la delincuencia organizada", en Garrido Carrillo (director), *Retos en la lucha contra la delincuencia organizada* (F. J. Garrido Carrillo, director), Aranzadi 2021, pp. 23-47.
4. ARNÁIZ SERRANO, A., "La articulación del derecho de defensa en la adopción de medidas cautelares de naturaleza personal en los delitos de terrorismo en el ordenamiento jurídico español", *Estudios Penales y Criminológicos*, vol. XXXVI (2016), pp. 493-494.
5. Reglamento (UE) 2021/7884 del Parlamento Europeo y del Consejo, de 29 de abril de 2021 sobre la lucha contra la difusión de contenidos terroristas en línea (DO L 172/79, de 17.5.2021).
6. VELASCO NÚÑEZ, E. *Delincuencia informática* (con Sanchís Crespo, C.), Tirant lo Blanch, Valencia, 2019, p. 27. Sobre Internet como facilitador de los procesos de radicalización y difusión del terrorismo *vid*., asimismo, MIRO LLINARES, F., "La detección del discurso radical en Internet. Aproximación, encuadre y propuesta de mejora de los análisis de Big Data desde un enfoque de Smart Data criminológico", en Alonso Rimo, A., Cuerda Arnau, M.L. y Fernández Hernández, A., *Terrorismo, sistema penal y derechos fundamentales*, Ed. Tirant lo Blanch, Valencia, 2018, pp. 626 a 632, especialmente.

de cultivo perfecto para las organizaciones terroristas[7] que han sabido explotar una vez más con versatilidad las herramientas disponibles en cada época[8].

Los contenidos terroristas compartidos en línea con fines de reclutar a seguidores y prepararlos, para planear y facilitar actividades terroristas, para glorificar sus atrocidades y para animar a otros a seguir ese ejemplo e insuflar el miedo en la opinión pública se difunden a través de prestadores de servicios de alojamiento de datos que permiten subir contenidos de terceros. Esos contenidos se han revelado como esenciales para la radicalización y para incentivar acciones por parte de los llamados «lobos solitarios», como las producidas en varios ataques terroristas recientes en Europa. Dichos contenidos no solo tienen repercusiones negativas importantes para las personas y la sociedad en general, sino que también reducen la confianza de los usuarios en Internet y menoscaban los modelos de negocio y la reputación de las empresas afectadas[9].

El Reglamento constituye el punto de llegada de un camino emprendido en 2015 por la Unión Europea[10] para combatir la difusión de los contenidos terroristas en línea con la creación del Foro de Internet de la Unión Europea[11] y de la Unidad de Notificación de Contenidos de Internet de Europol en el seno del Centro Europeo de Lucha contra el Terrorismo[12]. De un marco de cooperación voluntaria entre Estados miembros

7. BUSTOS GISBERT, R., "Libertad de expresión y control de la Red", en *Terrorismo y Derecho bajo la estela del 11 de septiembre* (Revenga Sánchez, editor), Tirant lo Blanch, Valencia, 2014, p. 166.
8. Así lo indica MONTES NOBLEJAS, D., "A vueltas con el terrorismo e internet: hacia una definición de ciberterrorismo", *Revista de Derecho UNED*, núm. 27, 2021, pp. 719 y 710.
9. Exposición de Motivos de la inicial *Propuesta de Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea*, COM (2018) 640 final, de 12.9.2018.
10. La página del Consejo de la Unión Europea ofrece una visión panorámica de la cronología seguida en esta materia en la UE (https:// https://www.consilium.europa.eu/es/policies/fight-against-terrorism/history-fight-against-terrorism/).
11. Foro que reúne cada año a representantes de los gobiernos de los Estados miembros, Europol y empresas de tecnología para coordinarse y combatir el contenido terrorista y el discurso del odio. Este Foro ha promovido la creación de una base de más de 200.00 hashes que sirve para evitar que los vídeos o fotografías ya etiquetados como contenido terrorista puedan volver a compartirse. *Vid*. Comisión Europea, *EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online,* Press release, Brussels, 3.12.2015, disponible en https:// https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243. Última consulta, 30.09.2022.
12. European Union Referral Unit, (EU IRU) creada en julio de 2015 con el objetivo de detectar los contenidos extremistas terroristas y violentos en línea, frenar las

y prestadores de servicios de alojamiento de datos inaugurado en 2017 con la Comunicación de la Comisión "Hacia una mayor responsabilización de las plataformas en línea"[13], reforzado por la posterior Recomendación (UE) 2018/334 sobre "medidas para combatir eficazmente los contenidos ilícitos en línea"[14] y, por tanto, *soft law* se ha pasado a otro más riguroso (*hard law*) por medio de una norma de máximo nivel (Reglamento) de alcance general, obligatoria en todos sus elementos y directamente aplicable.

Solución legislativa justificada en la necesidad de establecer un marco jurídico claro y armonizado que evite el uso indebido de los servicios de alojamiento de datos para la difusión de contenidos terroristas en línea, con el fin de garantizar el correcto funcionamiento del mercado único digital y, al mismo tiempo, velar por la confianza y la seguridad. El Reglamento es directamente aplicable, ofrece claridad y mayor seguridad jurídica, y evita las interpretaciones divergentes en los Estados miembros y otros problemas de transposición que plantean otras normas europeas, como la Directiva, instrumento que se había empleado con anterioridad pero que en este ámbito (el de la lucha contra los contenidos terroristas en línea) no había dado los resultados esperados[15].

Dado que la norma europea contiene obligaciones impuestas a prestadores de servicios que habitualmente ofrecen sus servicios en más de un Estado miembro, las divergencias en la aplicación de sus disposiciones podrían dificultar la prestación de servicios por parte de los prestadores que ejercen su actividad en múltiples Estados miembros.

De aquí se explica que la base jurídica que lo sostiene sea el art. 114 del Tratado de Funcionamiento de la Unión Europea, que permite la

---

campañas de reclutamiento y enaltecimiento de actos violentos y asesorar a los Estados miembros sobre este tema. Unidad supervisada por el COSI cuyo mandato incluye notificar el contenido terrorista y extremista violento detectado a los proveedores de servicios en línea para que lo eliminen. *Vid*. al respecto, ESTÉVEZ MENDOZA, L., "Análisis de la efectividad e los mecanismos de lucha contra el terrorismo en la sociedad europea", en Garrido Carrillo, F. (dir.) y Faggiani, V. (coord.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: Instrumentos, límites y perspectivas en la era digital,* Thomson Reuters-Aranzadi, Cizur Menor, 2022, pp. 248 y 249.

13. COM (2017) 555 final.
14. DO L 63/50, de 6 de marzo de 2018.
15. Nos referimos a la Directiva (UE) 2017/541, ya citada (nota 2) que por primera vez estableció la obligación de los Estados miembros de adoptar medidas (legislativas, no legislativas o judiciales) para garantizar la rápida detección y eliminación de contenidos radicales, concretamente de aquellos que provoquen a la comisión de un delito de terrorismo, o su bloqueo (art. 21 y Considerando 22). Sobre este punto véase MIRO LLINARES, F., "La detección del discurso radical en Internet…", *op. cit*., pp. 629-631.

adopción de medidas que garanticen el funcionamiento del mercado interior y no ninguna de las disposiciones del Título V relativas al Espacio de Libertad, Seguridad y Justicia, por más que el fin de esta norma también sea el reforzamiento seguridad pública en la UE recurriendo para ello a la armonización de las condiciones de prestación de servicios transfronterizos por parte de los prestadores de servicios de alojamientos de datos.

II. ELEMENTOS BÁSICOS: ÁMBITO DE APLICACIÓN Y AUTORIDADES COMPETENTES

Como es tradicional en la legislación UE se establece en el Reglamento una serie de definiciones relevantes para determinar, entre otros extremos, el ámbito de aplicación subjetivo, objetivo y territorial (o geográfico) de la norma. Y se deja, según veremos, a la elección de los Estados miembros la designación de la autoridad o autoridades competentes para aplicar los instrumentos y soluciones en ella previstos.

Y pese a que no se trata de un instrumento de reconocimiento mutuo (recordemos, de nuevo, su base jurídica) toma de los instrumentos de reconocimiento mutuo propios del Espacio de Libertad, Seguridad y Justicia el empleo de formularios (plantillas) estandarizados y multilingües para facilitar la aplicación del que constituye su mecanismo estrella: la orden de retirada de contenidos terroristas en línea (en su caso, según veremos, con carácter transfronterizo).

1. ÁMBITO DE APLICACIÓN SUBJETIVO O PERSONAL

El ámbito de aplicación personal o subjetivo engloba a los prestadores de servicios de alojamiento de datos (PSAD, en adelante) que ofrecen sus servicios dentro de la Unión, independientemente de su lugar de establecimiento o de su tamaño[16]. A ellos les dirige el Reglamento una serie de obligaciones a las que después nos referiremos.

16. Algo que no ha escapado a la crítica puesto que dirigir de manera indiferenciada las órdenes de retirada a pequeños proveedores puede resultar desproporcionado porque les requerirá disponer de un mecanismo que pueda funcionar todos los días a todas las horas (24/7). *Vid*., en este sentido GASCÓN MARCÉN, A., "La responsabilidad de los intermediarios de Internet en la Unión Europea: iniciativas recientes y perspectivas de futuro", en Castelló Pastor, J.J. (director), *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi, Cizur Menor, 2021, p. 143 y, de la misma autora, "El nuevo Reglamento europeo para la prevención de contenidos terroristas en línea", en Fernández Cabrera, M. y Fernández Díaz, C.R. (directoras),

Quién sea PSAD viene definido por el art. 2.1 del Reglamento con remisión a la Directiva 2000/31/CE sobre el comercio electrónico[17] como cualquier persona física o jurídica que suministre servicios de la sociedad de la información dentro de la UE con independencia de su lugar de establecimiento (dentro o fuera de la UE) o de su tamaño, consistentes en el almacenamiento de información facilitada por el proveedor de contenidos a petición de éste.

El almacenamiento se entiende como "conservación de datos en la memoria de un servidor físico o virtual", según aclara el Considerando 13. De ahí que el Reglamento no resulte aplicable a otros intermediarios como los prestadores de servicios de mera transmisión o almacenamiento temporal (v.gr los proveedores de acceso a Internet), los proveedores de sistemas de nombres de dominio, los servicios de pago o los servicios de protección contra ataques de denegación de servicio distribuido, en la medida en que no implican el almacenamiento de contenidos.

La finalidad específica de luchar contra la difusión entre el público de contenidos terroristas lleva implícita que la información sea puesta a disposición de un número potencialmente ilimitado de personas, lo que conlleva la exclusión de los servicios de comunicaciones interpersonales como el correo electrónico, servicios de mensajería privada o servicios que requieren un registro o admisión previa para acceder a la información (Considerando 14). Caen en cambio dentro de esta categoría[18] los proveedores de medios sociales, los servicios de distribución de video, imágenes y audio, los servicios de intercambio de archivos y otros servicios en la nube, en la medida en que dichos servicios se emplean para poner la información almacenada a disposición del público previa solicitud directa del proveedor de contenidos[19].

Retos del Estado de Derecho en materia de inmigración y terrorismo, Ed. Iustel, Madrid, 2022, p. 532.

17. Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000).

18. *Vid*. sobre este punto STJ de 3 de octubre de 2019 en el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, C-18/18, EU:C:2019:821, donde entre otros extremos se analiza la consideración de *Facebook Ireland Limited* como prestador de servicios de alojamiento de datos en el sentido del artículo 14 de la Directiva 2000/31.*Vid*., asimismo, MORENO BLESA, L., "La retirada de contenidos ilícitos por los prestadores de servicios en línea", *Thémis-Revista de Derecho*, n.º 79, enero-junio 2021, pp. 73-86.

19. Por Proveedor de contenidos el Reglamento entiende cualquier usuario que ha proporcionado información que esté o haya estado almacenada y difundida entre el público por un PSAD (art. 2.2.º)

2. ÁMBITO DE APLICACIÓN OBJETIVO

El ámbito objetivo viene determinado básicamente por los "contenidos terroristas" en línea, que habrán de ser retirados en la forma que después veremos. Se trata de una categoría "porosa"[20] que debe delimitarse adecuadamente en la medida en que es la que se va a emplear para justificar que los contenidos calificados como tales van a ser expulsados del espacio público y, por ende, excluidos del ámbito de protección de las libertades de expresión e información amparadas por el art. 11 de la CDFUE[21].

La definición de "contenidos terroristas ilícitos" (art. 2.7 del Reglamento), que está en consonancia con la definición de delitos de terrorismo establecida en el art. 3.1 de la Directiva (UE) 2017/541, a la que remite el art. 2.6 del Reglamento, es la de material o información utilizada para incitar a la comisión de delitos de terrorismo y hacer apología de dichos delitos, inducir a una persona o grupo a cometerlos o contribuir a su comisión o a participar en las actividades de un grupo terrorista, proporcionar instrucciones sobre fabricación o uso de instrumentos y métodos para cometerlos.

Se trata de una definición que en la versión inicial de la Propuesta fue objeto de severas críticas por su amplitud[22]. Acertadamente, fue corregida y formulada de un modo más adecuado tomando como modelo precisamente el de la Directiva (UE) 2017/541. No obstante, subsiste en el precepto reformado una previsión final que sigue siendo excesivamente ambigua. La que considera también "contenido terrorista" el material que "constituya una amenaza de comisión de los delitos de terrorismo"[23].

---

20. En feliz expresión de TERUEL LOZANO, G. M., "Una lectura garantista de las nuevas tendencias en la lucha europea contrala difusión de mensajes terroristas en internet", *ReDC* núm. 34 Julio-Diciembre 2020, disponible en https://www.ugr.es/~redce/REDCE34/articulos/05_TERUEL.htm.
21. Véase la interesante propuesta de BUSTOS GISBERT para establecer una serie de criterios útiles para valorar, en cada caso concreto si un determinado contenido colgado en la Red incurre en alguno de los comportamientos delictivos descritos (BUSTOS GISBERT, R., "Libertad de expresión …", *op. cit.* apartado 4 –Criterios orientadores para la solución del conflicto entre libertad de expresión y lucha contra el terrorismo en la Red–, pp. 170-172).
22. C.fr., entre otros, las críticas de BARATA, J., *New EU Proposal on the Prevention of Terrorist Content Online: An Important Mutation of the E-Commerce Intermediaries' Regime*, Centre for Internet and Society, 2018, pp. 4 y 5, disponible (última consulta 27.09.2022) en: https://cyberlaw.stanford.edu/sites/default/files/publication/files/2018.10.11.Comment.Terrorism.pdf; TERUEL LOZANO, G. M., "Una lectura garantista…", *op. cit*.
23. Sobre los delitos de ciberterrorismo *vid*. VELASCO NÚÑEZ, E. *Delincuencia informática…*, *op. cit*. pp. 238-251.

Los Considerandos 11 y 12 aclaran y concretan el sentido del precepto examinado al precisar, el primero de ellos, que al evaluar si el material constituye contenido terrorista en el sentido del Reglamento, las autoridades competentes y los prestadores de servicios de alojamiento de datos deben tener en cuenta factores como la naturaleza y la literalidad de las declaraciones, el contexto en el que se realizaron y su potencial de conllevar consecuencias nocivas con respecto a la seguridad y la integridad de las personas. Y, asimismo, y a modo de prevención o salvaguardia para evitar confundir una actuación o publicación en el ejercicio de la libertad de prensa y de información con "difusión de contenidos terroristas" indica el Considerando 12 que el material difundido con fines educativos, periodísticos, artísticos o de investigación, o con fines de sensibilización contra actividades terroristas no debe considerarse contenido terrorista. Como tampoco lo son la expresión de puntos de vista radicales, polémicos o controvertidos en el debate público sobre cuestiones políticas sensibles. Al determinar si el material proporcionado por un proveedor de contenidos constituye «contenidos terroristas» con arreglo al Reglamento y, especialmente en los casos en que el proveedor de contenidos asuma una responsabilidad editorial, cualquier decisión relativa a la retirada de material difundido debe tener en cuenta las normas periodísticas, establecidas por la reglamentación de prensa o de los medios de comunicación, de conformidad con el Derecho de la Unión, incluida la Carta.

3. ÁMBITO DE APLICACIÓN ESPACIAL O GEOGRÁFICO

Las obligaciones impuestas por el Reglamento alcanzan a todos los prestadores de servicios de alojamiento de datos establecidos en la UE y en terceros países, en la medida en que ofrezcan sus servicios en la Unión.

La justificación de esta eficacia "extraterritorial" del Reglamento en cuanto también resulta aplicable a los prestadores de servicios de alojamiento de datos establecidos fuera de la Unión pero que ofrecen servicios dentro de ella es clara, dado que se busca garantizar que todas las empresas con actividad en el mercado único digital cumplan los mismos requisitos, independientemente de su país de establecimiento y habida cuenta de que una proporción significativa de los PSAD expuestos a contenidos terroristas en sus servicios están establecidos en terceros países. Resulta por ello una solución plenamente razonable y coherente con el fundamento y los objetivos del Reglamento[24].

24. En este sentido, DE MIGUEL ASENSIO, P. A., "Servicios de alojamiento de datos y medidas contra la difusión de contenidos terroristas en línea: el Reglamento (UE) 2021/784", *La Ley Unión Europea* n.º 93, 1 de junio de 2021 y, asimismo, "Reglamento

La determinación de si un PSAD ofrece dichos servicios en la Unión requiere evaluar si el prestador permite a las personas físicas o jurídicas que se encuentren en uno o más Estados miembros[25] utilizar sus servicios y si tiene una "conexión sustancial" con dichos Estados miembros. Conexión sustancial que se entiende concurrente cuando el PSAD tiene algún establecimiento –en sentido amplio– en la Unión y que, en otro caso, requiere para poder apreciarla estar fundada en "criterios objetivos específicos" que el Reglamento no establece de modo taxativo. aunque a título de ejemplo indica algunos en el art. 2.5 (tener un número significativo de usuarios de sus servicios en un Estado miembro u orientar sus actividades hacia uno o más Estados miembros[26]).

4. AUTORIDADES COMPETENTES

Cada Estado miembro designará la autoridad o autoridades competentes para ocuparse de los distintos cometidos ligados a la aplicación del Reglamento.

En primer lugar, para dictar órdenes de retirada de conformidad con el art. 3, y designación en su seno de un punto de contacto para tramitar las aclaraciones o peticiones de información derivadas de la emisión de la orden.

En segundo lugar, para examinar las órdenes de retirada dictadas por la autoridad competente de otro Estado miembro (las órdenes transfronterizas del art. 4).

En tercer lugar, para supervisar la aplicación de las medidas específicas (proactivas y/o preventivas) adoptadas por los PSAD de conformidad con el art. 5.

En cuarto y último lugar, para imponer sanciones a los PSAD que incumplan las obligaciones del Reglamento, de conformidad con el art. 18.

(UE) 2021/784 sobre la lucha contra la difusión de contenidos terroristas en línea: segunda parte", disponible en https://pedrodemiguelasensio.blogspot.com (entrada de 21 de mayo de 2021).

25. Imprecisa expresión a juicio de P. A. DE MIGUEL ASENSIO (*op. et locs.cits*) sin que en el articulado se concrete si lo determinante es la nacionalidad, la residencia o simplemente que se encuentren en la UE, si bien el Considerando 15 aclara que lo determinante a estos efectos es que el PSAD permita a las personas que se encuentran en uno o más Estados miembros utilizar sus servicios.

26. Lo cual puede deducirse, por ejemplo, del uso de una determinada lengua o empleo de una moneda propia de un Estado miembro. *Cfr.* Considerandos 5 y 16 del Reglamento (UE) 2021/784.

Si bien el art. 13 no indica el tipo de autoridad que debe ocuparse de tales cometidos, sí exige que actúen con garantía de independencia, objetividad y pleno respeto a los derechos fundamentales[27]. El Considerando 35 aclara que es facultad de cada Estado miembro decidir el número de autoridades que debe designar y si son de carácter administrativo, policial o judicial, sin perjuicio de que además puedan encomendarse tales funciones a un organismo ya existente.

De la consulta al Registro de autoridades hecho público por la Comisión en cumplimiento del art. 12.4 del Reglamento[28] se advierte una mayoritaria inclinación por autoridades policiales. Inclinación también seguida por España que ha designado como autoridad competente para emitir órdenes de retirada, examinar las de carácter transfronterizo y supervisar las medidas específicas al Centro de Inteligencia contra el Terrorismo y la Delincuencia Organizada (CITCO) dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior[29], encomendando la imposición de sanciones por infracciones leves y graves al Secretario de Estado de Seguridad y, por infracciones muy graves, al Ministro del Interior.

Sin perjuicio de que, según se acaba de indicar, el Reglamento deja en este punto total libertad a los Estados miembros, la solución ha sido muy criticada, especialmente en lo que se refiere a que no se reserve a autoridades judiciales la emisión de las órdenes de retirada y su intervención, según veremos, pueda limitarse al recurso que eventualmente se interponga frente a ellas (es decir, a un control *ex post*)[30].

27. *Cfr.* art. 13.2: Los Estados miembros garantizarán que sus autoridades competentes lleven a cabo sus funciones en virtud del presente Reglamento de forma objetiva y no discriminatoria, al tiempo que respetan plenamente los derechos fundamentales. Las autoridades competentes no solicitarán ni aceptarán instrucciones de ningún otro organismo en relación con la ejecución de sus funciones en virtud del artículo 12, apartado 1.

28. Disponible en https://ec.europa.eu/home-affairs/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en#austria.

29. Indicando como punto de contacto el propio Centro de Inteligencia contra el Terrorismo y la Delincuencia Organizada (CITCO), Secretaría de Estado de Seguridad del Ministerio del Interior por medio del correo electrónico iru@interior.es con copia a: citco@interior.es.

30. Véase, por ejemplo, TERUEL LOZANO, G. M. "Una lectura garantista…", *op. cit.*; RODRÍGUEZ RÍOS, S. F. " Una mirada al Reglamento (UE) 2021/784 como nuevo instrumento en la lucha contra la difusión del terrorismo en internet " en Pereira Puigvert, S. y Ordoñez Ponz, F. (directores), *Investigación y proceso penal en el siglo XXI: Nuevas tecnologías y protección de datos*, Thomson Reuters Aranzadi, Cizur Menor, 2021, p. 355. Algún autor, ante el texto de la inicial Propuesta de Reglamento ya daba por supuesto que en España debían ser autoridades judiciales las encargadas de la emisión de las órdenes atribuyendo expresamente este cometido a los Juzgados

III. ACTUACIONES PARA COMBATIR LA DIFUSIÓN. LAS OBLIGACIONES A CARGO DE LOS PROVEEDORES

El Reglamento incorpora una serie de obligaciones a los PSAD, en relación con contenidos terroristas, ya de carácter coercitivo, ya de carácter preventivo y/o proactivo, ya de carácter operativo.

Las de carácter coercitivo consisten básicamente en el cumplimiento de forma inmediata de la orden de retirada o bloqueo de contenidos que se les dirija, con la obligación adicional de su conservación por plazo determinado y el deber de designar un punto de contacto para su recepción y rápido tratamiento (art. 3 y 15)[31]. Téngase en cuenta que, según veremos a continuación, la ejecución de la orden de retirada ha de llevarse a cabo en el plazo de una hora.

El incumplimiento sistemático o persistente puede ser objeto de sanciones económicas de hasta el 4% del volumen de negocios mundial del prestador de servicios de alojamiento de datos en el ejercicio precedente (art. 18). Son los Estados miembros los encargados de establecer el régimen de sanciones (eficaces, proporcionadas y disuasorias)[32] aplicables a las infracciones del Reglamento[33], además de determinar –según hemos visto– la autoridad encargada de imponerlas.

Las de carácter preventivo/proactivo son, a su vez, de dos tipos.

Centrales de Instrucción de la Audiencia Nacional (así GIL GARCÍA, F. S., "Nueva Propuesta de Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea", en *FODERTICS 8.0: Estudios sobre tecnologías disruptivas y justicia* (Bueno de Mata, F. director), Ed. Comares, Granada, 2020, pp. 348 y 349).

31. El punto de contacto del PSAD debe consistir en cualquier medio específico, interno o externalizado, que permita la presentación electrónica de órdenes de retirada así como en los medios técnicos y personales que permitan su rápido tratamiento. El punto de contacto del prestador de servicios de alojamiento de datos no tiene que estar situado en la Unión y el PSAD es libre de utilizar un punto de contacto ya existente, siempre que este sea capaz de cumplir las funciones encomendadas en virtud del presente Reglamento. Con vistas a garantizar que los contenidos terroristas se retiren o que el acceso a ellos se bloquee en el plazo de una hora desde la recepción de una orden de retirada, los prestadores de servicios de alojamiento de datos deben garantizar que el punto de contacto está disponible ininterrumpidamente [Considerando 42 del Reglamento (UE) 2021/784].
32. Aunque el Reglamento (UE) no detalla las sanciones a imponer, sí determina en el art. 18.2 una serie de extremos que los Estados miembros deberán tener en cuenta para graduarlas correctamente, cuestión en la que incide, igualmente su Considerando 45.
33. En España tales sanciones son impuestas por la Secretaría de Estado de Interior para las leves y graves, y por el Ministro del Interior para las muy graves. Sanciones frente a las cuales puede interponerse recurso contencioso-administrativo ante la Sala de lo Contencioso de la Audiencia Nacional (art. 11 de la LJCA) cuya resolución es recurrible en casación ante la Sala Tercera del Tribunal Supremo.

Por una parte, las que podríamos denominar como "generales" consistentes en el deber de informar a las autoridades competentes (o al punto de contacto del Estado miembro de la Unión en que tengan su establecimiento principal o su representante legal) y a Europol cuando detecten contenidos terroristas que conlleven una amenaza inminente para la vida (art. 14.5).

Por otra, las que el Reglamento califica de "específicas" y que implican la adopción por los PSAD "expuestos a contenidos terroristas" de medidas específicas para impedir el alojamiento y difusión de contenidos terroristas.

Ser un PSDA "expuesto" es condición que se adquiere por decisión de la autoridad competente del Estado miembro del establecimiento principal del prestador o en el que su representante legal resida y que, una vez recibida, obliga a implementar medidas en un plazo máximo de tres meses.

La decisión indicada debe basarse en factores objetivos, si bien el art. 5.4 del Reglamento se limita a mencionar a modo de ejemplo el que se trate de un prestador que en los doce meses anteriores haya recibido dos o más órdenes de retirada.

En cuanto a las medidas a adoptar, a elección del PSAD, pueden ser cualquiera de las enumeradas en el art. 5.2 del Reglamento para luchar contra el uso indebido de sus servicios, entre las que se encuentra la adopción de medios técnicos apropiados para identificar y retirar los contenidos o bloquearlos con rapidez, lo que apunta a la posibilidad de emplear filtros automáticos[34], no siempre eficaces y adecuados atendida la dificultad de discernir en atención a su contexto la verdadera intencionalidad de un mensaje[35]. Se trata de seleccionar, en cada caso, aquéllas que sean

34. Filtros automáticos que pueden ser de dos tipos. Los que funcionan con hashes y comparan el contenido subido con una base de datos de contenidos que ya han sido clasificado como terrorista. O los que buscan detectar contenido a través de programas de inteligencia artificial como, por ejemplo, de procesamiento del lenguaje natural. Sobre estos filtros y los problemas que plantean *vid*. GASCÓN MARCÉN, A., "El nuevo Reglamento europeo…", *op. cit*., pp. 537 y 538; MIRO LLINARES, F. "La detección de discurso radical en Internet…", *op. cit*., pp. 632-636 y, del mismo autor, "Predictive policing: utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement", en *IDP: Revista de Internet, Derecho y Política*, n.º 30.

35. Como indica SÁNCHEZ RUBIO, no contamos con Inteligencia Artificial capaz de emular el pensamiento humano, sino que encontramos ciertas limitaciones. La IA sigue siendo como un niño pequeño superdotado al que entrenas para hacer tareas pequeñas pero que no tiene la sabiduría, el juicio o el sentido común de una persona con experiencia ["Los informes de inteligencia en la prevención del discurso del terrorismo", en Galán Muñoz, A. y Gómez Rivero, C. (directores), *La represión y persecución penal del discurso terrorista*, Ed. Tirant lo Blanch, Valencia, 2022, p. 793. *Vid*.,

eficaces, selectivas y proporcionadas atendida la gravedad del nivel de exposición de los servicios de PSAD a los contenidos terroristas, así como sus capacidades técnicas y solidez financiera y teniendo muy en cuenta los derechos fundamentales de los usuarios evitando una obligación general de supervisión[36] que pueda llegar a convertir a los PSAD en una suerte de "censores de la Red con potestades semi-públicas"[37].

El cese en tal condición ("expuesto") se produce por decisión de la autoridad competente adoptada de oficio o a petición del PSAD (art. 5 apartados 4.º a 7.º). Mientras eso sucede el PSAD está sometido a una cierta monitorización para comprobar su adecuación a la conducta debida tras el cumplimiento correcto de las medidas específicas empleadas.

Las obligaciones que podrían calificarse como de tipo operativo, en cuanto dirigidas a posibilitar la aplicación del Reglamento consisten, más allá de las de transparencia que aparecen recogidas en el art. 7[38] y en el ya citado nombramiento de un punto de contacto para recibir y tramitar las órdenes, en establecer un mecanismo eficaz y accesible para permitir que los proveedores de contenidos retirados o bloqueados reclamen y soliciten su restablecimiento (art. 10). Además, y para los PSAD que no tengan su establecimiento principal en la UE, en la obligación adicional de designar un representante legal en la Unión que deberá residir o estar establecido en un Estado miembro, a efectos de la recepción, el cumplimiento y la ejecución de órdenes de retirada y otras decisiones dictadas por las autoridades competentes (art. 17).

IV. ESPECIAL CONSIDERACIÓN DE LAS ÓRDENES DE RETIRADA DE CONTENIDOS TERRORISTAS EN LÍNEA

Sin duda, el instrumento estrella que introduce el Reglamento (UE) 2021/784 para la lucha contra la difusión por internet de contenidos

asimismo, pp. 734-741 sobre las distintas herramientas de IA para detectar contenidos terroristas].

36. El riesgo de censura privada se neutraliza con el mantenimiento de la exención de responsabilidad que prevé la Directiva 2000/31/CE (Comercio electrónico) ya citada (nota 17).
37. En expresión de TERUEL LOZANO, G. M., "Una lectura garantista…", *op. cit.* que expresa su temor al respecto y su preocupación también desde la perspectiva de la garantía de la libertad de expresión y del pluralismo.
38. Obligaciones recogidas en el art. 7 exigiendo que los PSAD detallen claramente en sus términos y condiciones su política destinada a luchar contra los contenidos terroristas en línea y en la publicación de un informe anual de transparencia cuando se trate de un PSAD que haya adoptado medidas en ese ámbito o al que se haya exigido su adopción en virtud del Reglamento.

terroristas lo constituyen las denominadas órdenes de retirada o de bloqueo que dan un significativo paso adelante sobre los "requerimientos" existentes hasta la fecha.

1. NATURALEZA DE LAS ÓRDENES

Se trata de decisiones vinculantes de carácter unilateral por las que la autoridad emisora competente de un Estado miembro obliga a un prestador de servicios en la UE y que en su caso puede estar establecido o representado en otro Estado miembro diferente, a la retirada de contenidos terroristas.

Adviértase, en primer lugar, la relevancia de este nuevo instrumento que ha aparecido en el escenario europeo para combatir la difusión de los contenidos terroristas. Se ha pasado, en este punto, de los "requerimientos" previstos en la ya citada Recomendación (UE) 2018/334 de la Comisión[39] para una retirada en cierto modo "voluntaria" y también en el texto de la inicial Propuesta de Reglamento[40], a las "órdenes de retirada" de obligatorio e inmediato cumplimiento por su destinatario. Se ha hablado, por ello, de un sistema de mera "notificación-acción", donde el proveedor no tiene obligación ni posibilidad alguna de valorar la orden, ni de decidir si la misma es correcta o no; solo ha de cumplirla[41].

Como característica significativa de estas órdenes cabe señalar que, a diferencia de los instrumentos de reconocimiento mutuo, el destinatario de la orden de retirada es directamente el PSAD establecido o representado en la UE bien en el propio Estado de la autoridad emisora de la orden, bien en otro diverso, pero no una autoridad de ese Estado. Es decir, la orden vinculante se dirige al proveedor de servicios (a su representante

39. Véase §§ 32-35 de la Recomendación (UE) 2018/334.

40. *Cfr.* Art. 5 de la Propuesta de Reglamento [COM (2018) 640 final]. Aunque dicho artículo se ha suprimido y no se ha llevado al articulado del Reglamento, el Considerando 40 aclara que el instrumento del requerimiento sigue estando a disposición de los Estados miembros. Con todo, y pese a su en apariencia menor relevancia, no escaparon a la crítica. En este sentido BARATA, J., (*New EU Proposal.., op. cit*.) indicaba que podrían convertirse en un mecanismo para delegar en entidades privadas la responsabilidad de decidir y hacer cumplir medidas que, de otro modo, tendrían que ser adoptadas por organismo públicos con la oportunidad adecuada de revisión judicial.

41. Así GALÁN MUÑOZ, A., "Redes sociales, discurso terrorista y Derecho Penal. Entre la prevención, las libertades fundamentales y ¿los negocios?", en Galán Muñoz, A. y Gómez Rivero, C. (directores), *La represión y persecución penal del discurso terrorista*, Ed. Tirant lo Blanch, Valencia, 2022, p. 293.

legal designado en la UE) quien deberá cumplirla sin necesidad de la intervención o supervisión directa y/o inmediata de ninguna autoridad del Estado de ejecución (más allá de lo que luego se dirá con referencia a las denominadas "órdenes transfronterizas").

Se trata del primer modelo que se implanta en la UE basado en una cooperación directa entre autoridades (policiales, administrativas o judiciales) y proveedores de servicios que encuentra su justificación en razones de eficacia y de celeridad en la respuesta. Adelanta así las soluciones previstas en la Propuesta de Reglamento (UE) sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal[42], por más que se trate de instrumentos totalmente diversos.

A la hora de su dictado se ha de tener presente que, en la medida que estas decisiones pueden suponer una injerencia en las libertades de expresión y de información, las mismas habrán de ser adoptadas en un proceso legalmente establecido en tutela de ciertos derechos o bienes constitucionales –como ocurre en este supuesto– y, en todo caso, deberán superar un estricto test sobre su proporcionalidad y necesidad según ha afirmado tanto el TEDH[43] como el Tribunal de Justicia UE[44].

2. REQUISITOS PARA SU EMISIÓN

Entre los que podemos considerar como de tipo objetivo, se requiere que la orden de retirada se proyecte sobre contenidos terroristas según

42. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, COM (2018) 225 final, de 17.4.2018.

43. Véase STEDH de 18 de diciembre de 2012, *Yildirim contra Tuquía*, en relación a la orden preventiva de bloqueo dictada por las autoridades turcas de una página web considerada ofensiva y, asimismo, STEDH de 1 de diciembre de 2015, caso *Cengiz y otros contra Turquía* y STEDH de 23 de junio de 2020, *Vladimir Kharitonov contra Rusia*. Consúltese con carácter general sobre la jurisprudencia del TEDH sobre esta materia, BUSTOS GISBERT, R., "Los derechos de libre comunicación en una sociedad democrática", en *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos* (García Roca, J. y Santolaya, P. coordinadores), Centro de Estudios Políticos y Constitucionales, 3.ª ed., Madrid, 2014, pp. 473-509.

44. *Vid*. STJ de 13 de marzo de 2019, P*olonia contra Parlamento Europeo y Consejo*, C-128/17, EU:C:2019:194, § 94; STJ de 3 de octubre de 2019, *Glawischnig-Piesczek*, C-18/18, EU:C:2019:821, §§ 33-48; STJ (GS) de 16 de julio de 2020, *Facebook Ireland y Schrems*, C-311/18, EU:C:2020:559, § 176; STJ (GS) de 17 de diciembre de 2020, *Centraal Israëlitisch Consistorie van België y otros*, C-336/19, EU:C:2020:1031, § 64; STJ (GS) de 26 de abril de 2022, *Polonia contra Parlamento Europeo y Consejo*, C-401/19, EU:C:2022:297, §§ 65-67.

se definen en art. 2.7 ya examinado del Reglamento; esto es, material que incite o induzca a cometer un delito de terrorismo [art. 3 de la Directiva (UE) 2017/541] o constituya una amenaza de comisión de tales delitos, o a participar en las actividades de un grupo terrorista o proporcione instrucción sobre la fabricación de explosivos o armas. La inclusión en alguna de las categorías citadas y la exclusión en ellas del material difundido con fines educativos, periodísticos, artísticos o de investigación exige una ponderación de las circunstancias del caso concreto atendidos los derechos a la libertad de información, expresión, libertad de artes y las ciencias. Y requiere, además, que en la orden se motive expresamente la razón por la que ese contenido finalmente es considerado terrorista y, en consecuencia, debe ser retirado [art. 3.4.b)] con la finalidad de permitir al PSAD y, en última instancia, al proveedor de contenidos, ejercer de forma efectiva su derecho a la tutela judicial efectiva en vía de recurso.

En lo referido a los requisitos subjetivos, la orden ha de ser dictada por la autoridad competente (judicial, policial o administrativa) del Estado miembro [art. 12.1.a) y 13] dirigida –art. 3.5– al establecimiento principal del prestador de servicios en la UE (y, concretamente, a su punto de contacto) o bien al representante legal designado en la UE de conformidad con el art. 17.

3. PROCEDIMIENTO

En los casos que podríamos considerar generales u ordinarios, en que la orden de retirada se dirige a un PSAD con establecimiento principal o representante legal en el Estado miembro emisor de la orden, se establece un procedimiento en el que las actuaciones a realizar se reparten entre la autoridad que emite la orden y el PSAD que la recibe.

3.1. Actuaciones a realizar por la autoridad competente que dicta la orden

Salvo supuestos de urgencia, debe facilitar al destinatario la información sobre los procedimientos y plazos aplicables con, al menos, doce horas de antelación a su dictado si es la primera vez que le dirige una orden.

Deberá emitir la orden empleando la plantilla o formulario que aparece en el Anexo I con el contenido del art. 3.4; a saber: identificación de la autoridad que la dicta y que autentifica la orden; motivación suficientemente detallada referida al carácter terrorista de los contenidos a retirar/

bloquear con indicación del supuesto en que se encuadran de entre los enumerados en el art. 2.7; URL que permita la identificación de los contenidos terroristas; datos temporales; información sobre vías de recurso y sus plazos para el PSAD y para el proveedor de contenidos; en su caso, decisión de que no se facilite información por el PSAD al proveedor de contenidos sobre la retirada/bloqueo por concurrir razones de seguridad pública (como la prevención, investigación, detección y enjuiciamiento de delitos de terrorismo)[45].

Obsérvese que una correcta intelección de lo previsto en el art. 2.7 indica que la autoridad competente de emisión debe valorar debidamente si el contenido on line ha de ser calificado como "terrorista" y plasmar en la plantilla su motivación en tal sentido, una vez llevado a cabo el necesario testde proporcionalidad de los derechos en juego.

La plantilla una vez cumplimentada en la lengua oficial del Estado miembro en el que el PSAD tiene su establecimiento principal o en el que reside o está establecido su representante legal (art. 15.2) y firmada electrónicamente por la autoridad competente será transmitida al punto de contacto del PSAD (art. 15.1) por medios electrónicos (art. 3.5.II) y una copia de ella se remitirá a Europol, al objeto de la debida cooperación y coordinación[46] reclamada por el Reglamento que evite duplicidades de trabajo, y para facilitar la futura emisión de su informe anual (art. 14.1 y 14.6).

3.2. Actuaciones a realizar por el PSAD que recibe la orden

Como regla general el PSAD recibida la orden retirará los materiales o bloqueará el acceso a ellos en el plazo de una hora tras la recepción de la orden y lo comunicará a la autoridad emisora mediante la plantilla que aparece en el Anexo II, que incluye la precisión de la hora en que ha tenido lugar.

Se trata de un plazo extraordinariamente breve, justificado en la necesidad de actuar con la máxima celeridad para atajar la difusión de la información, aunque criticado porque se aplica a todos los PSAD

45. El art. 11.3, que prevé esta reserva, fija un `plazo máximo de seis semanas, aunque admite una prórroga por otras seis semanas cuando dicha reserva siga estando justificada

46. *Vid*. al respecto "Europol explica cómo combate la difusión de contenidos terroristas en internet", información publicada en Escudo Digital el 28 de noviembre de 2021 disponible en https://www.escudodigital.com/ciberseguridad/europol-bases-combatir-contenidos-terroristas-internet_50273_102.html.

independientemente de su tamaño, lo cual puede resultar desproporcionado al requerir disponer de un mecanismo que pueda funcionar todos los días y a todas horas (24/7)[47]. Máxime atendidas las importantes sanciones que se anudan a un incumplimiento de las órdenes y que, conforme indica el art. 8, en caso de incumplimiento sistemático y persistente su importe puede llegar al 4% del volumen de negocios anual del PSAD en el ejercicio precedente.

A la vista de lo indicado en el art. 3 y el contenido de la propia plantilla de los Anexos II (Sección B) y III (Sección B) parece dejarse en manos de los PSAD decidir por cuál de las dos opciones (retirada de contenidos o bloqueo del acceso a ellos) se inclinan, apartándose en este punto de la solución apuntada por la Directiva (UE) 2017/541, relativa a la lucha contra el terrorismo, en la que se confería un carácter prioritario a la retirada y subsidiario, al bloqueo[48].

Como indica De Miguel Asensio, se trata de dos opciones con implicaciones diversas en la medida en que la retirada supone, en principio, que los contenidos dejen de estar accesibles a través de los servicios de ese prestador en cualquier lugar del mundo, mientras que el bloqueo se limita a imposibilitar el acceso a los mismos desde el territorio de la UE. Y si bien a la luz de la jurisprudencia del Tribunal de Justicia los mandamientos de retirada de contenidos ilícitos de Internet con alcance mundial resultan típicamente excepcionales, cuando se trata de contenidos terroristas puede estar justificada su imposición[49].

Salvo que medie prohibición de la autoridad emisora en la orden, el PSAD informará al proveedor de contenidos de los motivos de la retirada y del derecho a recurrir la orden, o bien le entregará copia de la orden en la que constan tales extremos (art. 11).

Además, deberá conservar de manera adecuada los contenidos retirados o bloqueados y datos conexos a efectos de los eventuales recursos que puedan interponerse frente a la orden (por el propio prestador o por el proveedor de

47. Así GASCÓN MARCÉN, A., "El nuevo Reglamento…", *op. cit*., p. 532.

48. Atendido su Considerando 22 en el que podía leerse que (la cursiva es nuestra): Los Estados miembros deben esforzarse al máximo por cooperar con terceros países al objeto de *garantizar la eliminación* de contenidos en línea que constituyan una provocación pública a la comisión de un delito de terrorismo desde los servidores ubicados en su territorio. *No obstante, cuando no sea factible la eliminación* de estos contenidos en origen, *también* pueden ponerse en marcha *mecanismos que bloqueen el acceso* a los mismos desde el territorio de la Unión…" Y añadía a continuación en su Considerando 23 que "la eliminación de contenidos en línea que constituyan una provocación pública a la comisión de un delito de terrorismo *o, cuando esto no sea posible*, el bloqueo del acceso…".

49. DE MIGUEL ASENSIO, P. A. "Servicios de alojamiento de datos…", *op. cit*. p. 4.

contenidos)[50], tramitación de denuncias de los proveedores de contenidos al amparo del art. 10 y, lo que es más relevante, prevención, detección, investigación o enjuiciamiento de delitos de terrorismo. Sin perjuicio de que el plazo de conservación debe limitarse al estrictamente necesario en cada caso en atención a los fines perseguidos, se fija el de seis meses como máximo por estimarse que garantiza la proporcionalidad debida al objeto de dejar el tiempo suficiente para iniciar el procedimiento de control administrativo o judicial y permitir a las autoridades policiales o judiciales el acceso a los datos necesarios para la investigación y enjuiciamiento de delitos de terrorismo. No obstante, a petición de la autoridad emisora o del órgano jurisdiccional competente, podrá prorrogarse por el plazo adicional imprescindible para los procedimientos de control administrativos y/o judiciales[51].

De esta solución general que pasa, según hemos visto, por dar cumplimiento inmediato a la orden de retirada se exceptúa únicamente el caso de que medie una imposibilidad de cumplirla por fuerza mayor, por existir razones técnicas u operativas o por contener errores manifiestos. Extremos estos que, en cualquier caso, no permiten una "valoración" del acierto o no de la orden en cuanto al fondo; esto es, si los contenidos son o no terroristas. Simplemente suspender temporalmente su acatamiento en espera de que se corrijan los defectos advertidos. En tales supuestos el PSAD deberá informar de inmediato a la autoridad emisora mediante el empleo de la plantilla recogida en el Anexo III, dando cuenta de los motivos concurrentes que imposibilitan el cumplimiento.

Si se subsanan los defectos o se proporciona la información complementaria necesaria, se ejecutará la orden en el plazo de una hora tras la recepción de las aclaraciones o desaparición de los impedimentos.

3.3. Actuaciones complementarias posteriores

Una vez que la orden sea firme (esto es, cuando expire el plazo para recurrir o, interpuesto recurso, una vez resuelto y confirmada la orden), la autoridad que la emitió deberá informar a la autoridad competente de supervisión (en caso de no ser ella misma) para futuras medidas específicas a cargo del PSAD (art. 3.9.II).

Además, tanto la autoridad emisora como el propio prestador de servicios deberán presentar los informes de transparencia anuales a que resultan obligados en virtud de los arts. 8.2, 7.2-3, respectivamente, del Reglamento.

50. Ante los órganos jurisdiccionales del Estado miembro que la dictó y conforme al procedimiento establecido por su legislación (art. 9).

51. *Cfr.* art. 6 y Considerandos 26 a 28 del Reglamento (UE) 2021/784.

4. ESPECIALIDADES EN LAS ÓRDENES DE RETIRADA TRANSFRONTERIZA

Bajo esta denominación –órdenes transfronterizas– regula el art. 4 del Reglamento una serie de disposiciones aplicables a las órdenes adoptadas por la autoridad competente de un Estado miembro distinto de aquel en el que el prestador destinatario de la medida tenga su establecimiento principal o en el que resida o esté establecido su representante legal.

En estos casos el procedimiento expuesto anteriormente se complica al entrar en juego otra autoridad (la del Estado miembro en el que el PSAD destinatario tiene su establecimiento principal o reside su representante legal) que debe ser informada del dictado de la orden tras lo cual, ya sea de oficio, ya a petición del PSAD o del proveedor de contenidos, examina la adecuación de la orden al Reglamento y puede vetarla.

Se trata de una solución acertada, adoptada para hacer frente a las críticas que había suscitado el texto de la inicial Propuesta de Reglamento con respecto a la posibilidad de que las órdenes pudieran dirigirse directamente a un intermediario situado en otro Estado miembro sin pasar por la autoridad de ese Estado[52]; es decir, sin que su carácter transfronterizo tuviera la más mínima relevancia[53]. El riesgo siempre latente de que este tipo de mecanismos pueda ser utilizado en otras jurisdicciones por gobiernos autoritarios para fomentar la censura, sobre todo si se hace una

52. *Vid*. en este sentido la Carta a los eurodiputados para impedir la aprobación del Reglamento, firmada por sesenta organizaciones de Derechos Humanos y de periodistas (ACCESS NOW, INTERNATIONAL & OTHERS, *Join letter to members of the European Parliament*, 2021, accesible en https://edri.org/wp-content/uploads/2021/04/MEP_TERREG_Letter_EN_78.pdf).

53. El acierto de esta solución se manifiesta asimismo en el hecho que probablemente este modelo también se extienda a las órdenes de entrega de pruebas electrónicas (Reglamento e-evidence) ya que el Parlamento Europeo ha insistido en que se notifique al Estado en que esté localizado el intermediario. *Cfr. Informe sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal*, de 11.12.2020, Doc. A9-0256/2020 PE642.987v02-00 LIB (Comisión de Libertades Civiles, Justicia y Asuntos de Interior. Ponente: Birgit Sippel). Sobre la Propuesta de Reglamento y análisis del Informe del Comité LIBE *vid*. CHRISTAKIS, T. "Lost in notification? Protective logic as compared to efficiency in the European Parliament's e-evidence Draft Report", en *Cross-Border Data Forum* posted 7.01.2020, disponible en https://www.crossborderdataforum.org/lost-in-notification-protective-logic-as-compared-to-efficiency-in-the-european-parliaments-e-evidence-draft-report/ (último acceso 30.09.2022) y DE HOYOS SANCHO, M., "Reflexiones acerca de la propuesta de Reglamento UE sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal", en *Revista General de Derecho Procesal* 58 (2022).

definición muy amplia de lo que son contenidos terroristas[54], aconsejaba crear salvaguardas para los derechos en juego dando entrada a la autoridad del Estado miembro del establecimiento del PSAD para que pudiera objetar la aplicación de la orden.

Veámoslo con algo más de detalle.

4.1. Actuaciones a realizar por la autoridad competente que dicta la orden

Con esta regulación se exige que la autoridad competente que dicta la orden, una vez cumplido con el trámite establecido en el art. 3 (información previa y dictado de la orden mediante el formulario del Anexo I con remisión al PSAD), envíe copia de la orden a la autoridad competente del Estado miembro en el que el PSAD destinatario tiene su establecimiento principal o resida su representante legal.

4.2. Actuaciones a realizar por el PSAD que recibe la orden

El PSAD, una vez recibida la orden debe cumplir con la retirada o bloqueo en el plazo de una hora, comunicándolo a la autoridad emisora mediante la plantilla correspondiente (Anexo II), informando de la retirada al proveedor de contenidos, y adoptando las cautelas necesarias para un eventual restablecimiento de contenidos o reactivación del acceso.

Pero, además, dentro del plazo de cuarenta y ocho horas desde la recepción de la orden puede remitir una solicitud motivada a la autoridad competente del Estado miembro en el que tiene su establecimiento o representante legal para que examine su regularidad.

4.3. Actuaciones de la autoridad competente del Estado miembro en el que el PSAD destinatario tiene su establecimiento principal o su representante legal

A esta autoridad se le confiere llevar a cabo el examen de la conformidad de la orden con las exigencias del Reglamento y de la Carta de Derechos Fundamentales de la UE, algo que puede realizar de oficio en el plazo de setenta y dos horas tras la recepción de la copia o que estará

54. *Vid*. GASCÓN MARCÉN, A., "El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea", *Cuadernos de Derecho Transnacional* (octubre 2021), Vol. 13, N.º 2, pp. 219-220.

obligado a realizar si media instancia del prestador de servicios o del proveedor de contenidos, en el plazo de setenta y dos horas tras recibir dicha solicitud.

De advertir que concurre alguna de dichas irregularidades ha de informar a la autoridad emisora de su intención de dictar una decisión contraria y de los motivos para hacerlo. Tras ello, y dentro de los plazos indicados emitirá una decisión motivada con comunicación a la autoridad que dictó la orden, a Europol y, en su caso, a los solicitantes. Si declara la existencia de una infracción en la orden, esto impedirá que despliegue efectos jurídicos y, por tanto, el PSAD deberá restablecer los contenidos retirados o el acceso a ellos[55].

En consecuencia, y como advierte De Miguel, prima el criterio de la autoridad del Estado miembro en el que el prestador destinatario de la medida tenga su establecimiento principal o en el que resida o esté establecido su representante legal, sin tener en cuenta a qué Estado o Estados miembros van dirigidos los contenidos en cuestión. El art. 4 no contempla que la disparidad de criterios al interpretar el Reglamento se resuelva de modo que el prestador de servicios de alojamiento deba bloquear el acceso a los contenidos únicamente desde el territorio del Estado miembro cuya autoridad competente ha considerado que constituyen contenidos terroristas; ni siquiera, según parece, aunque se trate de contenidos que puedan ser considerados como dirigidos específicamente a ese Estado miembro[56].

4.4. Eventuales actuaciones posteriores

También en el caso de estas órdenes transfronterizas queda abierta la vía de recurso por los PSAD y por los proveedores de contenidos. Ahora bien, teniendo en cuenta que en estas órdenes transfronterizas lo normal es que, ya sea de oficio, ya a instancia del prestador de servicios o del proveedor de contenidos, medie una decisión de la autoridad competente del Estado miembro en el que el PSAD destinatario tiene su establecimiento principal o su representante legal, se prevé que la impugnación de tal decisión "confirmatoria" de la orden de retirada se tramite precisamente

55. El art. 4 precisa en su apartado 7 que ese restablecimiento inmediato se impone "sin perjuicio de la posibilidad por parte del prestador de hacer cumplir sus términos y condiciones de conformidad con el Derecho de la Unión y el Derecho nacional". Se trata de una previsión que facilita que el prestador no restablezca esos materiales en caso de que considere que infringen sus condiciones y su retirada es conforme a Derecho.

56. DE MIGUEL ASENSIO, P. A. "Servicios de alojamiento de datos…", *op. cit*. p. 5.

ante los órganos jurisdiccionales del Estado miembro de la autoridad competente que dictó dicha decisión y no ante los de aquél que emitió la orden (art. 9.1 en relación con art. 4.4).

V. ALGUNAS REFLEXIONES FINALES

Expuesto el contenido fundamental del Reglamento (UE) 2021/784, podemos destacar ante todo su carácter innovador en el ámbito a que afecta (que no es otro que la lucha contra el terrorismo) y los avances innegables que de cara a aportar claridad, uniformidad y seguridad jurídica proporciona una norma de este tipo –Reglamento– frente a la Directiva, siempre prestada a transposiciones algo divergentes en los Estados miembros.

Pese a ello, y en nuestra opinión, la norma adolece de poca concreción y detalle en algunos aspectos (v.gr. coordinación con las autoridades competentes de otros Estados miembros y con Europol[57]) y deja excesivamente abiertos y/o a elección de los Estados miembros otros (v.gr. la naturaleza de las autoridades llamadas a intervenir en la tramitación de las órdenes) probablemente en una calculada visión de que se trataba de extremos que, en otro caso, podrían generar un mayor rechazo a la rápida aprobación del instrumento.

Y es que otra cuestión que merece la pena destacar es la rápida aprobación y puesta en marcha de este Reglamento (a diferencia de otras normas presentadas por las mismas fechas[58]), puesto que han transcurrido menos de cuatro años desde la presentación de la Propuesta por la Comisión,

57. No se olvide que entre las funciones de Europol el art. 4 de su Reglamento, en el apartado 1 incluye la de: "m) respaldar las acciones de los Estados miembros para prevenir y combatir las formas de delincuencia enumeradas en el anexo I que hayan sido facilitadas, fomentadas o cometidas a través de internet, incluyendo las siguientes actuaciones: i) ayudar a las autoridades competentes de los Estados miembros, a petición de estas, a responder a ciberataques de presunto origen delictivo, ii) cooperar con las autoridades competentes de los Estados miembros en relación con las órdenes de retirada, de conformidad con el artículo 14 del Reglamento (UE) 2021/784, y iii) notificar contenidos en línea a los proveedores de servicios en línea de que se trate para que examinen de manera voluntaria la compatibilidad de esos contenidos con sus propias condiciones contractuales". [art. 4.1.m) conforme nueva redacción dada por el Reglamento (UE) 2022/991 del Parlamento Europeo y del Consejo, de 8 de junio de 2022 por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación].

58. Y aun previamente, como, por ejemplo, la Propuesta de Reglamento del Parlamento europeo y del Consejo sobre las órdenes europeas de entrega y conservación de

hasta la entrada en vigor el pasado 7 de junio de 2022 de la norma europea. Aunque toca una materia sensible que afecta a derechos garantizados por la CDFUE, la incidencia en el ámbito de la seguridad colectiva y el interés con que la Propuesta fue acogida y seguida por el Consejo[59] han hecho que fuera aprobada en un tiempo *record*.

Los PSAD, se convierten en los protagonistas esenciales para la detección y eliminación del discurso terrorista en Internet, bien sea porque por iniciativa voluntaria asumen dicha responsabilidad social, bien sea porque el Estado les impone nuevas obligaciones y, por tanto, les restringe su libertad de prestación de servicios de una forma sin precedentes[60]. Y los instrumentos previstos en el Reglamento para luchar contra la difusión de los contenidos terroristas en línea se revelan adecuados y eficaces; en especial, las órdenes de retirada[61], sin duda el instrumento estrella de la norma europea.

Sin perjuicio de las bondades de la nueva regulación, su eficacia no está exenta de problemas puesto que la calificación de un contenido en línea como "terrorista" presenta perfiles complejos que difícilmente pueden acreditarse mediante simples decisiones algorítmicas[62] toda vez que

---

pruebas electrónicas a efectos de enjuiciamiento penal [COM (2018), 225 final], presentada por la Comisión europea el 14 de abril de 2018.

59. *Vid*. Conclusiones del Consejo Europeo de 10 y 11 de diciembre de 2020 (EUCO 22/20, Bruselas, 1.12.2020).

60. En este sentido y ya antes de la aprobación de este Reglamento lo afirmaba MIRO LLINARES, "La detección del discurso radical en Internet…", *op. cit*., pp. 630 y 631.

61. Como indica BUENO DE MATA, la función del Derecho no es solo la de resolver los conflictos, sino que tiene una labor principal anterior en la prevención de los mismos. Se necesitan así instrumentos enfocados a inteligencia, es decir, saber prever lo que puede ocurrir y frenar los ataques antes de que se ejecuten [BUENO DE MATA, F., "Análisis de las medidas de cooperación judicial internacional para la obtención transfronteriza de pruebas en materia de cibercrimen", en *La Transformación digital de la cooperación jurídica penal internacional* (Fontestad Portalés, L., directora), Thomson Reuters Aranzadi, Cizur Menor, 2021, p. 29]. En este sentido y en nuestra opinión las órdenes de retirada de contenidos terroristas en línea son un buen ejemplo de este tipo de instrumentos, de finalidad claramente preventiva, para hacer frente a la amenaza terrorista.

62. Como advierte MIRO LLINARES ("La detección del discurso radical…", *op. cit.*, pp. 644 y 645), resulta esencial continuar con las estrategias de detección y retirada de los contenidos radicales y de propaganda extremista y terrorista en el ciberespacio, pero ello exige el uso de herramientas y técnicas que vayan más allá de la informática y tengan en cuenta el conocimiento criminológico y jurídico para la detección de los auténticos contenidos con capacidad de radicalización. La prevención del discurso radical online por medio de la detección, bloqueo y retirada de contenidos se encuentra en un estado muy embrionario y sólo superará tal fase cuando incorpore los hallazgos y métodos de detección de contenidos comunicativos radicales que puede aportar la criminología y el derecho y seamos capaces

tal concepto en su origen ha sido formulado para ser determinado judicialmente tras un procedimiento contradictorio en el que se pruebe la concurrencia de los elementos objetivos y subjetivos del delito objeto de la acusación[63]. A esto se añade el dato, muy relevante, de que las autoridades que emiten las órdenes de retirada no tienen por qué ser judiciales al dejarse a los Estados miembros libertad para optar por autoridades de este tipo o bien de tipo administrativo o policial, inclinándose mayoritariamente por estas últimas tal y como revela la consulta al Registro *on line* de la Comisión.

Y, a este respecto, suscita dudas si la eficacia, la celeridad y aún la seguridad de esta solución y que la intervención de los órganos jurisdiccionales se limite a un control *ex post* casan bien con el respeto a los derechos afectados (básicamente libertad de expresión y de comunicación). Dudas que, por ejemplo, ya ha despejado el Consejo constitucional francés avalando la solución que permite la norma (y que en Francia ha determinado que se confiera a autoridades administrativas la emisión de las órdenes) en sentencia de 3 de agosto de 2022. En ella ha considerado constitucional la previsión indicada atendidas, de una parte, las prevenciones establecidas en el Reglamento para evitar que el contenido difundido al público con fines educativos, periodísticos, artísticos o de investigación, pueda ser considerado "contenido terrorista"; de otra, la exigencia de que para acordar la retirada la autoridad administrativa competente deba incluir no sólo una referencia al tipo de contenido de que se trate, sino también una motivación suficientemente detallada que explique las razones por las que se considera de carácter terrorista; y, por último, la posibilidad de recurso ante los órganos jurisdiccionales en vía contencioso-administrativa[64].

---

de traducirlos al lenguaje de las ciencias de la computación. Sólo así, generando sinergias para el desarrollo de algoritmos capaces de discriminar si un determinado mensaje es radical o neutral, o identificando los patrones situacionales que definen el entorno donde se ha publicado dicho mensaje, podremos estar seguros de que estamos identificando aquello que realmente queremos evitar, y siempre bajo el respeto a los derechos fundamentales y, aquí en especial, a la libertad de expresión

63. Así lo indica SCHEININ, M.: The EU Regulation on Terrorist Content: An Emperor without Clothes, VerfBlog, entrada del 2019/1/30, disponible en https://verfassungsblog.de/the-eu-regulation-on-terrorist-content-an-emperor-without-clothes/, DOI: 10.17176/20190211-214620-0. Como indica el autor citado, lo que realmente ocurrió (actus reus) importa, pero también importa la intención con la que se cometió el acto (mens rea). Por lo tanto, copiar y pegar incluso exactamente la misma redacción en una normativa que permita a los algoritmos o a los analistas humanos retirar material de Internet no puede basarse en los mismos criterios, ya que sólo pueden aplicarse mediante la presentación de pruebas reales sobre la intención y el contexto.

64. Sentencia 2022-841 DC disponible en Rol N.º 843-2022.

Finalmente, debemos advertir, como problema añadido, el de la fragmentación en la regulación europea sobre la lucha contra los contenidos ilícitos *on line*. No deja de entrañar una cierta complejidad para los operadores jurídicos y aún para las empresas que operan en el sector de las comunicaciones y que deben cooperar en las actuaciones frente a la difusión de contenidos ilícitos la multiplicidad de normas aplicables a una misma materia. Más allá de las normas europeas sobre terrorismo, adoptadas en el marco del ELSJ y, por tanto, con base en el título V del TFUE[65], confluyen varias normas sobre servicios digitales adoptadas con base en el art. 114 TFUE que prevén la retirada de contenidos ilícitos. Y es que al Reglamento (UE) 2021/784 que hemos analizado en estas páginas se ha sumado recientemente el Reglamento (UE) 2022/2065 de servicios digitales[66] (conocido como Ley de servicios digitales o por su acrónimo DSA del inglés Digital Services Act)[67] en cuyo articulado se prevé también una orden de retirada de contenidos ilícitos[68]. Cierto es que dicha norma una vez resulte aplicable (con carácter general, a partir del 17 de noviembre de 2024)[69] actuará como *lex generalis* y el Reglamento (UE) 2021/784 lo hará como *lex specialis*[70]. Pero con independencia de esta solución queda la duda de si no hubiera sido más conveniente que el nuevo Reglamento incorporara en su seno las normas del Reglamento (UE) 2021/784 en aras de ese esfuerzo de consolidación y de clarificación que recomienda la propia UE para aligerar el entramado normativo[71] y que, sin embargo, omite sistemáticamente.

65. En el momento actual contamos con una Propuesta sobre el intercambio de información digital en casos de terrorismo y Propuesta por la que se crea una plataforma de colaboración para los ECIS presentadas por la Comisión el 2 y el 8 de diciembre de 2021, respectivamente (Documentos 9259/22 y 14684/21).
66. Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales), DO L 277, de 27 de octubre de 2022.
67. *Vid*., CUATRECASAS, "Puntos clave de la Propuesta de Digital Services Act: nuevas obligaciones para intermediarios y plataformas en línea", *Legal Flash de propiedad intelectual y Derecho Digital*, 21 de enero de 2021.
68. "Orden de actuación contra contenidos ilícitos", regulada en el art. 9 del Reglamento (UE) 2022/2065 al que se añade, en el art. 10, una "Orden de entrega de información".
69. *Cfr.* art. 93 del Reglamento de Servicios Digitales.
70. *Cfr.* art. 2.4 y Considerandos 10 y 44.II del Reglamento (UE) 2022/2065.
71. *Vid*. PASCUA MATEO, F., "La técnica normativa en el sistema jurídico comunitario", en *Cuadernos de Derecho Público*, n.º 28, 2006, pp. 125-169.

Capítulo 9

Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo[1]

Montserrat de Hoyos Sancho

Catedrática de Derecho Procesal
Ex–Directora del Instituto de Estudios Europeos
Universidad de Valladolid

I. IMPORTANCIA DE LA OBTENCIÓN TRANSFRONTERIZA DE INFORMACIÓN ELECTRÓNICA DE LA QUE DISPONEN LOS PROVEEDORES DE SERVICIOS ON-LINE E INSUFICIENCIA DE LA NORMATIVA ACTUAL EN LA UNIÓN EUROPEA

Pocas dudas podemos albergar acerca de la importancia que la llamada "prueba electrónica" o *e-evidence* tiene y seguirá teniendo en la investigación y enjuiciamiento de hechos delictivos.

La necesidad de recabar información electrónica, y en concreto aquella de la que disponen los que genéricamente conocemos como "proveedores de servicios de internet", es algo con lo que los operadores jurídicos tienen que contar, según los últimos datos publicados[2], en un 85% de las investigaciones penales, incluso aunque el delito no se hubiera cometido

1. Este trabajo es resultado del Proyecto de investigación del Ministerio de Ciencia e Innovación: *"Proceso penal y Unión Europea. Análisis y propuestas"* –PID2020-116848GB-100–, así como del Grupo de Investigación Reconocido "*Garantías procesales y Unión Europea*", de la Universidad de Valladolid.

2. *Vid*. más ampliamente los datos contenidos en el documento de la Comisión europea *Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border*

a través de medios informáticos. Así, para investigar y probar *v.gr.* un simple homicidio con arma blanca, puede ser necesario obtener pruebas digitales del tipo: correos electrónicos entre autor y víctima, consulta de sus perfiles privados de Facebook o Instragram, mensajes de WhatsApp, compras online, coordinadas de GPS de una ruta determinada, rastreo de información buscada en internet, etc. Además, esas mismas fuentes nos indican que en dos tercios de estas investigaciones tales pruebas tuvieron que obtenerse de proveedores de servicios *on line* implantados en territorios de otras jurisdicciones.

Por lo tanto, está claro que es imprescindible disponer de instrumentos normativos que permitan a las autoridades competentes obtener esa información electrónica tan necesaria, de manera selectiva, rápida y fiable, al tiempo que se asegura el pleno respeto de los derechos esenciales, que desde luego incluyen las garantías procesales fundamentales, así como la protección de la información y los datos personales.

En el ámbito jurídico de la Unión Europea ya disponemos desde hace años de una valiosa herramienta para la obtención transfronteriza de pruebas: la orden europea de investigación[3] –OEI en lo sucesivo–. Pero este que ha demostrado ser un instrumento de cooperación muy eficaz, basado en la comunicación directa entre autoridades y en el reconocimiento mutuo de resoluciones judiciales, presenta limitaciones importantes cuando lo que se necesitan son pruebas electrónicas o digitales que están en poder de los proveedores de servicios de internet, en sentido amplio.

En muchos casos tales proveedores estarán radicados en países distintos de aquellos en los que se tramita la investigación o la causa penal, por lo que será preciso acudir a la cooperación transfronteriza[4]. Sin embargo, incluso tratándose de países entre los que está vigente el sistema de la OEI, éste puede ser un instrumento insuficiente, por las siguientes razones: es muy probable que los datos electrónicos que se necesitan estén dispersos

access to electronic evidence for judicial cooperation in criminal matters, COM (2019) 70 final, pp. 1 y ss., publicada en Bruselas el 5.2.2019.

3. Directiva 2014/41/CE del Parlamento europeo y del Consejo, de 3 de abril de 2015, relativa a la orden europea de investigación en materia penal, DOUE 1.5.2014, L. 130/1. Transpuesta al ordenamiento español por Ley 3/2018, de 11 de junio, incorporando el instrumento OEI en el Título X de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, BOE núm. 282, de 21.11.2014.

4. Si el proveedor de servicios que ha de proporcionar los datos electrónicos que se necesitan en una causa penal estuviera establecido en el mismo Estado en que se investigan o enjuician los hechos, no sería necesaria la cooperación transfronteriza para su obtención; se trataría entonces de una prueba "doméstica".

en servidores de distintos Estados, también fuera de la UE, puede que ni siquiera se sepa en qué países están en el momento en que se ha de cursar la petición, o incluso que estén repartidos en servidores de distintos países, o que la información electrónica esté almacenada de manera itinerante. Tengamos presente que los servicios basados en el uso de internet se pueden prestar desde cualquier lugar, pues no requieren infraestructura o personal en el país donde en efecto se ofrece y se presta el servicio.

De otro lado, los datos electrónicos son extremadamente "volátiles", de tal manera que la tramitación de una OEI[5], por rápida que fuera, podría resultar demasiado lenta[6], y perderse esa prueba en el lapso de tiempo que fuera necesario emplear para su solicitud[7].

Por estas razones, expuestas ahora de manera sucinta, el legislador de la Unión ha considerado que para la obtención de este tipo de pruebas o datos electrónicos era necesario designar como destinatario de la solicitud de cooperación directamente al *prestador de servicios on line* que está establecido, representado o que presta sus servicios en la Unión, en un Estado distinto de aquél en que se sigue la investigación o el proceso penal, no siendo por tanto relevante a estos efectos el concreto lugar o lugares donde pudieran estar almacenadas la información electrónica, ni dónde tenga su sede central o delegaciones la compañía que presta el servicio.

El principio de territorialidad en relación con la concreta ubicación o almacenamiento de los datos, que según el sistema OEI determinaría el país/autoridad a la que debe remitirse la Orden con la solicitud de cooperación, deja por tanto de ser operativo cuando hablamos de este tipo de pruebas almacenadas "en la nube"[8].

---

5. En la Directiva OEI se hace mención expresa a la posible obtención de información transfronteriza sobre titulares de un número de teléfono o de una dirección IP concreta, y no se descarta que se pueda emplear para la obtención de otro tipo de datos electrónicos almacenados por los proveedores de servicios que fueran necesarios para la investigación y prueba de hechos delictivos. *Vid.* art. 10.1.e).
6. Así lo destaca BUENO DE MATA, F.: "Análisis de las medidas de cooperación judicial internacional para la obtención transfronteriza de pruebas en materia de cibercrimen", en *La transformación digital de la cooperación jurídica penal internacional.* L. Fontestad (Dir.), Cizur Menor: Aranzadi, 2021, esp. p. 27.
7. En el sistema OEI está previsto que, salvo en casos graves o urgentes, la autoridad de ejecución deberá adoptar la resolución de reconocimiento o ejecución "a más tardar en 30 días después de la recepción de la OEI", y deberá llevar a cabo tal medida de investigación sin demora "a más tardar 90 días después". *Vid*. art. 12 Directiva OEI.
8. Sobre la necesidad de dejar de lado el principio de territorialidad en este materia, entre otros: TOSZA, S.: "All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order", *New Journal of European Criminal Law*, vol. II (2), 2020, pp. 161 y ss., esp. p. 170; TINOCO PASTRANA, A.: "Las órdenes europeas de entrega

II. LA PROPUESTA DE REGLAMENTO DE LA UNIÓN EUROPEA SOBRE ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN DE PRUEBAS ELECTRÓNICAS A EFECTOS DEL ENJUICIAMIENTO PENAL

Tratando de dar respuesta a las necesidades apuntadas en las líneas precedentes, las instituciones UE debaten actualmente sobre este texto presentado el 14 de abril de 2018 por la Comisión europea: *Propuesta de Reglamento del Parlamento europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal*[9], que no sustituirá a la ya vigente OEI, sino que ambas herramientas coexistirán; se empleará una u otra en función de las necesidades de la causa concreta.

Este Reglamento[10] y la Directiva que le acompaña[11] obligarán a todos los proveedores de servicios online que operen en la Unión a designar representantes legales para dar respuesta a las solicitudes de cooperación

---

y conservación: la futura obtención transnacional de la prueba electrónica en los procesos penales en la Unión Europea", *Cuadernos de política criminal*, núm. 135, 2021, pp. 203 y ss.; LARO GONZÁLEZ, E.: "El Reglamento E-evidence: instrumento adicional a la Orden europea de investigación", *La Ley Probática*, núm. 3, 2021, pp. 1 y ss., esp. p. 6.

9. Documento COM (2018), 225 final. Pueden verse sobre esta Propuesta los comentarios y valoraciones de FUENTES SORIANO, O.: "Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes: las órdenes europeas de entrega y conservación de pruebas electrónicas", en *Era digital, sociedad y derecho.* O. Fuentes Soriano (Dir.), Valencia: Tirant lo Blanch, 2020, pp. 281 y ss., el *supra* citado trabajo de TINOCO PASTRANA, así como BUJOSA VADELL, L.: "Cooperación judicial para la obtención y transmisión de pruebas electrónicas", en *A vueltas con la transformación digital de la cooperación jurídico penal internacional*, L. Fontestad (Dir.), Cizur Menor: Aranzadi, 2022, pp. 79 y ss., y BUENO DE MATA, F.: "Análisis de las medidas…", *op. cit.*, pp. 19 y ss. Más recientemente me he ocupado específicamente del tema en DE HOYOS SANCHO, M.: "Reflexiones acerca de la propuesta de Reglamento UE sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos del enjuiciamiento penal", *RGDP,* núm. 58, 2022, pp. 1 y ss.

10. Como apuntan GIALUZ y DELLA TORRE, el uso del instrumento normativo "Reglamento" es una buena prueba de que la Unión se fía realmente poco de cómo los Estados miembros reciben habitualmente los instrumentos eurounitarios en materia procesal penal, por lo que en este caso han optado por eludir el problema, proponiendo un acto *self-executing*. *Vid.* su trabajo "Lotta alla criminalità nel cyberspazio: la Commisione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali", *Diritto Penale Contemporaneo*, núm. 5, 2018, pp. 277 y ss., esp. p. 292.

11. Junto a este documento, el 17 de abril de 2018 se presentó también una propuesta de Directiva del Parlamento europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, COM (2018) 226 final.

y suministrar los datos requeridos, a no ser que concurra alguna de las muy limitadas causas de denegación expresamente previstas en la norma.

Resumiremos a continuación los elementos definidores de este nuevo instrumento de cooperación transfronteriza, tal y como fue diseñado por la Comisión en la citada Propuesta.

Según disponen los arts. 1 y 3, el Reglamento será de aplicación a los supuestos en que una autoridad competente de un Estado miembro UE[12] necesite obtener datos almacenados por un proveedor de servicios de pago que esté establecido, representado, u ofrezca servicios[13] en el territorio de otro Estado miembro, con independencia de la ubicación de los datos, siempre que éstos sean necesarios como elementos de investigación o prueba en procesos penales concretos.

Estas decisiones "vinculantes y obligatorias" que emitan las autoridades competentes, las órdenes de conservación y entrega de pruebas electrónicas, sólo podrán remitirse con este carácter transfronterizo si a nivel nacional, en el propio Estado emisor de las mismas, existe la posibilidad de adoptar una medida similar para la misma infracción y en una situación comparable. Se pretende así evitar el *forum shopping*, es decir, que se soliciten fuera del país medias que no podrían adoptarse en el propio ordenamiento. Además, no podrán tener una finalidad meramente prospectiva o preventiva; los hechos que se investigan habrán de ser delitos concretos, ya cometidos y en relación con autores específicos, y los datos que se piden son datos almacenados por el proveedor en el momento de cursar la petición, no los que pudieran obtenerse en el futuro, tras la recepción de la orden.

La norma proyectada parte de una distinción generalmente admitida entre dos categorías de datos almacenados que podrían solicitar y obtener las autoridades competentes –*Vid.* art. 2–. Por un lado, los datos no relativos al contenido, entre los que se contarían los datos de los abonados[14],

12. En los Considerandos 64.º y 65.º podemos leer que Irlanda ha notificado su deseo de participar en la adopción y aplicación de este Reglamento, mientras que Dinamarca no lo hará.

13. El proveedor de servicios ha de tener una "vinculación significativa" con uno más Estados miembros. Si no tuviera establecimiento como tal, bastará con que tenga un número significativo de usuarios, e incluso podrá deducirse su vínculo con Estados UE considerando otros factores, como la lengua o la moneda empleada en su oferta de productos, publicidad local de sus servicios, o la disponibilidad de una aplicación móvil en esos Estados miembros. *Vid.* más ampliamente, Exposición de motivos de la Propuesta, p. 16.

14. Son datos de los abonados cualquier dato en relación con su identidad: nombre, fecha de nacimiento, dirección postal, datos sobre facturación y pagos, teléfono, dirección de email, tipo de servicio y duración, incluidos otros datos técnicos, como los de interfaces, de validación de uso del servicio, etc. *Vid.* art. 2, apdo. 6.º.

los de acceso[15] y los de transacciones[16]; por otro lado, con un tratamiento diferenciado, estarían los datos de contenido[17]. La entrega o conservación de cada uno de esos tipos de datos conlleva distintos grados de injerencia en los derechos del afectado, por lo que en el texto se establecen condiciones y garantías diferentes para cada supuesto –*Vid.* arts. 4 y ss.–.

En todo caso, una orden de estas características solo podrá emitirse si fuera necesaria y proporcionada en el caso concreto para alcanzar un fin legítimo, como es la obtención de datos relevantes y necesarios para la investigación y prueba de hechos concretos.

Las órdenes de entrega de datos de abonados o de acceso podrán emitirse, para la investigación de todo tipo de delitos, por un juez, por un fiscal o incluso por la policía, con validación posterior en el último caso. Para la petición de entrega de datos de transacciones o de contenidos, ha de tratarse de delitos que conlleven más de tres años de privación de libertad, o que afecten a un gran número de personas o de terrorismo, y solo un juez podrá emitir esas órdenes.

Las órdenes de conservación de información electrónica pueden emitirse por juez o fiscal competente, o incluso por la policía, sea cual fuere el tipo y gravedad de la infracción penal, pues su finalidad es evitar la eliminación o modificación de datos, para preparar posteriormente una orden de entrega o una OEI.

Las referidas órdenes de entrega o conservación se remitirán directamente al representante legal designado por el proveedor de servicios, indica la Propuesta de Reglamento en su art. 7, aunque lo que realmente se remitirá será un "Certificado" –no la orden propiamente dicha, en la que sí constarán todos los datos de la causa, la motivación de la orden, la justificación de la necesidad y proporcionalidad de la medida, etc.–. Esos "Certificados" son documentos multilingües y estandarizados, en

15. Son datos relativos al acceso aquellos que se refieren al inicio y final de una sesión del servicio, fecha y hora de acceso o conexión y desconexión, dirección IP asignada al usuario por el proveedor de servicios de internet, datos de la interfaz utilizada y de identificación del usuario; incluye los metadatos de comunicaciones electrónicas. *Vid.* art. 2, apdo. 7.º.

16. Son datos de transacciones relacionadas con la prestación de un servicio por ese proveedor que facilitan información contextual o adicional sobre ese servicio, como origen y destino de un mensaje, ubicación del dispositivo, fecha, hora, duración, tamaño, ruta, formato y protocolo utilizado, tipo de compresión, siempre que éstos no sean datos relativos al acceso. También se incluyen aquí los metadatos. *Vid.* art. 2, apdo. 8.º.

17. Datos de contenido son aquellos almacenados en formato digital, como textos, voz, videos, imágenes o sonidos, distintos de los datos de los abonados, de acceso o transacciones. *Vid.* art. 2, apdo. 9.º.

los que evita el uso de "texto libre" para reducir el coste de traducción todo lo posible; se denominan respectivamente EPOC y EPOC-PR[18], por sus siglas en inglés, y se transmitirán por cualquier medio que garantice su autenticidad, indica el art. 8.

Los plazos previstos para dar cumplimiento al EPOC recibido, dando respuesta directa a la autoridad emisora, son los siguientes: a más tardar en 10 días desde la recepción, salvo que se solicitara una actuación más rápida; en casos urgentes puede solicitarse que se remitan "sin demora, a más tardare en un plazo de seis horas tras la recepción" –*Vid.* art. 9, apdo. 2.º–. Si el destinatario de la orden, el proveedor de servicios, no pudiera cumplirla, podría pedir información adicional a la autoridad de emisión y, en último término, informar a ésta de que no podrá satisfacer la solicitud recibida.

Para el cumplimiento de un EPOC-PR el art. 10 dispone que el proveedor de servicios deberá conservar sin demora los datos solicitados, y tal preservación expirará tras 60 días si no se ha puesto en marcha antes la petición de entrega[19].

Por lo demás, la persona cuyos datos se han solicitado sólo será informada de la emisión y cumplimiento de estas órdenes posteriormente, una vez transcurrido el tiempo "necesario y proporcionado" para que no se vea afectado el proceso penal en curso. Esa información posterior al usuario del servicio por parte de la autoridad de emisión incluirá la relativa a las vías de recurso disponibles –*Vid.* arts. 11 y 17–.

Una cuestión que a nuestro juicio afectará notablemente a la eficacia práctica que finalmente puedan alcanzar estas órdenes de entrega y conservación es la relativa a las posibles sanciones en caso de incumplimiento, y la subsidiaria intervención en esos casos de la autoridad del Estado de ejecución.

La Propuesta de Reglamento prevé que, sin perjuicio de posibles sanciones penales previstas en las leyes nacionales, los Estados miembros

18. Los modelos de certificados se encuentran en los Anexos I y II de la propuesta de Reglamento.

19. En el sistema de la OEI pueden alcanzar los 30 días para la decisión de reconocimiento, prorrogables por otros 30, y hasta 90 días más para la ejecución, ampliables otros 30, véase el art. 12 de la Directiva OEI. *Vid.* también el análisis contenido en ARANGÜENA FANEGO, C.: "Orden europea de investigación: próxima implementación en España del nuevo instrumento de obtención de prueba penal transfronteriza", *Revista de Derecho Comunitario Europeo,* núm. 58, 2017, pp. 905 y ss., esp. pp. 932 a 934; LARO GONZÁLEZ, E.: *La Orden Europea de Investigación en el espacio europeo de justicia,* Valencia, 2021, pp. 217 a 224; LLORENTE SÁNCHEZ-ARJONA, M.: *La orden europea de investigación y su incorporación al ordenamiento español*, Valencia: Tirant lo Blanch, 2020, pp. 159 a 162.

deberán establecer sanciones pecuniarias en caso de que los proveedores de servicios incumplan con sus obligaciones de entrega o conservación de datos requeridos, que deberán ser "eficaces, proporcionadas y disuasorias"; nada más se indica al respecto en el art. 13.

Además, si el proveedor no cumpliera en plazo la orden recibida, ni aportara razones aceptadas por la autoridad emisora, ésta podrá trasladar su petición a la autoridad competente del Estado de ejecución, para que tome las medidas de coerción necesarias en un máximo de 5 días, a no ser que concurran motivos de rechazo.

Por lo que respecta a los motivos de oposición a la ejecución de las órdenes que puede esgrimir el destinatario de las mismas, es decir, el proveedor de servicios, el art. 14 de la Propuesta enuncia los siguientes, que son de carácter facultativo[20]: la orden no fue emitida o validada por autoridad competente, o no se refiere a alguna de las infracciones admitidas, o es imposible cumplirla por razones materiales o de fuerza mayor, o por errores en el certificado no subsanados, o porque el proveedor afirma no disponer de esos datos, o por no estar cubierta la solicitud por el Reglamento. Se añade también como motivo genérico de oposición a la ejecución de la orden que ésta sea contraria a la Carta de Derechos Fundamentales de la UE o manifiestamente abusiva[21].

Es sin duda destacable que este listado de motivos de rechazo no incluya una referencia al incumplimiento del requisito de doble incriminación, por lo que sería posible tener que ejecutar una orden para investigar o enjuiciar hechos delictivos en el Estado de emisión, que no lo son en el de ejecución. A nuestro juicio, en este punto se debería haber seguido el criterio tradicional de exención de la exigencia de doble incriminación para el listado de los 32 "eurodelitos", por encima del umbral punitivo de los tres años[22].

Por lo que respecta a las vías de impugnación de que disponen las personas investigadas o acusadas cuyos datos se hayan obtenido a través de

20. Llamamos la atención sobre el carácter facultativo de esta oposición por parte del proveedor de servicios, pues el precepto dice "podrá", y no "deberá" o "tendrá que". A nuestro juicio, este precepto tendría que estar redactado en sentido imperativo, de tal forma que, si en efecto concurrieran los motivos de oposición, el proveedor de servicios estaría obligado a responder a la autoridad emisora oponiéndose al cumplimiento de la orden recibida.

21. Recordemos en este punto que la información de que dispone la autoridad de ejecución es muy sucinta, solo la contenida en el Certificado EPOC o EPOC-PR.

22. En la OEI este sí es un motivo de denegación de la ejecución, de carácter facultativo. Más ampliamente sobre esta cuestión, DE HOYOS SANCHO, M.: "La Orden Europea de Investigación: reflexiones sobre su potencial efectividad a la vista de los motivos de denegación del reconocimiento y ejecución en España", *Revista General de Derecho Procesal,* núm. 47, 2019, pp. 1 y ss., esp. pp. 16-18.

órdenes de entrega, el art. 17 de la Propuesta dispone que éstas deberán ser "vías de recurso efectivas", que podrán emplearse "durante el proceso penal para el que se haya emitido esa orden". Por tanto, los recursos se ejercitarán en el Estado emisor de las órdenes, lo que puede complicar el ejercicio del derecho de defensa de los afectados por éstas cuando sean residentes en el Estado de ejecución.

En último término y a modo de resumen, las principales objeciones de fondo planteadas a esta Propuesta de Reglamento, documento que ha suscitado un intenso debate en diversos ámbitos jurídicos[23], son las siguientes:

¿Estamos realmente ante un instrumento de reconocimiento mutuo en sentido estricto? La respuesta ha de ser negativa a nuestro juicio, pues tal principio rector de la cooperación transfronteriza en el ámbito UE, al menos como ha venido siendo entendido hasta hoy, implica un doble control, por la autoridad de emisión y también por la de ejecución, el cual no existe en esta Propuesta de Reglamento, pues se trata de un sistema de cooperación directa con el proveedor de servicios, quien en la gran mayoría de los casos ejecutará sin un control judicial previo las órdenes que reciba. Según se ha expuesto, la autoridad del Estado de ejecución sólo intervendrá de manera excepcional, si el proveedor se niega a cumplir con el Certificado recibido.

De otro lado, este modelo de cooperación directa con los proveedores de servicios implica una "privatización" de la confianza mutua[24] y de la

23. Más allá del ámbito estrictamente académico, *Vid.* entre otros los informes de FAIR TRIALS de los años 2018 y 2019, respectivamente: "Position Paper: The new proposed EU Production and Preservation Orders", "Consultation Paper: E-evidence Position Paper", o del COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE –CCBE–: *Posición del CCBE sobre la Propuesta de Reglamento de la Comisión sobre las Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos del enjuiciamiento penal*, de 19 de octubre de 2018. Muy valioso también el informe coordinado por CARRERA, STEFAN y MITSILEGAS, presentado en octubre 2020 por el CEPS-QMUL *Task Force*, Centre for European Policy y Queen Mary University of London, *Cross-border data access in criminal proceedings and the future of digital justice. Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic*.

24. Críticos con la aplicación de este principio a la obtención transfronteriza de pruebas se muestran WILLEMS, A.: "The Court of Justice of the European Union's Mutual Trust Journey in EU Criminal Law: From a Presumption to (Room for) Rebuttal", *German Law Journal*, 20, 2019, pp. 468 y ss., y AMBOS, K.: "Desarrollos y adaptaciones del principio de reconocimiento mutuo – Reflexiones sobre los orígenes de la orden europea de investigación con vistas a una comprensión práctica del principio de reconocimiento mutuo", en M. Llorente Sánchez-Arjona (Dir.). *Estudios procesales sobre el espacio europeo de justicia penal*, Cizur Menor: Aranzadi, 2021, pp. 141 y ss., esp. pp. 164 a 166.

cooperación transfronteriza[25], lo que desde luego conlleva sus riesgos, pues tales proveedores actuarán, obviamente, sobre todo en pro de su beneficio empresarial[26].

También se está pidiendo a los representantes de los proveedores de servicios que controlen la legalidad, necesidad y proporcionalidad de todas las órdenes que reciban, que podrán llegar a ser numerosísimas, así como el respeto de las garantías y derechos fundamentales de los afectados por ellas, tareas que, además de exceder de sus principales objetivos empresariales, deberán realizar en poco tiempo y disponiendo de muy pocos datos para decidir sobre esas cuestiones. Ya hemos indicado que las representaciones de los proveedores sólo recibirán Certificados, formularios sucintos, no las órdenes de entrega o conservación propiamente dichas redactadas por las autoridades de emisión competentes, en las que sí se explicitarían los motivos y fundamentos de la solicitud cursada.

La suma de todas estas circunstancias, unidas a las posibles sanciones pecuniarias y eventualmente penales a los proveedores que no cumplan con las órdenes de entrega y conservación, puede dar como resultado una ejecución masiva y *cuasi* automática de las órdenes de entrega y retención de información electrónica almacenada por los proveedores de

25. Más ampliamente MITSILEGAS: En el nuevo modelo se establece una relación entre las autoridades encargadas de la aplicación de la ley –*law enforcement*– y los actores privados –las compañías proveedoras de servicios–, los cuales, quieran o no, se convertirán en brazos ejecutores de las autoridades, reemplazando así a sus propias autoridades nacionales en la tarea de recibir, cumplir *y evaluar* las órdenes. Sin embargo, a diferencia de las autoridades nacionales, los proveedores de servicios deberán cumplir con esas funciones que se les enconmiendan *bajo la amenaza de sanciones por incumplimiento*, lo que hará que estos proveedores de servicios no puedan ser considerados fiables defensores de nuestros derechos fundamentales, concluye el autor. *Vid.* su trabajo "The privatisation of mutual trust in Europe's area of criminal Justice: The case of e-evidence", *Maastricht Journal of European and Comparative Law*, 2018, pp. 263 y ss., esp. p. 264. También DANIELE muestra su preocupación por esta tendencia a la "privatización de la tutela de los derechos fundamentales" que afirma se observa también en esta propuesta de Reglamento, pues se confía al proveedor de servicios, esto es, a empresas privadas, el control sobre la ejecución de las órdenes, con argumentos "esencialmente de tipo utilitarista". Destaca el autor que esta exclusión de los órganos estatales del Estado de ejecución no es exclusiva de la propuesta de Reglamento, pues una disposición semejante se encuentra en la CLOUD Act de 2018, su homólogo estadounidense. Se trata por tanto de una fuerte tendencia, a nivel global, que justamente por eso ha de ser valorada con la máxima cautela, concluye el autor en su trabajo"L'acquisizione delle prove digitali dai service provider: un preocupante cambio di paradigma nella cooperazione internazionale", *Riv. Bras. Dir. Proc.*, 2019, pp. 1277 y ss. esp. p. 1289.

26. Muy interesantes las reflexiones a este respecto de TOSZA en su trabajo "Internet service providers as law enforcers and adjudicators. A public role of private actors", *Computer Law & Security Review,* 43 (2021), pp. 1 y ss.

servicios, sin muchas más consideraciones, por lo que *de facto* se estaría prescindiendo del doble control de legalidad y de respeto de los derechos fundamentales, garantías que hasta ahora ha venido operando en la cooperación transfronteriza en la UE. Sería sin duda un cambio de paradigma, un verdadero giro copernicano en la materia; de "salto cuántico" lo ha calificado TOSZA[27].

En todo caso, sí le reconocemos una notable virtud a esta propuesta normativa: pretende superar el criterio de la territorialidad en materia de obtención transfronteriza de pruebas electrónicas. Según se expuso en los párrafos precedentes, no podemos seguir aplicando ese criterio cuando hablamos de la necesidad de obtener información electrónica, pues no está vinculada a un territorio concreto; está "en la nube", en servidores de distintos países, incluso almacenada de forma itinerante o fragmentada. Por lo tanto, en efecto, el referente en la cooperación ha de ser el proveedor de servicios; si éste opera en Estados de la Unión, tenga o no en ellos su sede o establecimiento, vendrá obligado a colaborar en la investigación y enjuiciamiento de hechos delictivos en la Unión, y tendrá que hacerlo designando al menos un representante a esos efectos.

Sin embargo, consideramos que lo antedicho no impide que siga existiendo un doble control por parte de las autoridades judiciales competentes, en el Estado de emisión y también en el Estado de ejecución. Tal control doble habrá de conjugarse de la forma más eficaz posible con el requisito de celeridad que exige la obtención de una prueba de estas características, muy volátil, muy frágil, muy fácil de trasladar.

Esta conjunción o equilibrio necesario entre eficacia, rapidez y garantías[28] se ha intentado alcanzar precisamente por parte de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento

27. Destaca el autor que en este tipo de órdenes para la obtención transfronteriza de *e-evidence* se está exigiendo un nivel de confianza en la autoridad de emisión mucho más alto que el existente hasta ahora, por lo que se produciría un "*quantum leap*", sin la suficiente armonización de garantías procesales, de los recursos disponibles para los afectados y de otros elementos que deberían sustentar esa confianza, como por ejemplo una mayor aproximación de la legislaciones en materia de "*privacy*". Eso por no mencionar el insatisfactorio nivel del "*rule of law*" en ciertos países, que de hecho actualmente afecta a la propia ejecución de los instrumentos de cooperación ya asentados sobre el reconocimiento mutuo, concluye el autor en "All evidence is equal…", *op. cit*., p. 181.

28. Como afirma DE BUSSER, cierto es que el sistema diseñado en este "*E-evidence package*" podría convertirse en una suerte de "*Fast-Track Line*" para pruebas electrónicas si se compara con el de la Directiva sobre Orden Europea de Investigación, pero deberíamos tener claro que no podemos optar por la rapidez a cualquier precio. *Vid.* "EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow", *German Law Journal*, Vol. 19, Issue 5, 2018, pp. 1251 y ss., esp. p. 1266.

europeo, quien en su relevante informe fechado el 11 de diciembre de 2020[29] formuló, entre otras propuestas de mejora, las que sintetizamos a continuación:

Las órdenes de entrega y conservación se deberán remitir *directa y simultáneamente* al proveedor de servicios y a la autoridad judicial que designe la legislación del Estado de ejecución. Así, tras la recepción del EPOC a fin de obtener datos de abonados y/o direcciones IP para identificar a una persona, *Vid.* art. 8 bis[30], el proveedor de servicios garantizará la transmisión de los datos a la autoridad de emisión en un plazo máximo de 10 días, o en 16 horas en caso de urgencia. La información simultánea de esta solicitud a la autoridad de ejecución "no tendrá efecto suspensivo en lo que respecta a las obligaciones del proveedor de servicios", pero si la autoridad de ejecución decidiera invocar, dentro de esos plazos, alguno de los motivos de no reconocimiento o no ejecución de los previstos en el Reglamento, informará inmediatamente a la autoridad de emisión y al proveedor de servicios. En el caso de que la autoridad de emisión ya hubiera recibido los datos, deberá suprimirlos y por tanto no podrá emplearlos; si aún no se hubieran transmitido, el proveedor de servicios se abstendrá de hacerlo. El art. 9 sería el relativo a la ejecución del EPOC cuando se solicitan datos de tráfico y/o de contenido, certificado que también se remitiría simultáneamente al proveedor de servicios y a la autoridad de ejecución. Como en el supuesto anterior, esta última podrá denegar la entrega de esos datos por alguna de las causas previstas en el propio Reglamento.

En el caso de EPOC-PR, que igualmente sería remitido directa y simultáneamente al proveedor de servicios y a la autoridad de ejecución, *Vid.* art. 10, la información a la autoridad de ejecución no tendría efecto suspensivo de las obligaciones del proveedor, de tal manera que, una vez recibido el certificado, éste debería actuar sin demora para conservar los datos solicitados. La conservación podrá mantenerse hasta un máximo de 60 días, más una prórroga de otros 30 si fuera necesaria una nueva evaluación de la pertinencia de los datos. Si el proveedor de servicios considera que el EPOC-PR está incompleto, contiene errores manifiestos, no contiene información suficiente para ejecutarlo, o es claramente abusivo, lo comunicará a la autoridad de emisión y de ejecución, a fin de que ésta solicite aclaraciones a la primera.

29. "Informe sobre la Propuesta de Reglamento del Parlamento europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal", Comisión LIBE, Ponente: Birgit Sippel, COM (2018) 0225 – C8-0155/2018 – 2018/0108(COD).

30. En los párrafos siguientes las referencias serán al articulado de la propuesta de Reglamento tal y como quedaría tras las modificaciones que indica el Parlamento en el Informe *supra* citado.

En conclusión, como se destaca en el propio Considerando 42.º ter 1, añadido por el citado Informe de la Comisión LIBE del Parlamento europeo: "Sin perjuicio del principio de confianza mutua, la autoridad de ejecución deberá tener la posibilidad de denegar el reconocimiento de la ejecución de una orden europea de entrega si dicha denegación se basa en el incumplimiento de las condiciones para la emisión de una orden europea de producción establecidas en el presente Reglamento o en los motivos específicos enumerados en el presente Reglamento".

A nuestro modo de ver, esta que se propone desde el Parlamento europeo puede ser una solución aceptable, pues mejoraría el modelo presentado por la Comisión en abril de 2018. Permitiría facilitar y agilizar la obtención transfronteriza de información electrónica, a la vez que se evitarían los ya apuntados problemas que seguro surgirían con la "privatización" del reconocimiento mutuo, pues se implantaría un control suficiente por parte de las autoridades competentes en ambos Estados, el de emisión y el de ejecución, en línea con los instrumentos hasta ahora empleados en materia de cooperación transfronteriza en la UE con base en el art. 82.1 TFUE y en el principio de reconocimiento mutuo.

Otra de las críticas que ha suscitado la propuesta de Reglamento presentada por la Comisión tiene que ver con que no se haga referencia en ella a la posibilidad de que también la defensa del investigado/acusado pueda solicitar la emisión de una de estas órdenes para la obtención de las pruebas electrónicas que ésta pudiera requerir; lo cual, por cierto, sí está previsto expresamente en la Directiva OEI, en su art. 1.3[31].

Como era de esperar, el primer colectivo profesional que alzó su voz en contra de esta carencia de la propuesta de Reglamento fue el de la Abogacía europea[32]. Concretamente el CCBE –*Council of Bars and Law Societies of Europe*[33]–, en el informe que hicieron público con fecha de 19 de octubre de 2018, y en relación con esta concreta cuestión[34], manifestaron que se

31. "La emisión de una OEI puede ser solicitada por una persona sospechosa o acusada (o por un abogado en su nombre), en el marco de los derechos de la defensa aplicables de conformidad con el procedimiento penal nacional".

32. También se manifestó en este sentido crítico la organización FAIR TRIALS, *Vid.* el citado informe *E-evidence Position Paper,* de 2019.

33. El CCBE –Consejo de la Abogacía Europea– representa a las Abogacías de 45 países y, a través de ellos, a más de 1 millón de abogados. El CCBE ya fue consultado por la Comisión antes de publicar su propuesta de Reglamento de abril de 2018, pero en este documento de octubre 2018 el CCBE amplió sus posiciones, a la vista de la concreta propuesta publicada por la Comisión.

34. *Posición del CCBE sobre la Propuesta de Reglamento de la Comisión sobre las Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos del enjuiciamiento penal, Vid*. esp. pp. 8 a 11. También puso de relieve el CCBE la importancia de preservar la

vulneraban los derechos de la defensa, la igualdad de armas y el juicio justo, ya que los Fiscales podían solicitar la emisión de una orden de entrega o conservación de datos de este tipo, pero no estaba previsto que los investigados/acusados, su defensa técnica, pudieran solicitar pruebas electrónicas a través de este instrumento de cooperación transfronteriza, lo que evidentemente "colocaba al acusado en una desventaja significativa"[35].

Por su parte, también la Comisión LIBE del Parlamento europeo en el Informe citado ha demandado expresamente que se incluya una previsión en aras de la vigencia de los referidos derechos de defensa e igualdad de armas. Así, propone que complete el articulado del Reglamento en este sentido: Art. 1 bis: "La emisión de una orden europea de entrega o de conservación podrá asimismo ser solicitada en nombre de una persona sospechosa o acusada, en el marco de los derechos de la defensa aplicables de conformidad con los procedimientos penales nacionales".

Suscribimos plenamente estas propuestas coincidentes de la Abogacía europea, de la organización no gubernamental *Fair Trials* y de la Comisión LIBE del Parlamento europeo. No obstante, desde la concreta perspectiva del proceso penal español, en el que también las víctimas pueden ejercitar la acción penal[36], sería deseable que se incorporara al texto que finalmente

---

confidencialidad de las comunicaciones abogado-cliente cuando se solicita conocer el contenido de una comunicación electrónica y, en consecuencia, "Si los datos están cubiertos por obligaciones de secreto profesional, la EPO no debe emitirse", pp. 19 y 20. Para facilitar que los proveedores de servicios conozcan en qué casos concurre esta circunstancia, el CCBE propone ayudar a crear un mecanismo que identifique abogados, previa recopilación de los listados de profesionales que suministren los propios Colegios profesionales. Este tipo de herramientas ya se utilizan en el contexto del sistema *e-Codex*, que entre otras utilidades ofrece una infraestructura digital para una comunicación transfronteriza segura en materia de justicia; *Vid*. más ampliamente la información contenida en: https://www.e-codex.eu.

35. Igualmente. muy rotundo en este sentido crítico, el Informe de FAIR TRIALS de 2018, p. 5: "The proposal, as drafted, is entirely one-sided. On the one hand, prosecutors can issue preservation orders at will and production orders for most offences. And on the other, no provisions exist to enable defendants to use or deal with electronic evidence. The proposal undermines the principle of equality of arms between prosecution and defence, placing the defendant at a significant disadvantage. Moreover, the draft legislation does not guide service providers in limiting disclosure of data to information that is relevant for the purposes of the criminal investigation. As drafted, the Orders could result in LEAs being swamped with data –and there is no provision to ensure that defendants don't in turn get snowed under the weight of the e-evidence in their case file– making it difficult, if not impossible, to prepare and exercise effectively their defence. This is particularly worrisome for indigent defendants in the light of the trend across the EU to cut back on legal aid".

36. Sobre esta cuestión, *in extenso*, DE HOYOS SANCHO, M.: *El ejercicio de la acción penal por las víctimas. Un estudio comparado*, Cizur Menor: Aranzadi, 2016.

se apruebe la posibilidad de que las acusaciones personadas en la causa soliciten la emisión de una orden europea de entrega o conservación de la información electrónica que eventualmente pudieran necesitar en defensa de sus propias pretensiones procesales.

Por lo que respecta a los motivos de denegación del reconocimiento o ejecución de una orden de entrega contenida en el correspondiente EPOC, la Comisión LIBE del Parlamento europeo ha propuesto que se añada[37], en el que sería el nuevo art. 10 bis, una referencia expresa y como motivo de denegación *obligatorio* –no facultativo, como en la propuesta de la Comisión– a la obligación de respetar los derechos fundamentales y principios jurídicos de la Carta y del art. 6 del TUE, incluido el derecho de defensa.

También debería ser un motivo de denegación *obligatorio* que la ejecución de la orden de entrega resultara contraria al principio "*ne bis in idem*", tal y como se reconoce en la Carta y desarrolla la jurisprudencia del TJUE. Así lo recoge el Considerando 42 ter del propio Informe del Parlamento europeo.

Igualmente se propone la incorporación de una referencia a la vulneración de la inmunidad o privilegio procesal en el Estado de ejecución como motivo de denegación *obligatorio* por la autoridad de ejecución[38], con especial alusión a las normas sobre limitación de la responsabilidad penal en relación con la libertad de prensa y de expresión conforme a la legislación del Estado de ejecución[39].

Además, entre otros motivos facultativos de denegación de la ejecución, concretamente en relación con un EPOC solicitando la entrega de datos de tráfico y de contenido, la referida Comisión LIBE propuso los siguientes –art. 10 bis, apdo. 2.º–: b) "Cuando la orden europea de entrega se refiera a una infracción penal presuntamente cometida fuera del Estado emisor, y total o parcialmente en el de ejecución, pero la conducta que dio origen a la emisión del EPOC no era constitutiva de infracción penal con arreglo a la legislación del Estado de ejecución. c) Cuando la conducta que dio origen a la emisión del EPOC no fuera constitutiva de infracción con arreglo a la legislación del Estado de ejecución, y no se trate de una de las

37. *Vid*. Considerando 42 *quáter*.

38. Tengamos en cuenta en este punto la importancia de que se preserve el "privilegio" que conlleva el derecho a la necesaria confidencialidad de las comunicaciones entre abogado y cliente. Sobre el particular, ampliamente, BACHMAIER WINTER, L. y MARTÍNEZ SANTOS, A. (Dirs.): *Asistencia letrada, confidencialidad abogado-cliente y proceso penal en la sociedad digital. Estudio de Derecho comparado*. Madrid: Marcial Pons, 2021.

39. Véase el Considerando 42 *quinquies*.

categorías delictivas del Anexo III bis[40], conforme indique la autoridad emisora del EPOC, siempre que en el Estado de emisión fuera punible con pena privativa de libertad o internamiento de una duración máxima no inferior a los 3 años. d) Cuando la ejecución de la orden europea de entrega esté limitada, con arreglo a la legislación del Estado de ejecución, a una lista o categoría de infracciones, o infracciones con un umbral más limitado".

Tras la lectura de lo previsto en los anteriormente transcritos apartados b), c) y d), puede concluirse que se propone una incorporación al texto del Reglamento del principio o exigencia de "doble incriminación", que según indicamos *supra* ha venido siendo reclamado también en materia de cooperación transfronteriza para la obtención de pruebas electrónicas[41], y que no había encontrado reflejo en la propuesta de Reglamento inicialmente presentada por la Comisión europea en abril de 2018.

Estamos totalmente de acuerdo con tal inclusión, pues no sería de recibo que, más allá de los clásicos 32 tipos delictivos que se presumen castigados en todos los Estados de la Unión y cuando la pena de privación de libertad prevista fuera superior a los tres años, se permitiera la entrega de información electrónica a una autoridad extranjera sin ese control de "doble incriminación"; es decir, que se obligara al proveedor de servicios a entregar información en supuestos en los que no se le podría haber solicitado ésta por una autoridad del propio Estado de ejecución, por no ser allí punible esa conducta.

En cuanto a los medios de impugnación que pudieran emplear las personas cuyos datos se han buscado mediante orden europea de entrega o conservación, la referida Comisión LIBE propone, de acuerdo con el sistema de doble control que pretende quede establecido –*Vid.* Considerando 54 de su Informe– que se puedan emplear las "vías de recurso efectivas"

40. Que contiene la clásica referencia a las treinta y dos "categorías de infracciones" exentas del control de doble incriminación, precisamente porque se presupone que todos esos tipos delictivos graves son punibles en todos los Estados de la Unión –criminalidad organizada, terrorismo, trata de seres humanos, homicidio, delitos informáticos, etc.–. Ya en su día el Supervisor Europeo de Protección de Datos, en su Informe de 2020, manifestó que "estaría a favor de definir una lista exhaustiva de infracciones graves que justificaran la emisión de órdenes europeas de entrega para obtener datos de transacciones y datos de contenido, ya que esto aumentaría también la seguridad jurídica de todas las partes interesadas participantes". *Vid. Dictamen sobre las propuestas relativas a las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal*, DOUE 31.1.2020, C 32/11.

41. Véase en particular el citado Informe del CCBE de 2018, p. 7, así como las conclusiones de TINOCO PASTRANA, "Las órdenes europeas de entrega y conservación…", *op. cit*., p. 245.

en relación con la legalidad, necesidad y proporcionalidad de las órdenes, tanto en el Estado emisor como en el de ejecución, de conformidad con las respectivas legislaciones nacionales, *Vid*. art. 17, apdo. 3. No obstante, los motivos de fondo por los que se emitió la orden únicamente podrán ser impugnados en el Estado de emisión, que es donde se tramita la causa penal; "sin perjuicio de las garantías de los derechos fundamentales en el Estado de emisión", se indica como tenor del que sería el apdo. 3 bis de este art. 17.

III. EL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO DE BUDAPEST CONTRA LA CIBERCRIMINALIDAD, EN EL MARCO DEL CONSEJO DE EUROPA

El 2.º Protocolo adicional al Convenio sobre ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas[42] –STCE núm. 224– fue adoptado por el Comité de Ministros del Consejo de Europa el 17 de noviembre de 2021, y ha sido suscrito hasta la fecha en que se redactan estas líneas por un total de 24 Estados[43], entre los que se encuentran, además de países miembros del Consejo de Europa y de la Unión Europea[44], otros que no lo son, pero que tienen incuestionable

42. Pueden leerse algunas valoraciones sobre el instrumento en: VELASCO NÚÑEZ, E.: "El Segundo Protocolo Adicional del Convenio de Budapest contra la cibercriminalidad", y DELGADO MARTÍN, J.: "Presente y futuro de la prueba digital internacional. El Segundo Protocolo Adicional del Convenio de Budapest contra la cibercriminalidad", ambos trabajos publicados en el *Diario La Ley*, de 24 de mayo de 2022. En ese mismo ejemplar del *Diario La Ley* se publicó una entrevista a D.ª Elvira Tejada, Fiscal de Sala Coordinadora contra la criminalidad informática, comentando el instrumento en cuestión. *Vid.* también el artículo de la Fiscal BAHAMONDE BLANCO, quien representó a nuestro M.º de Justicia en las negociaciones del instrumento: "Segundo Protocolo Adicional al Convenio de Budapest: Nuevos medios para la cooperación penal y la obtención de prueba electrónica", *La Ley Penal*, núm. 157, julio-agosto 2022. Más recientemente se ha ocupado de específicamente del tema GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E.: "El nuevo Protocolo del Convenio de Budapest de lucha contra la criminalidad", *Revista General de Derecho Procesal*, núm. 58, 2022, pp. 1 y ss.

43. España lo firmó el 15 de mayo de 2022. La entrada en vigor se producirá cuando se alcancen al menos cinco ratificaciones.

44. Por medio de la Decisión (UE) 2022/722 del Consejo, de 5 de abril de 2022, se autorizó a los Estados miembros de la Unión Europea a firmar, en interés de la Unión, este 2.º Protocolo adicional. Téngase en cuenta además lo dispuesto en el art. 15 apdo.1.b) del mismo instrumento: "Las Partes que también sean miembros de la Unión Europea podrán, en sus relaciones mutuas, aplicar el Derecho de la Unión Europea que regule las cuestiones tratadas en el presente Protocolo", de tal manera que si en el futuro entra en vigor el Reglamento UE sobre conservación y entrega de pruebas electrónicas, con un sistema de cooperación más sencillo y más rápido, con fundamento en el

relevancia en la materia que nos ocupa, como los Estados Unidos o algunos países del ámbito iberoamericano.

La aprobación de este instrumento se justifica, según puede leerse en el Preámbulo, en la proliferación de la cibercriminalidad[45] y en la creciente complejidad de la obtención de pruebas electrónicas, que pueden estar almacenadas en jurisdicciones extranjeras, múltiples, cambiantes o desconocidas, al tiempo que los poderes de los servicios estatales de persecución de los delitos se encuentran limitados en sus funciones por las fronteras territoriales.

Precisamente para salvar estas dificultades en lo posible, el referido 2.º Protocolo adicional establece una base jurídica internacional que vendrá a reforzar la *cooperación entre las autoridades de una Parte y los proveedores de servicios que se encuentren en el territorio de otra Parte,* quienes podrán ser requeridos de manera directa[46] para la entrega de información sobre el registro de nombres de dominio o datos de abonados que tengan almacenados, o bien a través de la autoridad competente del Estado requerido si lo que se solicitan son datos relativos al tráfico. También recoge una modalidad de cooperación inmediata todavía más amplia para supuestos de emergencia, al tiempo que se establecen garantías para los derechos fundamentales, en particular en materia de protección de datos personales.

La posibilidad de obtener directamente de los proveedores de servicios información sobre los datos de abonados ya se encontraba en el art. 18 del propio Convenio de Budapest de 2001[47], pero se excluía expresamente la posibilidad de que estos proveedores ofrecieran datos sobre el tráfico o sobre el contenido[48].

---

reconocimiento mutuo, los Estados UE preferirán que en sus relaciones de cooperación transfronteriza en la materia se aplique tal Reglamento.

45. Si bien se indica expresamente que este Protocolo es de aplicación también para la obtención "de pruebas electrónicas *de cualquier delito*", *Vid.* art. 2, apdo. 1.º.

46. Indica GUDÍN RODRÍGUEZ-MAGARIÑOS que, aunque no se mencione expresamente, el "principio de ubicuidad" es la clave de este Convenio, de tal manera que cualquier Estado en el que se manifieste la cibercriminalidad, debe dotar a sus autoridades de las facultades necesarias para el acceso a los datos que custodian las empresas, dentro o fuera de sus respectivos territorios. *Vid.* su trabajo *supra cit.,* pp. 18 y ss.

47. Ratificado por España el 14 de septiembre de 2010, B.O.E del 17 de septiembre. *Vid.* las valoraciones sobre lo que ha supuesto la vigencia del instrumento en estos años, y en particular la creación de la Red 24/7, en BUJOSA VADELL, L.: "Cooperación judicial para la obtención…", *op. cit.,* pp. 74 y ss.

48. Artículo 18. Orden de presentación:

"1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a) A una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en

Las principales novedades que aporta este 2.º Protocolo Adicional, que sigue basándose en el tradicional principio "*favor cooperationis*"[49] y en la exigencia de la doble incriminación[50], en lo que respecta a la obtención transfronteriza de pruebas electrónicas, son las siguientes[51]:

El art. 6 es el relativo a la "*Solicitud de información sobre el registro de nombres de dominio*", y dispone que cada Estado Parte deberá adoptar las medidas legislativas y de otro tipo que fueran necesarias para que sus autoridades puedan cursar una petición de este tipo a entidades que presten servicios de registro de nombres de dominio en el territorio de otra Parte, a fin de hallar al registrante de un nombre de dominio o para poder ponerse en contacto con él, "a efectos de investigaciones o procesos penales específicos". Cada parte deberá adoptar las medidas necesarias para permitir que tales entidades revelen esa información cuando reciban una solicitud de estas características.

En el art. 7 se aborda la cuestión de la "*Revelación de información relativa a abonados*", precepto que también exige a las Partes que adopten las medidas necesarias para que se pueda emitir un requerimiento directamente a

---

un sistema informático o en un medio de almacenamiento de datos informáticos; y b) a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.

2. Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos 14 y 15.

3. A los efectos del presente artículo, por «datos relativos a los abonados» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, *excluidos los datos sobre el tráfico o sobre el contenido*, y que permita determinar:

a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios".

49. Así, en el art. 5 de este 2.º Protocolo se insta a las Partes a seguir colaborando "en la mayor medida posible".

50. Bien entendido que este requisito se cumple, según puede leerse en el art. 5, apdo. 6.º, con independencia de que la legislación de la Parte requerida incluya el delito en la misma categoría delictiva o lo denomine con la misma terminología que la Parte requirente, "si el acto subsumible en el tipo delictivo respecto del que se solicita la asistencia constituye delito con arreglo a su legislación".

51. Este instrumento también se ocupa de otras cuestiones relevantes en materia de asistencia transfronteriza en investigaciones o causas penales, como son los requisitos de uso de la videoconferencia –art. 11–, de los equipos conjuntos de investigación, de las investigaciones conjuntas –art. 12–, o de la protección de datos de carácter personal –art. 14–.

un proveedor de servicios que se encuentre en el territorio de otra Parte, a fin de que suministre información específica por ellos almacenada o bajo su control relativa a abonados, igualmente "para investigaciones o procesos penales específicos de la Parte emisora". Añade este precepto en el apdo.1.b) que en la firma o ratificación del instrumento las Partes pueden exigir que estos requerimientos a los proveedores de servicios que se encuentren en su territorio sean dictados "por un fiscal u otra autoridad judicial, o estar bajo su supervisión, o ser dictado bajo supervisión independiente".

El art. 8 se dedica a la posibilidad de "Dar efecto a los requerimientos de la otra Parte para la *presentación rápida de información relativa a abonados y datos relativos al tráfico*", específicos y almacenados, que obren en poder o estén bajo el control de dicho proveedor de servicios y sean necesarios para investigaciones o procesos penales específicos de ese Estado. La Parte requerida de colaboración "aplicará una diligencia razonable para dar traslado al proveedor de servicios en un plazo de cuarenta y cinco días, o antes si fuera posible" y ordenará a tal proveedor que se le entregue la información o datos solicitados –*Vid.* art. 8, apdo. 6.º–, en veinte días si es información sobre abonados, y en cuarenta y cinco si son datos relativos al tráfico[52].

También está prevista la "*Revelación rápida de datos informáticos almacenados en caso de emergencia*[53]" –art. 9–, haciendo uso de los respectivos "puntos de contacto de la Red 24/7[54]" a los que se refería ya el art. 35 del Convenio, de tal manera que a través del respectivo punto de contacto nacional se transmita la solicitud de información electrónica al homólogo de la otra Parte, con el fin de que éste requiera a un proveedor de servicios que se encuentra en el territorio de dicha Parte para que revele "de forma

52. Se prevé también la posibilidad de que la Parte requerida se niegue a ejecutar la solicitud si concurren motivos del art. 25, apdo. 4.º, o en el art. 27, apdo. 4.º del Convenio de Budapest: se consideran delitos "políticos", o la ejecución de la solicitud atenta contra la soberanía, seguridad, orden público u otros intereses esenciales de la Parte. Importante es destacar también lo dispuesto en el art. 25.5 del Convenio y en semejantes términos en el art. 5, apdo. 6.º del 2.º Protocolo Adicional: "Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente". Bastará entonces con que los elementos objetivos y subjetivos del tipo respecto del que se solicita la asistencia constituyan delito con arreglo a su legislación.

53. Por situación de emergencia se entiende, según el art. 3.c): riesgo significativo e inminente para la vida o la seguridad de una o más personas físicas.

54. En España tal "Red 24/7" está radicada en la Comisaría General de Policía Judicial del Ministerio del Interior.

rápida *datos informáticos específicos* almacenados que obren en su poder o estén bajo su control, sin necesidad de presentar una solicitud de asistencia mutua". Por lo tanto, como este art. 9 del instrumento no distingue entre tipos de datos informáticos, ha de entenderse que en tales casos de emergencia podrán obtenerse a través de la Red 24/7, datos de abonados, de tráfico, e incluso de contenido, siempre que ya estén almacenados[55].

Es probable que este cauce de la asistencia mutua en situaciones de emergencia, definidas con cierta amplitud en el art. 3.c) del instrumento –riesgo significativo e inminente para la vida o la seguridad de una o más personas físicas–, sea muy utilizado en la práctica de la cooperación internacional. Además del citado art. 9, el art. 10 añade un considerable margen de actuación en tales situaciones de emergencia para demandar asistencia a través de la Red 24/7, por la versatilidad de las diligencias investigadoras que admite sean solicitadas en esos casos, que podrán ser de cualquier tipo, y porque la transmisión de la solicitud se simplifica mucho a través de los propios miembros de la Red[56].

Finalmente, sobre la eficacia esperable de este 2.º Protocolo adicional, debemos recordar que para su entrada en vigor se tiene que ratificar por los Estados Parte, al menos por cinco, cosa que no ha sucedido hasta la fecha y, además, los firmantes tendrán que introducir en sus respectivas legislaciones nacionales los cambios que fueran necesarios para dotar de efectividad al instrumento internacional. Es decir, los Estados Parte deberán facultar de manera expresa a los proveedores de servicios que se encuentren en su territorio para revelar directamente la información requerida por la autoridad competente extranjera.

De otro lado, como han destacado ya algunos analistas[57], el instrumento prevé un amplio catálogo de posibles declaraciones y reservas, a

55. Esta es la interpretación que hace BAHAMONDE BLANCO del art. 9 del 2.º Protocolo adicional, en cuyas negociaciones participó como Fiscal en representación del Ministerio de Justicia español. *Vid.* su trabajo "Segundo Protocolo adicional…", *op. cit*., p. 12. También en ese sentido VELASCO NÚÑEZ, E.: "El Segundo Protocolo adicional…", *op. cit.* p. 4: en caso de emergencia el proveedor tecnológico extranjero requerido deberá ceder rápidamente los datos electrónicos específicos almacenados en su poder; "no indica la norma cuáles, luego no se excluye ninguno". En consecuencia, a través del contacto de la Red 24/7 podrán pedirse "incluso datos de contenido", concluye el referido Magistrado de la Audiencia Nacional.

56. Es posible el contacto directo e inmediato entre ellos y además la documentación necesaria se restringe a la mínima expresión; se puede hacer uso de medios electrónicos de transmisión, e incluso cursar la solicitud verbalmente, con confirmación electrónica ulterior. *Vid.* GUDÍN RODRÍGUEZ-MAGARIÑOS, "El nuevo Protocolo del Convenio…", *op. cit.,* p.32.

57. *Vid.* BAHAMONDE BLANCO, M., *op. supra cit*., pp. 5 y 19, así como GUDÍN RODRÍGUEZ-MAGARIÑOS, *op. supra cit.,* pp. 44 y ss.

fin de que pueda adaptarse a los distintos sistemas jurídicos en que se aplicará, lo que le dotará de la necesaria flexibilidad. Sin embargo y al mismo tiempo, tal característica implica que hasta el momento en que se produzcan las respectivas ratificaciones, hasta que no conozcamos los concretos términos de las mismas, no podremos valorar toda la operatividad de estas nuevas herramientas de cooperación internacional. Las reservas y declaraciones determinarán cuestiones de tanta trascendencia como quiénes serán las concretas autoridades competentes para ejercer algunas de las funciones previstas en el texto, las opciones que ofrece cada uno de los preceptos[58], o la amplitud y alcance de las respectivas garantías.

En cualquier caso, este 2.º Protocolo adicional al Convenio de Budapest conlleva a nuestro juicio un claro avance, pues se amplía y actualiza el referido Convenio, que ha resultado ser muy eficaz en la práctica, al tiempo que se recogen en un instrumento normativo internacional y se garantizan algunas prácticas de cooperación transfronteriza en materia penal que ya se estaban llevando a cabo, en ocasiones basadas en Acuerdos bilaterales[59], como las colaboraciones directas y voluntarias prestadas por algunos proveedores de servicios radicados fuera del territorio del Estado reclamante en relación con peticiones de datos de abonados o incluso de tráfico[60].

58. Como ejemplo podemos mencionar el hecho de que los datos de abonados se podrán solicitar directamente al proveedor de servicios invocando el art. 7, pero también puede resultar que sea obligatorio cursar tal petición a través de las autoridades competentes de la Parte requerida, en los supuestos en que ese Estado Parte hubiera decidido que para obtener tal información será de aplicación el art. 8, y no el art. 7. *Vid.* los comentarios de D.ª Elvira Tejada en la publicación de la entrevista *supra* citada, p. 8.
59. Como en el importante Acuerdo de asistencia judicial entre los Estados Unidos de América y la Unión Europea, firmado el 25 de junio de 2003.
60. Colaboraciones que vienen prestando esos importantes proveedores de servicios de internet, o no, con base en sus propios criterios y respectivas políticas empresariales y de privacidad. *Vid.* la *Guía Práctica sobre preservación y obtención en Estados Unidos de datos de Internet,* p. 69, en su versión de 2019, parcialmente actualizada en 2021 y elaborada por la Magistratura de Enlace de España en Estados Unidos.

Capítulo 10

La digitalización de la cooperación judicial en materia penal en la Unión Europea: propuestas y perspectivas legislativas[1]

Alejandro Hernández López

Profesor Contratado Doctor de Derecho Procesal
Universidad de Valladolid

I. INTRODUCCIÓN

Una cooperación judicial en materia penal eficiente requiere el mantenimiento de una infraestructura de comunicación segura, de confianza y ágil entre las autoridades competentes, capaz de adaptarse a situaciones contingentes. Desde el punto de vista de los justiciables, debe garantizar su derecho a acceder a la Justicia en un tiempo razonable como parte de su derecho al debido proceso. En este sentido, la digitalización se muestra como una oportunidad y cauce óptimo para la consecución de estos objetivos.

La digitalización de la Justicia y, específicamente, de la cooperación judicial en materia penal, es una de las grandes asignaturas pendientes del proceso de consolidación del Espacio de Libertad y Justicia. Los últimos datos de la Comisión sobre digitalización de la cooperación judicial en la Unión Europea[2] muestran las enormes diferencias que, aún hoy,

1. El presente trabajo forma parte del proyecto de investigación nacional "Proceso penal y Unión Europea. Análisis y propuestas" (Ref. PID2020-116848GB-I00) y ha sido elaborado durante el desarrollo de un contrato "Margarita Salas" financiado por la Unión Europea – NextGenerationEU.

2. *Study on the Digitalisation of Cross-Border Judicial Cooperation in the EU –Final Report–*, agosto 2021 (publicado el 1 de abril de 2022), DOI 10.2838/174474, en especial, pp. 28-31.

existen entre los Estados miembros en cuanto al nivel de digitalización de sus sistemas de administración de justicia, y como la mayor parte de los intercambios formales de información siguen produciéndose en formato papel.

La situación excepcional vivida durante la pandemia por la COVID-19 no ha hecho más que evidenciar esta necesidad. La imposibilidad de desarrollar actuaciones presencialmente durante los momentos más álgidos de la crisis, unida a las fuertes restricciones a la movilidad establecidas tanto a nivel nacional como internacional, llevaron a la adopción temporal de soluciones basadas en medios digitales, que hasta el momento se aplicaban de manera excepcional, con el fin de evitar la paralización total de los procedimientos. Las lecciones aprendidas durante este periodo han llevado a los Estados miembros y a la Unión Europea a plantearse la necesidad de normalizar el uso de las TIC, convirtiendo en prioritaria la digitalización de todos los ámbitos de nuestra sociedad, incluida la cooperación judicial y el acceso a la Justicia.

Dentro de esta estrategia, la presente aportación se centra en el análisis crítico de algunas de las últimas propuestas sobre digitalización de la cooperación judicial publicadas por la Comisión como parte de un paquete legislativo más amplio y diseñado para llevar a cabo este cambio de paradigma.

II. ANTECEDENTES

1. EL PROCESO DE DIGITALIZACIÓN DE LA COOPERACIÓN JUDICIAL EN MATERIA PENAL EN LA UNIÓN EUROPEA

El uso de soluciones digitales en el ámbito de la cooperación judicial en materia penal no es una novedad reciente. En la Unión Europea, ya se prevé el uso de la videoconferencia en el Convenio de asistencia judicial en materia penal entre Estados miembros de la Unión Europea del año 2000[3]. En la misma línea, la hoy derogada Decisión marco 2001/220/JAI apostaba por recurrir, en la mayor medida posible, a la audiencia mediante videoconferencia de las víctimas residentes en el extranjero[4].

Desde entonces, la digitalización del Espacio de Libertad, Seguridad y Justicia siempre ha formado parte de los objetivos de la Unión Europea.

3. Art. 10 Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea (DO C 197 de 12 de julio de 2000).
4. Art. 11 Decisión marco 2001/220/JAI, relativa al estatuto de la víctima en el proceso penal (DO L 82 de 22 de marzo de 2001).

Así, el Consejo JAI decidió en junio de 2007 que debía promocionarse el uso de las TIC en el ámbito de la Justicia[5], concretándose en la creación del portal europeo e-Justice[6]. Esta estrategia ha seguido desarrollándose paulatinamente mediante el Plan de acción plurianual 2009-2013 relativo a la justicia en red europea[7], sus sucesivas reediciones[8], así como mediante las acciones y recomendaciones de las instituciones europeas[9].

No cabe duda de que la crisis sanitaria provocada por el virus SARS-CoV-2 ha supuesto un verdadero punto de inflexión en este proceso. Durante este aciago periodo en el que la presencialidad no era posible o estaba fuertemente limitada, los Estados miembros tuvieron que recurrir a soluciones transitorias, a menudo apoyadas en soluciones digitales, que en muchas ocasiones contaban con una nula o pobre cobertura legal y/o técnica que sirviera de apoyo. Esta situación excepcional lógicamente se trasladó al ámbito de la cooperación transfronteriza, ralentizando o directamente paralizando la aplicación de la mayoría de los instrumentos de cooperación, incluidos aquellos que dan efecto al principio de reconocimiento mutuo[10].

En este contexto, en junio de 2020 el Consejo adoptó sus Conclusiones sobre "la configuración del futuro digital en Europa"[11], que incluían como objetivo prioritario la digitalización de los sistemas judiciales de los Estados miembros para mejorar el acceso a la Justicia. Dentro de este objetivo amplio, el Consejo solicitó a la Comisión la proposición de medidas tendentes a facilitar los intercambios digitales transfronterizos entre los Estados miembros, tanto en materia civil[12] como penal, garantizando la sostenibilidad y el desarrollo continuo de las soluciones técnicas utilizadas

5. BUENO DE MATA, F., "Justicia online y ciudadanía: el portal europeo E-Justicia como medio de información y apoyo a los ciudadanos para solventar sus litigios transfronterizos", *Revista Europea de Derechos Fundamentales*, núm. 18, 2011, pp. 194-195.
6. GASCÓN INCHAUSTI, F., "La e-Justicia en la Unión Europea: balance de situación y planes para el futuro (en diciembre de 2009)", en SENÉS MOTILLA, C. (Coord.), *Presente y futuro de la E-Justicia en España*, Aranzadi, Cizur Menor, 2010, pp. 83-125.
7. DO C 75 de 31 de marzo de 2009.
8. Plan de acción plurianual 2014-2018 relativo a la Justicia en red europea (DO C 182 de 14 de junio de 2014); Plan de acción plurianual 2019-2023 (DO C 96 de 13 de marzo de 2019).
9. *V.g.* Recomendaciones del Consejo "Fomentar la utilización de las videoconferencias transfronterizas en el ámbito de la justicia en los Estados miembros y a escala de la UE y compartir las mejores prácticas" (DO C 250 de 31 de julio de 2015).
10. *Vid. The impact of COVID-19 on Judicial Cooperation in Criminal Matters. Analysis of Eurojust Casework.*, mayo 2021, DOI:10.2812/083631.
11. DO C 202 de 16 de junio de 2020.
12. Sobre los antecedentes del proceso de digitalización de la cooperación judicial en materia civil y mercantil, *vid.* ELVIRA BENAYAS, M. J., "Digitalización de la

para dichos intercambios. Ese mismo mes se completó el informe final encargado por la Comisión *Cross-border Digital Criminal Justice* –publicado en septiembre de 2020–[13], documento que analiza en profundidad los problemas y disfuncionalidades digitales detectadas a lo largo de los años por las autoridades judiciales, órganos, organismos y agencias de la Unión con un rol activo en la cooperación judicial, incluyendo algunas propuestas *de lege ferenda* en función de los diferentes escenarios posibles.

En octubre de 2020, el Consejo instó de nuevo a la Comisión a presentar medidas concretas para emprender la digitalización de la justicia y, concretamente, en el ámbito penal, solicitó evaluar la ampliación del Sistema Digital de Intercambio de Pruebas Electrónicas (eEDES), que ya se venía utilizando en el marco de la Orden Europea de Investigación (OEI), a otros instrumentos de cooperación judicial en materia penal[14]. La Comisión recogió el guante e incorporó en su programa de trabajo para 2021[15] la creación de una batería de nuevas medidas específicas dentro del denominado "paquete de cooperación judicial digital". Entre estas medidas, se contempló expresamente la creación de un mecanismo para el intercambio digital de información en casos transfronterizos de terrorismo; la creación de una plataforma de colaboración para los Equipos Conjuntos de Investigación; y la digitalización de la cooperación judicial transfronteriza. El lanzamiento de todas estas iniciativas se programó para el cuarto trimestre de 2021.

En diciembre de 2020, la Comisión publicó una nueva comunicación sobre la digitalización de la Justicia en la Unión Europea[16], incluyendo una serie de medidas destinadas a impulsar esta digitalización tanto a nivel nacional como a nivel europeo. En concreto, se estimaba la necesidad de aumentar la resiliencia de los sistemas judiciales europeos a situaciones contingentes como la vivida durante la pandemia y preveía como uno de los ejes principales de actuación la modernización de todos los procedimientos legislativos de cooperación judicial hacia la aplicación del principio "digital por defecto", es decir, la aplicación preferente de canales digitales de comunicación como medio para mejorar la eficiencia y la flexibilidad de la comunicación, así como para reducir los costes y la carga administrativa.

---

cooperación judicial internacional en materia civil o mercantil en la Unión Europea", *La Ley Unión Europea*, núm. 101, 2022, pp. 220-225.

13. *Cross-border Digital Criminal Justice. Final Report*, junio 2020, DOI: 10.2838/118529.
14. *Vid*. Conclusiones del Consejo "Acceso a la justicia: aprovechar las oportunidades de la digitalización" (DO C 342 de 14 de octubre de 2020), en especial Conclusión 27.
15. Documento COM(2020) 690 final, de 19 de octubre de 2020, *Commission Work Programme 2021: a Union of vitality in a world of fragility*, Anexo I, p. 5.
16. Documento COM(2020) 710 final, de 2 de diciembre de 2020.

2. EL PAQUETE LEGISLATIVO PROPUESTO POR LA COMISIÓN

Tal y como estaba inicialmente previsto, la Comisión publicó el 1 de diciembre de 2021 un conjunto de propuestas destinadas a hacer realidad algunos de los objetivos formulados sobre la digitalización de la cooperación judicial[17]. En la esfera penal, estas iniciativas son las siguientes: la Propuesta de Reglamento por el que se crea una plataforma de colaboración en apoyo del funcionamiento de los Equipos Conjuntos de Investigación[18]; La Propuesta de Reglamento sobre intercambio de información digital en casos de terrorismo[19]; Las propuestas de Reglamento y la Directiva sobre digitalización de la cooperación judicial en materia civil, mercantil y penal[20].

Dentro del paquete legislativo presentado por la Comisión, debido a su amplio ámbito de aplicación material, la Propuesta de Reglamento sobre digitalización de la cooperación judicial y acceso a la justicia en asuntos transfronterizos civiles, mercantiles y penales (en adelante, Propuesta de Reglamento DIG) es, junto con la Propuesta de Directiva que la acompaña, la iniciativa que posee un mayor potencial transformador. Por este motivo y por razones de extensión, dedicaremos las siguientes líneas a analizar exhaustivamente los cambios que propone el texto actual de esta iniciativa y su virtual impacto en Europa y en España.

III. LA PROPUESTA DE REGLAMENTO SOBRE DIGITALIZACIÓN DE LA COOPERACIÓN JUDICIAL COM(2021) 759 FINAL

1. OBJETIVO Y ÁMBITO DE APLICACIÓN

El objetivo principal de esta iniciativa es establecer el uso por defecto de canales digitales seguros en la aplicación de todos los mecanismos de cooperación judicial transfronteriza adoptados hasta la fecha, con el objetivo de mejorar la eficiencia, celeridad y contribuir al ahorro de costes materiales y temporales.

En este sentido, la Propuesta de Reglamento DIG busca introducir un nuevo marco jurídico para la comunicación electrónica entre autoridades competentes y entre personas físicas y jurídicas y autoridades competentes

17. REYNDERS, D., "Digitalising Justice Systems to Bring Out the Best in Justice", *Eucrim*, issue 4, 2021, pp. 236-237.
18. Documento COM(2021) 756 final, de 1 de diciembre de 2021.
19. Documento COM(2021) 757 final, de 1 de diciembre de 2021
20. Documentos COM(2021) 759 final y COM(2021) 760 final, de 1 de diciembre de 2021.

en el ámbito de la cooperación judicial en materia civil, mercantil y penal. Específicamente, la iniciativa de la Comisión busca establecer reglas mínimas comunes en torno a las siguientes cuestiones[21]:

1) La comunicación electrónica entre autoridades competentes y entre personas físicas o jurídicas y autoridades competentes.
2) El uso de la videoconferencia o medios análogos de comunicación a distancia con fines diferentes a la obtención de pruebas en asuntos civiles y mercantiles[22].
3) La aplicación de servicios de confianza electrónicos.
4) Regulación de los efectos jurídicos de los documentos electrónicos.
5) El pago electrónico de tasas.

Como puede observarse, el ámbito de aplicación material de la Propuesta de Reglamento DIG incluye aspectos relacionados con la cooperación judicial transfronteriza en materia civil, mercantil y penal. En lo que atañe específicamente a la cooperación judicial en materia penal, objeto al que se circunscribe el presente trabajo, el ámbito material que propone esta iniciativa afectaría exclusivamente a los siguientes ámbitos:

1) Comunicación electrónica entre autoridades competentes en el contexto de los actos de derecho de la Unión específicamente señalados en el Anexo II de la Propuesta de Reglamento DIG. Estos actos incluyen todos los instrumentos que dan efecto al principio de reconocimiento mutuo adoptados hasta la fecha. Son los siguientes[23]:
    i. Decisión marco 2002/465/JAI sobre equipos conjuntos de investigación (Decisión marco ECI)[24];
    ii. Decisión marco 2002/584/JAI relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (Decisión marco ODE)[25];
    iii. Decisión marco 2003/577/JAI relativa a la ejecución en la Unión Europea de las resoluciones de embargo preventivo de bienes y de aseguramiento de pruebas[26];

21. KRAMER, X., "Digitising access to justice: the next steps in the digitalisation of judicial cooperation in Europe", *Revista General de Derecho Europeo*, núm. 56, 2022, p. 5.
22. Este último aspecto ya regulado por el Reglamento (UE) 2020/1783 (DO L 405 de 2 de diciembre de 2020).
23. *Vid.* Anexo II Documento COM(2021) 759 final.
24. DO L 162 de 20 de junio de 2002.
25. DO L 190 de 18 de julio de 2002.
26. DO L 196 de 2 de agosto 2003.

iv. Decisión marco 2005/214/JAI relativa a la aplicación del principio de reconocimiento mutuo de sanciones pecuniarias[27];

v. Decisión marco 2006/783/JAI del Consejo, de 6 de octubre de 2006, relativa a la aplicación del principio de reconocimiento mutuo de resoluciones de decomiso[28];

vi. Decisión marco del Consejo 2008/909/JAI relativa a la aplicación del principio de reconocimiento mutuo de sentencias en materia penal por las que se imponen penas u otras medidas privativas de libertad a efectos de su ejecución en la Unión Europea[29];

vii. Decisión marco 2008/947/JAI relativa a la aplicación del principio de reconocimiento mutuo de sentencias y resoluciones de libertad vigilada con miras a la vigilancia de las medidas de libertad vigilada y las penas sustitutivas[30];

viii. Decisión marco 2009/829/JAI relativa a la aplicación, entre Estados miembros de la Unión Europea, del principio de reconocimiento mutuo a las resoluciones sobre medidas de vigilancia como sustitución de la prisión provisional[31];

ix. Decisión marco 2009/948/JAI sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales[32];

x. Directiva 2014/41/UE relativa a la orden europea de investigación en materia penal (Directiva OEI)[33].

xi. Reglamento (UE) 2018/1805 del Parlamento Europeo y del Consejo, sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso[34].

2) Uso de videoconferencia y otros medios de comunicación a distancia análogos en el desarrollo de procesos penales y, en especial, para la audiencia de investigados, acusados y condenados.

27. DO L 76 de 22 de marzo de 2005.
28. DO L 328 de 24 de noviembre de 2006.
29. DO L 327 de 5 de diciembre de 2008.
30. DO L 337 de 16 de noviembre de 2008.
31. DO L 294 de 11 de noviembre de 2009.
32. DO L 328 de 15 de diciembre de 2009.
33. DO L 130 de 1 de mayo de 2014.
34. DO L 303 de 28 de noviembre de 2018.

3) Utilización de servicios de confianza y regulación de la eficacia jurídica de los documentos electrónicos.

4) Protección de la información transmitida a través de estos medios.

En cuanto a su ámbito de aplicación espacial, en caso de ser adoptada, la Propuesta de Reglamento DIG se aplicaría a todos los Estados miembros salvo Irlanda y Dinamarca en aplicación de las cláusulas *opt in* y *opt out* de sus respectivos protocolos[35]. No obstante, Irlanda puede notificar su intención de participar en el instrumento en cualquier momento.

2. COMUNICACIÓN DIGITAL POR DEFECTO ENTRE AUTORIDADES COMPETENTES

El Capítulo II de la Propuesta de Reglamento DIG regula la comunicación a través de medios digitales entre las autoridades competentes de los Estados miembros. A efectos de esta iniciativa, debe entenderse por autoridad competente no solo a las autoridades judiciales *lato sensu* de los Estados miembros –jueces y fiscales–, sino también a los órganos y organismos de la Unión (v.g. Fiscalía Europea, Eurojust) y a otras autoridades que participen en procedimientos de cooperación judicial de acuerdo con lo dispuesto en los actos jurídicos de derecho de la Unión incluidos en su ámbito de aplicación (v.g. autoridades nacionales competentes establecidas en el art. 2 (c) (ii) de la Directiva OEI)[36].

Para este fin, el texto utiliza una fórmula genérica destinada a convertir la comunicación por medios electrónicos en la opción por defecto para el intercambio de información entre autoridades competentes. Así pues, todas las referencias a las comunicaciones que deben o pueden establecerse entre las autoridades competentes en cada uno de los actos jurídicos que abarca el listado de instrumentos de cooperación comprendidos en el Anexo II, incluido el intercambio de formularios, se llevará a cabo a través de medios digitales utilizando un sistema informático descentralizado, seguro y fiable[37]. Por lo tanto, no solo la comunicación digital será el medio que deberán utilizar las autoridades por defecto, sino que además esta comunicación deberá llevarse a cabo a través de un sistema

35. *Vid*. arts. 1, 2 y 4 bis (1) Protocolo núm. 21 al Tratado de Funcionamiento de la Unión Europea, sobre la posición de Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia (DO C 326, de 26 de octubre de 2012; arts. 1 y 2 Protocolo núm. 22 al Tratado de Funcionamiento de la Unión Europea, sobre la posición de Dinamarca (DO C 326 de 26 de octubre de 2012).

36. En consonancia con lo dispuesto en el art. 2 (1) de la Propuesta de Reglamento COM(2021) 759 final.

37. Art. 3 (1) Propuesta de Reglamento COM(2021) 759 final.

informático *ad hoc* que cuente con las características específicas anteriormente mencionadas –descentralizado, seguro, y fiable–. El carácter descentralizado de ese sistema informático debería permitir intercambios de datos seguros exclusivamente entre un Estado miembro y otro, sin la intervención de terceros en el contenido. Aunque el articulado de la Propuesta de Reglamento DIG no lo especifica, los puntos de acceso del sistema deberán estar basados en la tecnología de la plataforma e-CODEX[38], cuyo Reglamento además ha sido recientemente adoptado[39].

A pesar de instaurar obligatoriamente el principio "digital por defecto" en las comunicaciones entre autoridades a través de un sistema descentralizado, la propia Propuesta de Reglamento DIG prevé excepciones al uso obligatorio de este sistema. En primer lugar, se contempla expresamente la posibilidad de que la comunicación electrónica no se pueda transmitir a través del sistema informático descentralizado *ad hoc* porque este no esté operativo debido a alguna interrupción transitoria, o bien porque la naturaleza del material a transmitir o circunstancias excepcionales desaconsejen su uso. En estos casos, la redacción actual de la Propuesta de Reglamento DIG permitiría que la comunicación se lleve a cabo a través del medio alternativo más rápido y apropiado, siempre teniendo en cuenta la necesidad de asegurar que el intercambio de información se realiza de una manera segura y fiable[40]. Esto en la práctica se traducirá en la posibilidad de utilizar un sistema de transmisión alternativo –tanto digital como tradicional– para el intercambio de información, siempre y cuando este sistema ofrezca unos estándares de seguridad y fiabilidad adecuados. A falta de una mayor concreción en el texto actual de la iniciativa, parece que serán los Estados miembros los encargados de determinar qué tipo de sistemas alternativos (v.g. correo electrónico seguro, correo postal certificado) pueden suplir válidamente al sistema descentralizado en caso de disrupción transitoria del sistema o la concurrencia cualquiera de las otras causas tasadas –y excesivamente ambiguas– previstas como excepción.

En segundo lugar, cuando el uso del sistema informático descentralizado no se estime apropiado en atención a las especificas circunstancias de la comunicación a transmitir, cualquier otro medio de comunicación podrá usarse[41]. Esta cláusula de escape permitiría el uso subsidiario y excepcional de medios comunicación más informales entre las autoridades

38. *Vid*. Considerando 11 Propuesta de Reglamento COM(2021) 759 final.
39. Reglamento (UE) 2022/850 relativo a un sistema informatizado para el intercambio electrónico transfronterizo de datos en el ámbito de la cooperación judicial en materia civil y penal (sistema e-CODEX) (DO L 150 de 1 de junio de 2022).
40. Art. 3 (2) Propuesta de Reglamento COM(2021) 759 final.
41. Art. 3 (3) Propuesta de Reglamento COM(2021) 759 final.

nacionales, tales como el correo electrónico convencional. Nuevamente, nada dice la actual redacción de la Propuesta de Reglamento DIG sobre qué circunstancias específicas podrían llegar a motivar este uso subsidiario de la comunicación no segura, por lo que ha de entenderse que su recurso quedará sujeto al prudente arbitrio de las propias autoridades que llevarán a cabo la comunicación. No obstante, el texto sí prohíbe expresamente el uso de esta excepción para el intercambio de formularios previstos en los instrumentos enumerados en el Anexo II (por ejemplo, el intercambio de formularios de ODE o de OEI), que por lo tanto deberán transmitirse utilizando medios seguros y fiables y, preferentemente, de manera electrónica[42].

3. USO DE VIDEOCONFERENCIA U OTROS MEDIOS ANÁLOGOS DE COMUNICACIÓN A DISTANCIA EN PROCESOS PENALES TRANSFRONTERIZOS

3.1. Requisitos comunes básicos: la prevalencia del consentimiento

El Capítulo IV – art. 8 de la Propuesta de Reglamento DIG se centra en el uso de la videoconferencia u otras tecnologías de comunicación a distancia en el curso de procesos penales con elementos transfronterizos en los Estados miembros de la Unión Europea.

Cuando la autoridad nacional competente de un Estado miembro solicite la audiencia de una persona investigada, acusada o condenada en procedimientos encuadrados dentro de cualquiera de los actos jurídicos listados en el Anexo II, la autoridad competente que recibe la solicitud debe permitir la participación en la audiencia mediante videoconferencia u otro medio de comunicación a distancia, siempre y cuando la tecnología esté disponible[43]; las circunstancias particulares del caso justifiquen el uso de dicha tecnología[44] y la persona investigada o condenada exprese su consentimiento[45]. En relación con este último requisito, la persona investigada, acusada o condenada debe tener la posibilidad de ser asesorado por un abogado de conformidad con el derecho de la Unión[46] antes de prestar

42. Art. 3 (4) Propuesta de Reglamento COM(2021) 759 final.
43. Art. 8 (1) (a) Propuesta de Reglamento COM(2021) 759 final.
44. Art. 8 (1) (b) Propuesta de Reglamento COM(2021) 759 final.
45. Art. 8 (1) (c) Propuesta de Reglamento COM(2021) 759 final.
46. En consonancia con lo dispuesto en la Directiva 2013/48/UE sobre el derecho a la asistencia de letrado en los procesos penales y en los procedimientos relativos a la orden de detención europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades

válidamente su consentimiento. Por lo tanto, la Propuesta de Reglamento DIG, a diferencia de otros instrumentos de la Unión, configura el consentimiento expreso como una condición previa y obligatoria para la válida realización de la declaración mediante videoconferencia.

La disposición anterior debe considerarse una norma general –y especialmente garantista–, pero que sin embargo deberá coexistir con otras previsiones específicas que regulan el uso de videoconferencia y otros medios análogos en otros instrumentos de cooperación judicial en materia penal. En este sentido, la propia Propuesta de Reglamento DIG limita su ámbito de aplicación material, al establecer que sus disposiciones se entienden sin perjuicio de lo dispuesto en los actos jurídicos establecidos en el Anexo II[47]. Uno de estos actos jurídicos es precisamente la Directiva OEI, que en su art. 24 ya regula detalladamente la comparecencia mediante videoconferencia tanto de testigos y peritos como del propio investigado o acusado. En relación con este último caso, la Directiva OEI, a diferencia de la actual Propuesta de Reglamento DIG, contempla la falta de consentimiento del investigado o acusado como motivo de denegación potestativo y específico, por lo que su necesidad dependerá, en gran medida, de la rigidez con la que cada Estado miembros haya transpuesto esta disposición y de la propia praxis judicial a nivel nacional. Asimismo, la Directiva OEI guarda silencio sobre el tiempo y forma en la que debe prestarse este consentimiento y, especialmente, si este debe ser o no informado con la concurrencia de asistencia letrada. Este mismo esquema se repite en la ley de transposición española, la Ley de Reconocimiento Mutuo (LRM)[48], cuyo articulado solo reconoce la falta de consentimiento como motivo de denegación facultativo y no contempla expresamente la asistencia letrada previa a la hora de otorgar el consentimiento[49].

> Sin perjuicio de lo anterior, sí han de aplicarse las normas de derecho español sobre comparecencia de investigados y acusados[50], por lo que ha de entenderse que en España cualquier declaración de un investigado o

consulares durante la privación de libertad (DO L 294 de 6 de noviembre de 2013). Para un análisis en profundidad del instrumento, ARANGÜENA FANEGO, C., "El derecho a la asistencia letrada en la directiva 2013/48/UE", *Revista General de Derecho Europeo*, núm. 51, 2014.

47. Art. 8 (2) Propuesta de Reglamento COM(2021) 759 final.
48. Ley 23/2014, de reconocimiento mutuo de resoluciones penales en la Unión Europea (BOE n.º 282 de 21 de noviembre de 2014).
49. Art. 216 LRM. *Vid.* DE HOYOS SANCHO, M., "La Orden Europea de Investigación: reflexiones sobre su potencial efectividad a la vista de los motivos de denegación del reconocimiento y ejecución en España", *Revista General de Derecho Procesal*, núm. 4, 2019.
50. Art. 216 (2) (b) LRM.

> acusado mediante videoconferencia solicitada a través de una OEI –o de cualquier otro instrumento de reconocimiento mutuo o de cooperación judicial internacional– debe siempre garantizar sus derechos de defensa y, concretamente, la concurrencia de asistencia letrada efectiva.

Así pues, la regulación genérica que propone actualmente la Propuesta de Reglamento DIG difiere en aspectos clave –singularmente, la obligatoriedad de que el investigado o acusado otorgue previamente su consentimiento– con la regulación específica preexistente en otros instrumentos ya adoptados, tales como la Directiva OEI. La actual redacción de la Propuesta de Reglamento DIG remarca su carácter subsidiario, por lo que debe entenderse que regulaciones más restrictivas desde el punto de vista de las garantías procesales prevalecerán. A mi juicio este planteamiento es erróneo, ya que la redacción genérica y más garantista que propone la Propuesta de Reglamento DIG, que además resulta en línea con las directrices más actuales de la CEPEJ[51] y la jurisprudencia del TEDH sobre esta materia[52], debería prevalecer respecto a cualesquiera otras regulaciones específicas menos garantistas. Además, la eficacia directa y no necesidad de transposición que brinda el instrumento legislativo utilizado para esta iniciativa (reglamento) permitiría, una vez adoptado, contar con un estándar mínimo uniforme en toda la Unión, acabando así con la actual fragmentación normativa fruto de la disparidad de disposiciones nacionales y la transposición desigual de la Directiva OEI en los ordenamientos jurídicos de los diferentes Estados miembros. En consecuencia, sería conveniente que durante las negociaciones se discutiese la posibilidad de convertir la regulación del uso de videoconferencia y medios análogos que contiene la Propuesta de Reglamento DIG en prevalente, de tal manera que todas las disposiciones específicas sobre la misma materia contenidas en el resto de actos jurídicos recogidos en el Anexo II solo se consideraran compatibles en tanto en cuanto no se opongan a lo dispuesto en esta. En otras palabras, esto supondría invertir el planteamiento actual del legislador europeo y convertir lo que hoy es una mera propuesta de regulación supletoria en una propuesta de aplicación preferente.

---

51. *Vid*. *Guidelines on videoconferencing in judicial proceedings*, documento adoptado por la CEPEJ en su trigésimo sexta reunión plenaria (junio 2021), pp. 14 y ss.
52. *Cfr*. entre otras SSTEDH *Marcello Viola c. Italia*, de 5 de octubre de 2006, CE:ECHR:2006:1005JUD004510604; *Asciutto c. Italia*, de 27 de noviembre de 2007, CE:ECHR:2007:1127JUD003579502; *Shulepov c. Rusia*, de 26 de junio de 2008, CE:ECHR:2008:0626JUD001543503. Sobre el uso de la videoconferencia y su incidencia en los derechos fundamentales durante la pandemia, GORI, P. y PAHLADSINGH, A., "Fundamental rights under COVID-19: an European perspective on videoconferencing in court", *ERA Forum*, vol. 21, issue 4, 2021, pp. 561-577.

3.2. Norma aplicable: el problemático reenvío al derecho nacional

En relación con las normas aplicables al procedimiento de realización de la videoconferencia u otros medios de comunicación a distancia, la Propuesta de Reglamento DIG se limita a indicar que deberá regirse por la ley del Estado miembro dónde esta se celebre, debiéndose entender por tal el Estado miembro que la organiza[53]. Naturalmente en este punto es donde podemos encontrar en la práctica mayores problemas y aplicaciones heterogéneas en función de lo dispuesto en cada ordenamiento jurídico nacional.

Esta cuestión es especialmente relevante para nuestro país. En España, se encuentra en fase avanzada de tramitación parlamentaria el Proyecto de Ley de medidas de Eficiencia Procesal (PLEP)[54] que contempla, entre otras muchas cuestiones, la racionalización y la limitación del uso de las videoconferencias en el orden penal. Conforme a su redacción actual, se requerirá la presencia física del acusado y de su letrado, con independencia de si este consiente o no prestar declaración mediante videoconferencia, en todos aquellos juicios que se sigan por delito grave[55] –es decir, que tengan asociada una pena privativa de libertad superior a cinco años–. Esta restricción no es más que la reedición y normalización, a su vez, de la que ya se lleva aplicando temporalmente desde la situación de pandemia[56], vigente en la actualidad en virtud de la Ley 3/2020[57]. Por lo tanto, si la redacción actual del PLEP finalmente entra en vigor, la legislación española seguirá manteniendo una fuerte restricción interna al uso de la videoconferencia para las declaraciones de acusados que no aparece contemplada en la Propuesta de Reglamento DIG.

53. Art. 8 (3) en relación con considerando 19 Propuesta de Reglamento COM(2021) 759 final.
54. Disponible en: https://www.congreso.es/public_oficiales/L14/CONG/BOCG/A/BOCG-14-A-97-1.PDF.
55. *Vid.* Disposición adicional octava a la LECrim incluida en el Proyecto de Ley de medidas de eficiencia procesal del servicio público de justicia (PLEP).
56. Sobre la aplicación temporal de esta restricción, resulta especialmente clarificadora la STS núm. 652/2021, de 22 de julio de 2021, ES:TS:2021:3144, FD 1.º.
57. A pesar de que, en principio, su vigencia temporal se limitaba hasta el 20 de junio de 2021, la Ley 3/2020 contempló la posibilidad de mantener las medidas contenidas en su Capítulo III –entre las que se encuentran las relativas al uso de la videoconferencia en el orden penal– hasta la declaración por parte del Gobierno de la finalización de situación de crisis sanitaria ocasionada por la COVID-19, declaración que aún no se ha producido. *Vid.* art. 14 (2) en relación con la Disposición transitoria segunda Ley 3/2020, de 18 de septiembre, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia (BOE núm. 250 de 19 de septiembre de 2020).

Particularmente interesante será determinar si esta restricción que se aplica a nivel nacional debería también aplicarse, en su caso, en la ejecución de videoconferencias solicitadas en virtud de instrumentos de cooperación basados en el principio de reconocimiento mutuo tales como la OEI, habida cuenta de la existencia de regulación específica en la Directiva OEI –el ya citado art. 24– y de la actual aplicación supletoria de la Propuesta de Reglamento DIG en estos casos. Sobre esta cuestión, lo cierto es que ni la Directiva OEI ni la LRM española limitan el ámbito penológico de aplicación de la videoconferencia, como tampoco contemplan un motivo de denegación específico basado en este motivo[58], por lo que las restricciones que contiene actualmente el derecho español y que virtualmente se mantienen en el PLEP no deberían aplicarse al contexto transfronterizo de ejecución de una OEI, so pena de incurrir en causa de incumplimiento del derecho de la Unión[59]. Bien es cierto que la Directiva OEI sí contempla como motivo potestativo específico de no ejecución que su uso en el caso concreto sea contrario a los principios fundamentales del derecho de Estado de ejecución[60], motivo que además nuestra LRM ha convertido en obligatorio[61]. Pero esta cláusula de orden público europeo[62], que no es más que una concreción de la debida protección de los derechos fundamentales[63], jamás sería aplicable en el presente supuesto, ya que la instauración de esta excepción se produjo de manera temporal en el contexto pandémico y su

58. Siendo jurisprudencia consolidada del Tribunal de Luxemburgo que la aplicación de cualquier motivo de denegación en el marco de instrumentos de reconocimiento mutuo debe considerarse la excepción. *Cfr.* entre otras SSTJUE de 5 de abril de 2016, *Aranyosi y Căldăraru*, C-404 15 Y C-659/15, EU:C:2016:198; de 1 de junio de 2016, *Bob-Dogi*, C-241/15, EU:C:2016:385; de 10 de agosto de 2017, *Tupikas*, C-270/17 PPU, EU:C:2017:628; de 23 de enero de 2018, *Piotrowski*, C-367/16, EU:C:2018:27; de 25 De julio de 2018, *ML*, C-220/18 PPU, EU:C:2018:589; de 25 de julio de 2018, *Minister for Justice and Equality*, C-216/18 PPU, EU:C:2018:586; de 15 de octubre de 2019, *Dorobantu*, C-128/18, EU:C:2019:857.

59. En este mismo sentido, Dictamen 1/21 de la Fiscalía General del Estado, sobre el uso de la videoconferencia en la cooperación judicial internacional en materia penal, en especial, pp. 28-30.

60. Art. 24 (2) (b) Directiva 2014/41/UE.

61. Art. 216 (1) LRM: "La autoridad española competente denegará el reconocimiento y ejecución de la orden europea de investigación para una comparecencia por videoconferencia u otros medios de transmisión audiovisual (…) en caso de que la ejecución de dicha medida de investigación en un caso concreto sea contraria a los principios jurídicos fundamentales del Derecho español".

62. BACHMAIER WINTER, L., "Prueba transnacional penal en Europa: la Directiva 2014/41 relativa a la Orden Europea de Investigación", *Revista General de Derecho Europeo*, núm. 36, 2015.

63. En esta misma línea, RODRÍGUEZ-MEDEL NIETO, C., *Obtención y admisibilidad en España de la prueba penal transfronteriza. De las comisiones rogatorias a la orden europea de investigación*, Thomson Reuters-Aranzadi, Cizur Menor, 2016, Capítulo VI.

posible futura consolidación aún está siendo objeto de debate. Existiendo consentimiento expreso del investigado o acusado, verdadero pilar sobre el que, a mi juicio y salvo conflicto con un interés público relevante examinado a la luz de los principios de proporcionalidad y necesidad, debería establecerse el uso de la videoconferencia en el proceso penal, no parece razonable considerar que la aplicación *ope legis* de esta restricción sirva como garantía adicional de protección de sus derechos fundamentales ni actúe como principio jurídico fundamental del derecho español, máxime cuando la audiencia mediante videoconferencia puede resultar mucho más conveniente para todas las partes involucradas, incluido el propio acusado, cuando las circunstancias específicas así lo aconsejen.

Afortunadamente, la redacción más actual del PLEP, a diferencia de su versión inicial como Anteproyecto[64] y de la vigente Ley 3/2020, sí contempla expresamente la posibilidad de no aplicar esta restricción cuando la videoconferencia se realice en el marco de la ejecución de una solicitud de cooperación internacional, siempre y cuando el acusado preste su consentimiento. Así pues, si la actual redacción del PLEP se mantiene y prospera, las autoridades competentes españolas no deberán aplicar la restricción al uso de la videoconferencia en juicios por delito grave en el contexto de aplicación de los actos jurídicos de derecho de la Unión que recoge el Anexo II de la Propuesta de Reglamento DIG. Las otras dos limitaciones que introduce el PLEP al uso de videoconferencia en procesos penales –nuevamente recuperadas de las aplicadas temporalmente en virtud de la Ley 3/2020– no resultarían problemáticas en este contexto, al depender su aplicación del consentimiento del acusado o de su abogado[65].

En síntesis, la interrelación de la normativa actualmente proyectada en la Unión Europea y en España podría abocarnos a la aplicación de diferentes regímenes y limitaciones para la audiencia mediante videoconferencia en función de su ámbito de aplicación: procesos penales puramente domésticos, en cuyo seno sí operaría la restricción al uso de la videoconferencia para la comparecencia del acusado en juicios por delitos graves propuesta por el PLEP; procedimientos de ejecución de OEI en España, en los que no debería aplicarse dicha restricción; declaraciones

64. Anteproyecto de Ley de medidas de eficiencia procesal del servicio público de Justicia. Disponible en: https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/APL%20Eficiencia%20Procesal.pdf.

65. *Vid.* Disposición adicional octava a la LECrim incluida en el PLEP. Así, se exigirá también la presencia física del investigado o acusado, a petición propia o de su defensa (es decir, en ausencia de consentimiento), en la celebración de la "vistilla" del art. 505 LECrim cuando alguna de las acusaciones interese la prisión provisional o durante el juicio en aquellos supuestos en los que la acusación solicite una pena de prisión superior a dos años.

mediante videoconferencia en el contexto de otros actos jurídicos de cooperación judicial en materia penal incluidos en el Anexo II de la Propuesta de Reglamento DIG y que no cuenten con regulación propia –singularmente, la ODE–, en los que en la actualidad las autoridades competentes españolas podrían llegar a plantearse la aplicación de la restricción nacional actualmente vigente a falta de que se apruebe la redacción actual del PLEP. No parece que la aplicación eventual de este régimen diferenciado, excesivamente complejo y que además discrimina entre acusados en procesos nacionales y transfronterizos, sea la solución más eficiente y respetuosa con las garantías de los justiciables, por lo que sería conveniente que el legislador español evaluará la oportunidad de alinear aún más nuestras disposiciones internas al régimen propuesto por el derecho de la Unión.

3.3. Realización de la videoconferencia, confidencialidad y documentación del acto

En cuanto a la forma de llevar a cabo y dirigir el acto procesal de la videoconferencia, este aspecto también se regirá por lo dispuesto en el ordenamiento jurídico de cada Estado miembro. En el caso español, más allá de las disposiciones aplicables de la LOPJ[66] y la LECrim[67] y su interpretación jurisprudencial[68], hay que tener en cuenta que el PLEP prevé la inclusión de un nuevo art. 137 bis LEC que actuará como normativa supletoria en la jurisdicción penal[69]. Esta nueva disposición, mucho más detallada que las preexistentes, establece la forma de documentación de las actuaciones, el lugar en el que debe intervenir quién declara en función de su situación personal y la necesidad de solicitar el uso de estos medios con antelación suficiente y, en todo caso, en el plazo máximo de tres días desde la notificación de la citación o del señalamiento. En el caso de la ejecución de OEI, se debe tener en cuenta también la aplicación del art. 216 LRM[70].

La Propuesta de Reglamento DIG establece que debe garantizarse la confidencialidad de las comunicaciones entre las personas investigadas,

66. *Vid*. art. 229 LOPJ.
67. *Vid*. arts. 123 (5), 306, 325, 520 (1) (c), 707, 731 bis LECrim.
68. *Cfr.* entre otras STS núm. 161/2015, de 17 de marzo de 2015, ES:TS:2015:812; STS núm. 863/2015, de 30 de diciembre de 2015, ES:TS:2015:5685; STS núm. 331/2019, de 27 de junio de 2019, ES:TS:2019:2163.
69. Disposición adicional octava a la LECrim incluida en el PLEP. La redacción del Anteproyecto preveía, en cambio, la aplicación preferente del art. 137 bis LEC en el orden jurisdiccional penal.
70. Para un estudio en profundidad, *vid.* LARO GONZÁLEZ, E., *La Orden Europea de Investigación en el Espacio Europeo de Justicia*, Tirant lo Blanch, Valencia, 2021, pp. 232-237.

acusadas o condenadas y sus respectivos abogados tanto antes como durante la audiencia mediante videoconferencia u otro medio de comunicación a distancia[71]. En definitiva, se trata de generalizar la aplicación de las mismas reglas que ya operan en los Estados miembros de la Unión Europea para las audiencias físicas tras la transposición nacional de la directiva sobre el derecho a la asistencia letrada de investigados y acusados[72]. Por lo tanto, el desafío realmente reside en asegurar que el entorno informático digital utilizado permite técnica y efectivamente esta comunicación confidencial entre la persona que comparece y su abogado, condición que normalmente le corresponderá facilitar a la autoridad que dirige el acto[73]. Este desafío es aún mayor cuando la videoconferencia se realiza en el marco de una ODE y el reclamado ejercita su derecho a la doble asistencia letrada[74], pues la confidencialidad no solo se extenderá también a la comunicación con el abogado nombrado en el Estado de emisión, sino también a las comunicaciones que puedan mantener ambos letrados para coordinar su estrategia de defensa[75].

Asimismo, cuando la grabación de las audiencias físicas esté prevista en la ley nacional del Estado miembro para casos puramente domésticos, las mismas reglas se deberán aplicar a las audiencias llevadas a cabo mediante videoconferencia u otros medios de comunicación a distancia en casos transfronterizos[76]. En todo caso, los Estados miembros deben tomar todas las medidas necesarias para asegurar que estas grabaciones son almacenadas de manera segura y que no son divulgadas públicamente.

3.4. Protección de menores y derecho a la tutela judicial efectiva

La iniciativa contempla la aplicación de reglas especiales en el caso de que la persona investigada, acusada o condenada sea menor de edad[77]. En estos casos, y en consonancia con las disposiciones de la Directiva

71. Art. 8 (4) Propuesta de Reglamento COM(2021) 759 final.
72. Art. 3 en relación con el considerando 23 de la Directiva 2013/48/UE.
73. Conforme a la jurisprudencia consolidada del TEDH, el declarante debe tener garantizada una línea de comunicación segura y reservada con su abogado, o su presencia física en las mismas condiciones. *Cfr.* SSTEDH *Shulepov c. Rusia*, de 26 de junio de 2008, CE:ECHR:2008:0626JUD001543503; Gorbunov y Gorbachev c. Rusia, de 1 de marzo de 2016, ECHR:2016:0301JUD004318306; *Sakhnovskiy c. Rusia*, de 27 de noviembre de 2018, ECHR:2018:1127JUD003915912.
74. Art. 10 Directiva 2013/48/UE; art. 50 LRM.
75. Sobre esta cuestión, *vid.* Dictamen 1/21 de la Fiscalía General del Estado, *op. cit*., pp. 30-31.
76. Art. 8 (6) Propuesta de Reglamento COM(2021) 759 final.
77. Art. 8 (5) Propuesta de Reglamento COM(2021) 759 final.

relativa a las garantías procesales de menores investigados o acusados en procesos penales[78], los titulares de la patria potestad u otro adulto adecuado designado por el menor y aceptado como tal por la autoridad competente deben ser avisados sin dilación y antes de que se lleve a cabo la audiencia. La autoridad competente debe tener en cuenta el interés superior del menor cuando decida acceder a la comparecencia del menor a través de videoconferencia u otro medio de comunicación a distancia.

Finalmente, la Propuesta de Reglamento DIG prevé que el investigado, acusado o persona condenada tenga derecho en todo caso a la tutela judicial efectiva conforme al derecho nacional de cada Estado miembro cuando entienda que alguna de las disposiciones generales de este precepto ha sido vulnerada[79]. El texto en español no concreta cuál debe ser el alcance de esta tutela judicial efectiva, mientras que la versión inglesa utiliza la expresión *effective legal remedy* y la francesa *recours juridictionnel effectif*. Parece claro que la intención de la Comisión es reconocer la posibilidad de la persona investigada, acusada o condenada de denunciar la infracción de cualquiera de las disposiciones generales que establece mediante la interposición de un recurso jurisdiccional conforme a las normas aplicables del derecho nacional. Sin embargo, teniendo nuevamente en cuenta el limitado ámbito de aplicación y el carácter subsidiario que establece el actual texto de la Propuesta de Reglamento DIG respecto a sus propias disposiciones, no está claro cuál será exactamente el ámbito de aplicación de este derecho al recurso, que además podría colisionar con la actual regulación de los Estados miembros en la aplicación de determinados instrumentos de cooperación transfronterizos[80].

---

78. Arts. 3 (2) y 5 (2) Directiva (UE) 2016/800 (DO L 132 de 21 de mayo de 2016). Sobre la aplicación de esta norma desde una perspectiva práctica, *vid.* GARRIDO CARRILLO, F. y JIMÉNEZ MARTÍN, J., "Guide to Good Practices in Procedural Treatment of Minor Offenders. The Procedural Guarantees of Suspected or Accused Minors in Criminal Proceedings", en ARANGÜENA FANEGO, C., DE HOYOS SANCHO, M. y HERNÁNDEZ LÓPEZ, A. (Eds.), *Procedural Safeguards for Suspects and Accused Persons in Criminal Proceedings. Good Practices Throughout the European Union*, Springer, Cham, 2021, pp. 73-80.

79. Art. 8 (6) Propuesta de Reglamento COM(2021) 759 final.

80. Tal podría ser el caso de España en aquellos supuestos en los que el reconocimiento y ejecución de una OEI se lleve a cabo por el Ministerio Fiscal, pues conforme al art. 24 (4) LRM, contra el decreto que se adopte no cabe recurso, sin perjuicio de las posibles impugnaciones sobre el fondo ante la autoridad de emisión y de su valoración posterior en el procedimiento penal que se siga en el Estado de emisión. Sobre esta última cuestión, *cfr*. STJUE de 11 de noviembre de 2021 *Gavanozov II*, C-852/19, EU:C:2021:902. desde la perspectiva de las autoridades españolas de emisión de OEI, *vid*. GARRIDO CARRILLO, F. J., "Debilidades de la Orden Europea de Investigación (OEI) en la lucha contra la delincuencia organizada", en GARRIDO CARRILLO, F.J. (Dir.) y FAGGIANI, V. (Coord.), *Lucha contra la criminalidad organizada y*

4. IDENTIFICACIÓN ELECTRÓNICA Y EFECTOS JURÍDICOS DE LOS DOCUMENTOS ELECTRÓNICOS

El Capítulo V de la Propuesta de Reglamento DIG pretende normalizar el uso y reconocimiento de medios y firmas digitales en el ámbito de la cooperación judicial. En este punto, la Propuesta de Reglamento DIG utiliza nuevamente una cláusula de reenvío[81], esta vez a otro acto de derecho de la Unión, de tal manera que el marco jurídico general sobre esta cuestión seguirá siendo el Reglamento (UE) n.º 910/2014 relativo a la identificación electrónica y los servicios de confianza para transacciones en el mercado interior[82]. Así pues, las disposiciones sobre servicios de confianza que establece el Reglamento (UE) n.º 910/2014 se deberán aplicar a todas las comunicaciones a través de medios electrónicos que instaurará por defecto la Propuesta de Reglamento DIG[83]. Del mismo modo, para las comunicaciones electrónicas entre autoridades competentes –incluidas las que se produzcan en el ámbito penal– en las que un documento transmitido como parte de la comunicación requiera o contenga un sello o firma manuscrita, se podrán usar indistintamente sellos y firmas electrónicas cualificadas conforme a lo dispuesto en el citado Reglamento[84].

Respecto a la eficacia jurídica de los documentos electrónicos, la Propuesta de Reglamento DIG prohíbe expresamente que se pueda denegar su eficacia en el contexto de procesos judiciales transfronterizos por el mero hecho de que se presenten en forma electrónica[85]. Esta cláusula impedirá que la aceptación de dichos documentos se supedite a su formato, equiparando así la validez y eficacia de los documentos físicos y electrónicos que se aporten al proceso. Obviamente, las autoridades judiciales deberán aplicar el mismo régimen de admisión que el que opera para los documentos en formato físico, por lo que podrán seguir denegando justificadamente su eficacia, incluso cuando la causa sea específica de los documentos electrónicos[86], pero no podrán en ningún caso requerir su aportación obligatoria en formato físico como condición para su plena validez.

---

cooperación judicial en la UE: instrumentos, límites y perspectivas en la era digital, Thomson Reuters-Aranzadi, Cizur Menor, 2022, pp. 53-54.

81. Art. 9 (1) Propuesta de Reglamento COM(2021) 759 final.
82. DO L 257 de 28 de agosto de 2014.
83. Art. 9 (2) Propuesta de Reglamento COM(2021) 759 final.
84. Art. 9 (3) Propuesta de Reglamento COM(2021) 759 final.
85. Art. 10 Propuesta de Reglamento COM(2021) 759 final.
86. *V.g.* cuando las firmas o sellos electrónicos no estén debidamente autenticados, en línea con la aplicación subsidiaria del art. 326 LEC.

5. ESTABLECIMIENTO DEL SISTEMA INFORMÁTICO DESCENTRALIZADO Y COSTES

La Propuesta de Reglamento DIG establece la obligación por parte de la Comisión de adoptar actos de ejecución para establecer el Sistema informático descentralizado. Esto incluye los siguientes extremos[87]:

1) Las especificaciones técnicas que definan los métodos de comunicación mediante medios electrónicos para el propósito del sistema informático descentralizado.

2) Las especificaciones técnicas de los protocolos de comunicación.

3) Los objetivos de seguridad de la información y las medidas técnicas pertinentes para asegurar un estándar mínimo de seguridad en la información y un alto nivel de ciberseguridad en el procesamiento y comunicación de información mediante el sistema informático descentralizado.

4) Los objetivos de mínima disponibilidad y los posibles requisitos técnicos relacionados con los servicios suministrados por el sistema informático descentralizado.

El plazo de adopción de estos actos de ejecución difiere ampliamente en función del instrumento al que se vayan a aplicar. La iniciativa propone una implementación escalonada, que comprende desde un mínimo de dos años desde su entrada en vigor (v.g. Decisión marco ODE) hasta un periodo máximo de seis años (v.g. Decisión marco ECI, sin perjuicio de la iniciativa independiente que instaurará una plataforma de colaboración).

En lo relativo a los costes de implementación del sistema, la Comisión será responsable de la creación, mantenimiento y desarrollo del software de implementación de referencia que los Estados Miembros podrán elegir aplicar como su sistema de vigilancia (*back-end*) en lugar de un sistema informático nacional propio[88]. Este sistema será financiado con cargo al presupuesto de la UE y la Comisión deberá proveer, mantener y dar soporte gratuitamente a este software de implementación de referencia[89].

Por lo que respecta a los costes del sistema informático descentralizado y los portales informáticos nacionales, estos se repartirán entre los diferentes actores envueltos en la cooperación judicial transfronteriza –Estados miembros, órganos y organismos de la Unión–. Los costes derivados de la instalación, operación y mantenimiento de los puntos de acceso del

87. Art. 12 Propuesta de Reglamento COM(2021) 759 final.
88. Art. 13 (1) Propuesta de Reglamento COM(2021) 759 final.
89. Art. 13 (2) Propuesta de Reglamento COM(2021) 759 final.

sistema descentralizado correrán a cargo del Estado miembro en el que estén localizados[90]. Igualmente, deberán afrontar los costes derivados de establecer y ajustar sus sistemas informáticos nacionales con los puntos de acceso para hacerlos interoperables –uno de los pilares de la estrategia de digitalización–, así como los costes de administración, operación y mantenimiento de dichos sistemas[91]. Para hacer frente a estos costes, los Estados miembros podrán solicitar ayudas dentro de los programas de financiación de la Unión Europea[92], siguiendo el modelo del proyecto e-CODEX.

Las agencias y órganos de la Unión también deberán asumir sus propios costes de instalación, operación y mantenimiento de los componentes que comprenden el sistema informático descentralizado que recaigan sobre su responsabilidad[93]. Asimismo, deberán asumir los costes derivados de ajustar sus sistemas de gestión de casos (*CMS*) para hacerlos interoperables con los puntos de acceso nacionales, así como sus costes de administración, operación y mantenimiento[94]. Por su parte, la Comisión deberá asumir todos los costes relacionados con el punto de acceso electrónico europeo[95].

6. PROTECCIÓN DE LA INFORMACIÓN TRANSMITIDA

Una de las mayores preocupaciones para los Estados miembros y para las instituciones, órganos y organismos de la Unión es la seguridad y confidencialidad de la información y datos transmitidos a través de medios digitales[96]. En este punto, en el ámbito penal, la Propuesta de Reglamento DIG no añade nada nuevo, ya que se limita a establecer que la autoridad competente conforme al acto jurídico aplicable en cada caso debe considerarse responsable del tratamiento a los efectos de lo dispuesto en la Directiva (UE) 2016/680[97] respecto el procesamiento de datos enviados o recibidos a través del sistema informático descentralizado[98]. En el

90. Art. 14 (1) Propuesta de Reglamento COM(2021) 759 final.
91. Art. 14 (2) Propuesta de Reglamento COM(2021) 759 final.
92. Art. 14 (3) Propuesta de Reglamento COM(2021) 759 final.
93. Art. 14 (4) Propuesta de Reglamento COM(2021) 759 final.
94. Art. 14 (5) Propuesta de Reglamento COM(2021) 759 final.
95. Art. 14 (6) Propuesta de Reglamento COM(2021) 759 final.
96. En este sentido, *vid.* las conclusiones del Dictamen del Comité Económico y Social Europeo respecto a la Propuesta de Reglamento COM(2021) 759 final y la Propuesta de Directiva COM(2021) 760 final (Documento SOC/711-EESC-2022, de 18 de mayo de 2022), en el que la seguridad y confidencialidad de las comunicaciones se consideran características esenciales para la viabilidad del sistema.
97. Art. 3 (8) Directiva (UE) 2016/680 (DO L 119 de 4 de mayo de 2016).
98. Art. 15 (1) Propuesta de Reglamento COM(2021) 759 final.

mismo sentido, la propia Comisión debe ser considerada como responsable del tratamiento a los efectos de lo dispuesto en el Reglamento (UE) 2018/1725[99] respecto a los datos personales procesados por el punto de acceso electrónico europeo[100].

En todo caso, las autoridades competentes deben procurar que la información considerada confidencial y transmitida a otra autoridad competente en el contexto de procedimientos judiciales de carácter transfronterizo, se mantiene como confidencial de acuerdo con la ley nacional del Estado miembro que recibe dicha información[101].

7. MODIFICACIÓN DE ACTOS LEGISLATIVOS

En materia de cooperación judicial penal, el propio texto de la Propuesta de Reglamento DIG incorpora disposiciones para la reforma del único instrumento legislativo de todos los listados en el anexo II que se adoptó mediante un reglamento: el Reglamento (UE) 2018/1805 sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso[102].

Las modificaciones propuestas para este acto legislativo se limitan, en esencia, a introducir en su articulado la obligación de comunicación mediante medios electrónicos por defecto entre autoridades competentes derivada del art. 3 de la Propuesta de Reglamento DIG[103] en los términos que ya han sido analizados previamente.

IV. LA PROPUESTA DE DIRECTIVA COM(2021) 760 FINAL

1. RAZÓN DE SER Y ÁMBITO DE APLICACIÓN OBJETIVO

En paralelo a la Propuesta de Reglamento DIG, la Comisión ha lanzado una propuesta de Directiva sobre la digitalización de la cooperación judicial (Propuesta de Directiva DIG). Esta directiva no introduce realmente ninguna novedad respecto a lo ya dispuesto en la Propuesta de Reglamento DIG, sino que se trata de un acto legislativo complementario y meramente instrumental que sirve de cauce idóneo para reformar ciertos instrumentos legislativos –mayoría en el ámbito penal– listados en

99. DO L 295 de 21 de noviembre de 2018.
100. Art. 15 (2) Propuesta de Reglamento COM(2021) 759 final.
101. Art. 15 (3) Propuesta de Reglamento COM(2021) 759 final.
102. DO L 303 de 28 de noviembre de 2018.
103. Art. 23 Propuesta de Reglamento COM(2021) 759 final.

los anexos de la Propuesta de Reglamento DIG. Así pues, la utilización de un acto jurídico adicional para esta labor se debe exclusivamente a las limitaciones y a la rigidez legislativa impuesta por el derecho originario, traducidas en la necesidad de modificar determinados actos –decisiones marco y directivas– mediante el uso de una directiva[104].

En consecuencia, el principal y único objetivo de la Propuesta de Directiva DIG es incorporar las disposiciones de la Propuesta de Reglamento DIG, especialmente las derivadas de su art. 3 –transmisión de información entre autoridades competentes por medios electrónicos– y de su art. 8 –uso de videoconferencia, solo para la Decisión marco ODE– en todos aquellos actos que no pueden ser reformados mediante un reglamento[105]. En materia penal, estos actos son todos los recogidos en el Anexo II, a excepción del Reglamento (UE) 2018/1805.

Nótese que el listado anterior incluye dos actos legislativos que actualmente se encuentran derogados para la mayor parte de los Estados miembros: las Decisiones marco 2003/577/JAI y 2006/783/JAI. Sin embargo, ambos instrumentos sí se siguen aplicando en las relaciones con y entre los Estados miembros que no participan en el Reglamento (UE) 2018/1805 (particularmente, Irlanda y Dinamarca), por lo que su modificación tiene como objetivo adaptar preventivamente estos actos a la era de la digitalización en el caso de que Irlanda opte finalmente por participar en la Propuesta de Reglamento DIG.

2. ÁMBITO DE APLICACIÓN ESPACIAL Y PLAZOS DE TRANSPOSICIÓN

De la misma manera que sucede con la Propuesta de Reglamento DIG, en principio todos los Estados miembros salvo Irlanda y Dinamarca participarán y estarán obligados a transponer las disposiciones de la Propuesta de Directiva DIG en el evento de que finalmente sea adoptada.

En cuanto a los plazos de transposición, se establece un plazo común general de dos años, pero que debe ponerse en relación con los plazos de implementación de los actos de ejecución que establece la Propuesta de Reglamento DIG para cada uno de los actos legislativo del Anexo II[106]. Como resultado, la siguiente tabla de transposición se aplicará a los instrumentos de cooperación judicial penal que modificará este instrumento:

104. *Vid*. en este sentido la exposición de motivos de la Propuesta de Directiva COM(2021) 760 final.
105. *Vid*. arts. 1-11 Propuesta de Directiva COM(2021) 760 final.
106. *Vid*. arts. 12-15 Propuesta de Directiva COM(2021) 760 final.

1) Decisión marco 2002/584/JAI (ODE), Decisión Marco del Consejo 2008/909/JAI y Directiva 2014/41/UE (OEI): dos años desde la adopción del acto de implementación referido en el art. 12 (3) de la Propuesta de Reglamento DIG. Es decir, un máximo de cuatro años (2+2) desde su adopción.
2) Decisión marco 2003/577/JAI, Decisión Marco 2005/214/JAI, Decisión marco 2006/783/JAI y Decisión marco 2009/948/JAI: dos años desde la adopción del acto de implementación referido en el art. 12 (5) de la Propuesta de Reglamento DIG. Es decir, un máximo de siete años (5+2) desde su adopción.
3) Decisión marco 2002/465/JAI, Decisión marco 2008/947/JAI y Decisión marco 2009/829/JAI: dos años desde la adopción del acto de implementación referido en el art. 12 (6) de la Propuesta de Reglamento DIG. Es decir, un máximo de ocho años (6+2) desde su adopción.

V. A MODO DE CONCLUSIÓN

Tras el análisis realizado en las líneas precedentes, se puede concluir que la Propuesta de Reglamento DIG –y la Directiva DIG que la complementa– introduce un marco jurídico general y aporta seguridad jurídica en aspectos clave de la cooperación judicial transfronteriza, tales como el intercambio de información por medios digitales, el uso de la videoconferencia, o el efecto jurídico de las firmas y documentos electrónicos. Todo ello debería conducir al establecimiento de una cooperación más rápida y eficiente, en línea con la estrategia de la Unión Europea, con un impacto positivo en términos de costes materiales, temporales y medioambientales[107].

Sin perjuicio de lo anterior, considero que la iniciativa peca en ocasiones de falta de ambición. La comunicación por defecto entre autoridades nacionales por medio de un sistema digital descentralizado, seguro, y fiable, uno de los objetivos principales de esta iniciativa, en realidad

107. Según datos de la evaluación de impacto de la Propuesta de Reglamento COM(2021) 759 final, el ahorro anual global medio a escala de la UE se estima en 23.372.900 € en gastos de envío y 2.216.160 € en costes de papel, lo que supone un total de 25.589.060 €. Las personas físicas y jurídicas ahorrarán 4.098.600 € en gastos de envío y 388.800 € en costes de papel. Asimismo, se ahorrarán 874 personas/año en el esfuerzo de tramitación a nivel de órganos jurisdiccionales y autoridades competentes. Cabe esperar además que el uso del canal digital tenga un impacto medioambiental positivo, debido al uso de menos papel y franqueo postal.

se ve atemperada con la inclusión de hasta dos excepciones diferentes que permiten soslayar su uso. De la misma manera, el marco general que establece para la audiencia de investigados, acusados o condenados mediante videoconferencia, acertadamente garantista y construido en torno al consentimiento, se ve ensombrecido por su carácter subsidiario y el reenvío constante al derecho nacional de los Estados miembros, lo que reduce enormemente su ámbito de aplicación real y su capacidad armonizadora.

A la falta de ambición de algunas de sus disposiciones sobre cuestiones específicas, se suman otros problemas generales que afectan al texto en su conjunto. En este sentido, se echa en falta una mayor atención a la incidencia que este proceso de digitalización puede tener en las personas –brecha digital– y, en especial, en las garantías de los investigados, acusados y condenados. Por otra parte, la incidencia de esta brecha digital en los operadores jurídicos, así como el volumen de los costes derivados de la implementación de los medios y sistemas digitales y, sobre todo, de la formación de los operadores en el uso de estos sistemas, no se reflejan con suficiente claridad en su evaluación de impacto. Tampoco ayudan los extensos periodos de implementación y transposición que recogen los actuales textos que, en determinados supuestos, pueden llegar a ser de hasta ocho años tras la adopción del Reglamento DIG, lo que puede derivar en una suerte de obsolescencia prematura de sus disposiciones.

El *iter* legislativo del paquete de propuestas presentadas por la Comisión sigue su curso con normalidad. El Consejo ya ha adoptado sendos mandatos de negociación en relación con las Propuestas de Reglamento sobre el intercambio de información en casos de terrorismo transfronterizo y sobre el establecimiento de una plataforma de colaboración para los Equipos Conjuntos de Investigación[108]. Se espera que ocurra lo mismo en los próximos meses con las Propuestas de Reglamento y Directiva DIG que han sido aquí analizadas. La reciente adopción del Reglamento e-CODEX supone sin duda un gran impulso a este proceso, al dotar de coherencia interna y seguridad jurídica a las disposiciones de las propuestas relativas al uso de un sistema de intercambio de información descentralizado, seguro y de confianza.

En definitiva, a pesar de los problemas señalados a lo largo de este estudio, estamos ante un paquete legislativo que posee verdadero potencial para adecuar la cooperación judicial en la Unión Europea a la era digital. No obstante, no hay que perder de vista que todas estas propuestas

108. *Vid.* Reunión del Consejo JAI de 9 de junio de 2022.

aún están en periodo de debate legislativo, por lo que es posible –y en algunos ámbitos, incluso deseable– que su contenido cambie sustancialmente antes de su eventual adopción final. En cualquier caso, el proceso de transición digital de la cooperación judicial en materia penal ya está en marcha, y su ineludible culminación sin duda supondrá un salto cualitativo para el Espacio de Libertad, Seguridad y Justicia en términos de mayor eficiencia y resiliencia.

IV

Criminalidad organizada, responsabilidad de las personas jurídicas y nuevas tecnologías

Capítulo 11

Compliance y sistema penal español: potencialidades y retos

Nicolás Rodríguez-García[1]

Catedrático de Derecho Procesal
Universidad de Salamanca

I. PROEMIO DE CONTEXTO

La delincuencia "moderna", en particular por la dimensión económica de sus acciones y de los efectos derivados de la misma, y los intrincados entramados financieros para generar y conservar la riqueza que ésta produce, provoca, a su vez, que las organizaciones criminales tengan la necesidad de generar estructuras y mecanismos a través de los cuales ocultar, integrar al mercado legal, operar y reinvertir los recursos ilícitos obtenidos, así como los resultados que de los mismos se obtengan. Y es sabido que en los escenarios criminales más lesivos la persona jurídica ha sido utilizada por las organizaciones delictivas, apoyándose en los efectos sinérgicos y complementarios de las concreciones del desarrollo tecnológico (*blockchain*, inteligencia artificial, internet de las cosas, gemelos digitales, etc.)[2], como pieza de su ingeniería financiera: los hechos ilícitos se producen "en" o "con" las personas jurídicas –o cuando menos "en su

1. ORCID ID 0000-0003-0045-796X y RESEARCHER ID A-8577-2017. Director, en la Universidad de Salamanca, del Grupo de Investigación "GIR: Justicia, sistema penal y criminología" (JUS-USAL). Codirector del "Máster Iberoamericano en *Compliance*", del "Máster Iberoamericano en Justicia Penal" y del "Máster Iberoamericano en Políticas Anticorrupción". Investigador del Centro de Investigación para la Gobernanza Global (CIGG-USAL). Este trabajo se ha elaborado en el marco de los Proyectos PID2019-107743RB-I00 (Ministerio de Ciencia e Innovación) –en el que soy Investigador Principal– y RED2018-102533-T (Ministerio de Economía y Competitividad).

2. *Vid*. KSHETRI, N., The Rise of Blockchains. *Disrupting Economies and Transforming Societies*, Edward Elgar Publishing, Northampton, 2022, pp. 31 y ss.

beneficio"[3]–, de ahí que cada día sea más frecuente encontrar en las diligencias penales algunas de ellas investigadas, encausadas, procesadas, acusadas y condenadas, estándose produciendo una suerte de "aprendizaje forense" sobre la marcha, al menos en nuestro sistema judicial[4].

La proliferación de este tipo de criminalidad (fraude, corrupción, crimen organizado, narcotráfico, blanqueo de capitales…) y el interés que suscita su combate, no solo al interior de los países, en los que se llegan a esgrimir inclusive amenazas a la seguridad nacional[5], sino en la comunidad internacional por afectar al desarrollo y al crecimiento económico de las regiones[6], han dado lugar a la existencia de figuras e instituciones antes ajenas al campo jurídico, las cuales han visto la luz a partir de la puesta en práctica de las estrategias político-criminales de enfrentamiento de estas clases de delincuencia[7]. Y ello podemos ejemplificarlo en nuestros días con la necesaria configuración de planes antifraude –y programas de cumplimiento normativo– para la mejor gestión de los fondos europeos *Next Generation*[8].

3. "Directo" o "indirecto", tal y como se plantea en la STS 320/2022, de 30 de marzo.
4. Así se puede constatar en la lectura de la recientemente presentada *Memoria elevada al Gobierno de S. M. presentada al inicio del año judicial por el Fiscal General del Estado Excmo. Sr. D. Álvaro García Ortiz (Madrid, 2022)*, en la que entre muchas menciones al proceso penal de las personas jurídicas se señala por una Fiscalía (Huelva) "[…] la dificultad y falta de práctica para introducir en el proceso la responsabilidad de las personas jurídicas, observándose que en ocasiones se deja de dar traslado por los órganos de instrucción de la imputación a las empresas o sociedades contra las que también se dirige el procedimiento" (p. 937).
5. *Vid.* GONZÁLEZ CUSSAC, J., "La corrupción como amenaza a la seguridad nacional", *Revista Penal*, núm. 50, 2022, pp. 152 y ss.
6. LEO CASTELA, J. I., SÁNCHEZ MACÍAS, J. I., "Las políticas de integridad corporativa como política económica en la OCDE", *Revista Finanzas y Política Económica*, vol. 13, núm. 1, 2021, pp. 143 y ss.
7. *Vid*. GÓMEZ TOMILLO, M., *Compliance penal y política legislativa. El deber personal y empresarial de evitar la comisión de ilícitos en el seno de las personas jurídicas*, Tirant lo Blanch, Valencia, 2016.
8. El Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, *por el que se establece el Mecanismo de Recuperación y Resiliencia*, en su artículo 22 establece que los Estados miembros están obligador a proteger los intereses financieros de la Unión Europea, entre otras formas tomando medidas oportunas para prevenir, detectar y corregir el fraude, la corrupción y los conflictos de intereses. En nuestro país, para hacer efectivas las iniciativas planteadas en el "Plan España Puede", las Administraciones Públicas deben adaptar los procedimientos de gestión y el modelo de control; así, algunas medidas de agilización se establecieron mediante el Real Decreto-Ley 36/2020, de 30 de diciembre, *por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia*. Además, en el desarrollo de un "sistema de gestión" que facilita la tramitación eficaz de las solicitudes de desembolso a los Servicios de la Comisión Europea, se ha aprobado la Orden HFP/1030/2021, de 29 de septiembre, *por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia*, en cuyo artículo 6 se recoge la exigencia de tener que redactar un

Aunque se considera que antaño ya se perfilaba como una medida de política criminal que se asomaba de forma tenue en el Código Penal de 1995[9], la responsabilidad penal de las personas jurídicas, y con ella los programas de cumplimiento penal *(criminal compliance programs)*, hizo su aparición en la legislación penal española en el pasado decenio a partir de las dos grandes reformas del Código Penal de 2010 y 2015, en las que, a través de los "modelos de organización y gestión", de raigambre estadounidense, se importaban estándares procedentes del marco de la autorregulación de las corporaciones privadas, las cuales buscaban establecer y capilarizar en las mismas una panoplia de principios y valores que, por su esencia, es contraria a cualquier tipo de incumplimiento legal[10]. Por tanto, una "cultura" –vasta y duradera– y no simplemente un ramillete de procesos y procedimientos a conocer y ejecutar, temporalmente, por un limitado conjunto de actores más o menos cualificados[11], requiriéndose, por ende, una adecuada institucionalización en las organizaciones[12].

A partir de estos dos hitos, y con el acicate legal de que disponer de medidas de vigilancia y control idóneas para prevenir delitos –o para reducir de forma significativa el riesgo de su comisión– puede llegar a suponer una exención de la responsabilidad penal[13], esta temática ha cobrado importancia máxima atrayendo la atención del ámbito académico,

plan de medidas antifraude para cada organismo gestor de fondos del Mecanismo de Recuperación y Resiliencia (MRR), con el objetivo de asegurar la prevención, detección y corrección del fraude, la corrupción y los conflictos de intereses. Con relación a toda esta materia véase JIMÉNEZ ASENSIO, R., "Integridad pública y prevención: a propósito del diseño y aplicación de las medidas de prevención en los planes antifraude en la gestión de fondos europeos", en REGO VILAR, S. (coord.), *Auditoría y control de la respuesta al Covid-19 y de la implementación de la iniciativa Next Generation UE. XIV Encuentros técnicos de los OCEX de Santiago de Compostela. II Premio Carlos G. Otero Díaz*, Aranzadi, Pamplona, 2022, pp. 102 y ss.; SUBIRANA DE LA CRUZ, S., FORTUNY CENDRA, M., "Implementación de medidas antifraude para la gestión de fondos Next Generation", *La Administración Práctica: Enciclopedia de Administración Municipal*, núm. 6, 2022, pp. 67 y ss.

9. *Vid.* DE LA CUESTA ARZAMENDI, J. L., "Responsabilidad penal de las personas jurídicas en el derecho español", en DE LA CUESTA ARZAMENDI, J. L. (dir.), *Responsabilidad penal de las personas jurídicas*, Aranzadi, Pamplona, 2013, pp. 49 y ss.
10. BACIGALUPO SAGGESE, S., "Compliance", *Eunomía. Revista en Cultura de la Legalidad*, núm. 21, 2021, pp. 265 y ss.
11. *Vid.* MORTON, J. C., "The development of a compliance culture", *Journal of Investment Compliance*, vol. 6, núm. 4, 2005, pp. 59 y ss.
12. *Vid.* NIETO MARTÍN, A., "La institucionalización del sistema de cumplimiento", en NIETO MARTÍN, A. (DIR.), *Manual de cumplimiento penal en la empresa*, Tirant lo Blanch, Valencia, 2015, pp. 187 y ss.
13. En relación con las estrategias habidas para incorporar en los sistemas jurídicos los programas de cumplimiento normativo *vid.* SCANDELARI, G. B., Compliance *e Prevenção Corporativa de Ilícitos. Inovações e Aprimoramentos para Programas de Integridade*, Almedina, São Paulo, 2022, pp. 63 y ss.

del sector empresarial, de la comunidad internacional y, en general, del entorno vinculado a las organizaciones en cuanto a los alcances y formas apropiadas del sistema de intervención estatal[14]. Resulta, pues, evidente que, especialmente en el ámbito criminal, el papel de la persona jurídica se haya vuelto tan trascendente, captando el interés general a consecuencia de percibirse las organizaciones como un foco de delincuencia, específicamente de aquélla con propósitos económicos, por lo cual no están eximidas de ver cómo se le pueden imponer sanciones proporcionadas, efectivas y disuasorias, tal y como orientan las instituciones europeas[15].

En este entorno complejo y enmarañado, el *compliance* se ha erigido como el instrumento a través del cual se promueve no solamente la autorregulación sino la actuación ética de la empresa; en otras palabras, el *compliance* se considera como la herramienta que posibilita que las organizaciones puedan cumplir con sus obligaciones normativas, prevengan riesgos de distintas especies y ejecuten una cultura de comportamiento ético, en una suerte de mutua retroalimentación y reciprocidad en los pensamientos y en las conductas[16]. Por ello, en el ámbito criminal, a partir de 2015 el cumplimiento corporativo ha arribado a la legislación penal española como un mecanismo tendente a la prevención –general y especial– de la criminalidad en el seno de la empresa, dando con ello muestras de la relevancia de los instrumentos institucionales en el desarrollo de una efectiva política criminal bifronte que en el Estado de Derecho coloque esquemas de promoción y protección de ideales como transparencia, ética, integridad y rendición de cuentas.

El protagonismo adquirido por la figura del *compliance* –o "complianza"[17]– como palanca de cambio para la vehiculización de una nueva política económica, jurídica e institucional mundial no debiera entenderse

14. *Vid.* DE LA CUESTA ARZAMENDI, J. L., "Responsabilidad penal…", *cit.*, pp. 49 y ss.
15. *Vid.* DE LA MATA BARRANCO, N. J., "El cumplimiento por el legislador español del mandato de la Unión Europea de sancionar a las personas jurídicas", en DE LA CUESTA ARZAMENDI, J. L. (dir.), *Responsabilidad penal de las personas jurídicas*, Aranzadi, Pamplona, 2013, pp. 161 y ss.
16. Tal y como estudian JIMÉNEZ SÁNCHEZ, F., ROS MEDINA, J. L., VILLORIA MENDIETA, M., "Determinantes de la calidad del gobierno: una exploración de los gobiernos autonómicos españoles", *Revista Española de Investigaciones Sociológicas*, núm. 180, 2022, pp. 68-69, con relación a la relevancia del comportamiento de los demás en el entorno social y organizacional, por un lado la confianza en los demás y en las principales instituciones políticas es un aspecto clave para dimensionar cómo de costoso es comportarse de manera oportunista frente al interés general; y, por otro, cuanto mayor es la percepción de abuso y corrupción y también más grande es la percepción de que los demás se comportan con oportunismo, más fácil es que un individuo justifique su propio comportamiento poco ético.
17. SÁNCHEZ MACÍAS, J. I., RODRÍGUEZ LÓPEZ, F., "Estudio preliminar", en RODRÍGUEZ-GARCÍA, N. (dir.), *Tratado angloiberoamericano sobre compliance penal*, Tirant lo Blanch, Valencia, 2021, pp. 27 y ss.

como una "moda" coyuntural y efímera, puesto que su real importancia radica en el potencial no solo preventivo del delito sino como fuente de cultura de actuación ética de la organización y la posibilidad de advertir riesgos que impacten en su reputación.

Los programas de cumplimiento emulan los principios de transparencia y buen gobierno, de ahí que también se considere como la vía que conduce el actuar ético y de autogobierno de la empresa, cuestiones que la posicionan como una herramienta de la máxima importancia en cuanto a la prevención del delito. Pero, al mismo tiempo, como el elemento que coloca a las personas jurídicas en el campo de la legalidad, del comportamiento ético y de la ejemplaridad, en el sentido de que ante los peligros inherentes a un mundo globalizado y digitalizado el marchamo de legalidad que se explicita con los *compliance programs* de las corporaciones tiene un notable efecto reputacional frente a terceros, tanto en sentido "positivo" (confiabilidad) como "negativo" (riesgos). Por ello, desde la perspectiva de la estructura empresarial, el *compliance* se ha interpretado como una institución que permite la organización y el desenvolvimiento de la actividad de la misma con apego al marco legal, en beneficio propio (directivos y empleados) y de terceros (proveedores, consumidores… y orden económico y empresarial).

Es importante resaltar que el *compliance*, como "instrumento de gestión de la desconfianza"[18], forma parte de la agenda mundial 2030 al contribuir con el cumplimiento de las metas en las que se descompone el objetivo de desarrollo sostenible (ODS) número 16 ("Paz, justicia e instituciones sólidas"), relacionadas con el combate al soborno y a la corrupción en todas sus formas, así como a la lucha contra la delincuencia, estrategia en la que adquieren una relevancia significativa las consecuencias patrimoniales de los delitos, que por su volumen se convierten en un elemento contrario al desarrollo y al crecimiento económico de los países[19] y de las regiones más desfavorecidas[20], con grave connivencia de los centros financieros extraterritoriales[21]; justamente por ello existe un empeño colectivo en maximizar

18. DARNACULLETA GARDELLA, M. M., "Consideraciones críticas sobre el *public compliance* como instrumento de gestión de la desconfianza", *La Ley Compliance Penal*, núm. 6, 2021.
19. *Vid*. ALCALÁ AGULLÓ, F., JIMÉNEZ SÁNCHEZ, F., *Los costes económicos del déficit de calidad institucional y la corrupción en España*, Fundación BBVA, Madrid, 2018, pp. 15 y ss.
20. *Vid.* ZANUTO ANDRADE SANTOS, H. C., FRAGA, G. J., "Corrupción, estructura productiva y desarrollo económico en los países en desarrollo", *Revista de la CEPAL*, núm. 130, 2020, pp. 65 y ss.
21. *Vid.* ANDERSEN, J. J., JOHANNESEN, N., RIJKERS, B., *Elite Capture of Foreign Aid. Evidence from Offshore Bank Accounts*, World Bank Group, New York, 2020.

los resultados de las políticas y acciones de recuperación de los activos robados[22]. No puede pasar inadvertida la forma en la que el ODS de referencia se posiciona como una condición posibilitante del resto de objetivos que integran la hoja de ruta mundial y a la que podemos considerar como cláusula de cuarta generación[23], que resulta la más innovadora y compleja de la Agenda al consolidarse como eje posibilitador del resto[24].

Resulta evidente el nexo entre la visión común de la humanidad para el año 2030 y el surgimiento y desarrollo de figuras como el *compliance* debido a las bondades que puede aportar a las organizaciones empresariales en forma de (auto)blindaje ante el delito. Sin embargo, debemos apreciar claramente que cuando nos encontramos en los terrenos de los *compliance programs* no podemos centrarnos exclusivamente en lo que se ha entendido como cumplimiento normativo con énfasis en el ámbito penal y remitirnos simplemente a colmar el principio de legalidad, pues estaríamos ante un reduccionismo simplista, que impediría dimensionar la magnitud y alcances del *compliance*: además de ingredientes vinculados con la prevención de riesgos económicos y reputacionales para la empresa, la generación de una cultura ética organizacional entre sus miembros y la tendencia al buen gobierno corporativo en su estructura[25].

El *compliance* es una figura que permite a la organización traspasar las fronteras del cumplimiento del marco normativo para extenderlo a un ámbito preventivo que posibilita evaluar riesgos económicos, reputacionales

22. *Vid.* BERDUGO GÓMEZ DE LA TORRE, I., FABIÁN CAPARRÓS, E. A., RODRÍGUEZ-GARCÍA, N. (dirs.), *Recuperación de activos y decomiso: reflexiones desde los sistemas penales iberoamericanos*, Tirant lo Blanch, Valencia, 2017; RODRÍGUEZ-GARCÍA, N., CARRIZO GONZÁLEZ-CASTELL, A., RODRÍGUEZ LÓPEZ, F. (dirs.), *Corrupción: compliance, represión y recuperación de activos*, Tirant lo Blanch, Valencia, 2019; BERDUGO GÓMEZ DE LA TORRE, I., RODRÍGUEZ-GARCÍA, N. (coords.), *Decomiso y recuperación de activos "Crime doesn't pay"*, Tirant lo Blanch, Valencia, 2020.

23. *Vid.* RODRÍGUEZ-GARCÍA, N., PAHUL ROBREDO, M. G., "El ODS-16 en América Latina: condicionantes, retos y materiales para su estudio comparado", en ARRABAL PLATERO, P., *Los ODS en la Justicia: El Derecho Procesal y la inteligencia artificial*, Tirant lo Blanch, Valencia, 2022, pp. 143 y ss.

24. *Vid.* BELLOSO MARTÍN, N., "El ODS 16 en la agenda 2030: de la indefinición a algunas propuestas (iusfilosóficas) para su concreción", *Quaestio Iuris*, vol. 13, núm. 4, 2020, pp. 1939 y ss.

25. De hecho, para el caso de España, la Fiscalía General del Estado, en la Circular 1/2016, de 22 de enero, *sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015 [https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2016-00001.pdf]*, ordena a los fiscales a conceder especial valor al descubrimiento de los delitos por la propia empresa, llegando hasta tener que solicitar la exención de la pena, tanto por el hecho de que la misma cuenta con un modelo de cumplimiento válido y eficaz como por evidenciarse con ello que el mismo está insertado en una cultura de cumplimiento corporativo.

y delictivos con el propósito de contar con elementos suficientes y diseñar una estrategia para evitarlos y –en su caso– corregir situaciones que puedan suponer una amenaza para la misma. Dicho de otra forma: el *compliance* promueve la reputación de la organización como una práctica continuada, pero también contribuye a prevenir y evitar riesgos, lo que la convierte en un mecanismo anticipado ante un posible escenario, pertinente e individualizable en cada caso, minado de posibles vulnerabilidades, sean o no queridas por los actores –internos y externos– de la persona jurídica.

La conveniencia de contar con esta herramienta de protección de la organización es una de las razones para que el cumplimiento normativo se considere un ingrediente muy socorrido en el desarrollo de políticas públicas dedicadas a enfrentar la delincuencia vinculada con el entorno empresarial, que por definición siempre tiene un móvil de carácter esencialmente económico. De ahí que la generalización de su estudio, diseño, implantación y control haya venido de la mano de los grandes lineamientos de organismos internacionales de base económica como el Banco Mundial[26] y la Organización para la Cooperación y el Desarrollo Económico[27], puesto que su mayor o menor éxito, junto a otros mecanismos preventivos y reactivos, en especial en materia de fraude y corrupción, darán o quitarán posiciones –absolutas y relativas– a los países en las mediciones de gobernabilidad[28] o de fortaleza del Estado de Derecho[29].

26. *Vid.* HEILBRUNN, J. R., "The Fight Against Corruption: The World Bank Debarment Policy", en MANACORDA, E., CENTONZE, F., FORTI, G., *Preventing corporate corruption: the anti-bribery compliance model*, Springer, New York, 2014, pp. 315 y ss.; SELVAGGI, N., "Las listas negras en el Banco Mundial: ¿Hacia un sistema global de sanciones?", en NIETO MARTÍN, A., MAROTO CALATAYUD, M. (dirs.), *"Public compliance": prevención de la corrupción en administraciones públicas y partidos políticos*, Universidad de Castilla-La Mancha, Cuenca, 2014, pp. 115 y ss.

27. *Vid.* RIBES RIBES, A., "Retos del International Compliance Assurance Programme (ICAP) permanente de la OCDE como modelo de cumplimiento cooperativo multilateral", *Crónica Tributaria*, núm. 182, 2022, pp. 91 y ss.; LEO CASTELA, J. I., SÁNCHEZ MACÍAS, J. I., "Las políticas de integridad…", *cit.*

28. Así sucede con los "Indicadores de Gobernabilidad" del Banco Mundial, quien utiliza como uno de ellos para ranquear más de doscientos países –y regiones– el "Índice de Control de la Corrupción", que se utiliza para dimensionar las percepciones sociales acerca de que el poder público es ejercido en beneficio privado, siendo incluidas todas las formas de corrupción, así como la captura del Estado por parte de las élites y los intereses privados. Véase *https://info.worldbank.org/governance/wgi/*.

29. *Vid.* los reportes del "Índice de Estado de Derecho", preparado por el *World Justice Project*, que mide el Estado de Derecho con base en las experiencias y percepciones tanto de la ciudadanía como de expertos de más de ciento veinte países, quienes puntúan, para prelacionarlos, ocho factores, entre ellos la "ausencia de corrupción", factor que toma en cuenta algunas formas específicas de corrupción –sobornos, influencias indebidas por intereses públicos o privados y la apropiación indebida de fondos públicos u otros recursos– y su incidencia en los tres poderes, la policía y el ejército. Véase *https://worldjusticeproject.org*.

El espacio de protección de las organizaciones a partir de los programas de *compliance* les permite contar con estrategias anticipatorias a la tutela jurídica del Estado porque llevan implícita la autorregulación –"estimulada" legalmente y, en ocasiones, "obligada"– y los controles internos como primera frontera ante los riesgos por comportamientos que puedan constituir una eventual amenaza para la persona jurídica. Una vez que se hayan traspasado los límites autoimpuestos en los controles de la organización, corresponderá al Estado someterlos a examen a través de la actividad jurisdiccional.

El *compliance* en el ámbito de la legislación penal ha venido cobrando importancia paulatinamente para la organización empresarial, transformándose poco a poco en un elemento que aporta valor a la misma toda vez que potencia el cuidado de su reputación y la protege de las conductas delictivas tanto a nivel preventivo como también por la posibilidad de servir como paliativo en caso de fincamiento de responsabilidad penal –y civil– de la persona jurídica.

La tarea de desarrollar el programa de *compliance* de una entidad es tan especial que debe encargarse a una persona capaz de detectar debilidades y posibles riesgos reputacionales y económicos para la empresa y evitar que solamente lleve a cabo una interpretación ventajosa del marco normativo aplicable. Quién puede ser, o cuando menos quién no, este oficial de cumplimiento –*compliance officer*– es una de las muchas cuestiones controvertidas en materia de *compliance*[30]. Lo que sí es indubitado es que debe ser una persona neutral y al mismo tiempo experta, no solo en cuanto a la normativa aplicable sino a la actividad de la empresa y a sus características estructurales y peculiaridades; el plan que desarrolle deberá ser "personalizado", es decir que se atendrá a las características y necesidades específicas de cada organización[31]. El oficial de cumplimiento, a través del programa de cumplimiento individualizado y exclusivo creado especialmente para una empresa, también debe dar pie a que se corrijan las debilidades y se eviten los riesgos. Por ello, el ejercicio del *compliance program* dentro de la empresa debe asignarse a una persona independiente e imparcial con respecto a la empresa y que sea capaz de generar y transmitir la cultura de integridad, transparencia y cumplimiento para el éxito y prosperidad de la organización. En suma, muchos requerimientos,

30. *Vid.* GÓMEZ MARÍN, V., "El *compliance officer* en los modelos de prevención de delitos: siete preguntas, ¿sin respuesta?", *La Ley Compliance Penal*, núm. 1, 2020.

31. *Vid.* DE LA MATA BARRANCO, N. J., "El órgano de control permanente de la persona jurídica (oficial de cumplimiento) en el marco de la responsabilidad penal corporativa", *Revista Penal México*, núm. 21, 2022, pp. 2 y ss.

amplios deberes y, como no podía ser de otra forma, una gran responsabilidad jurídica y judicial[32].

El *compliance* deberá alcanzar e implicar a todos los integrantes de la organización, incluyendo también a las más altas esferas de la misma –los "apicales"–, lo que no es óbice a que en la fijación legal de los niveles de responsabilidad y de los presupuestos a ser satisfechos en la determinación de las eventuales consecuencias jurídicas por hechos desviados se produzca una estratificación y jerarquización entre las personas de la organización[33].

Ante la necesidad de acreditar que se cuenta con un programa de cumplimiento y que el mismo se encuentra actualizado y vigente, se vuelve un factor fundamental como mecanismo para poder determinar en qué medida la entidad ha cumplido con los deberes de supervisión, vigilancia y control de la actividad de sus miembros.

La prueba relativa a los programas de cumplimiento normativo que suponen la materialización de la parte del *compliance* dedicado al ámbito penal principalmente, permitiría evidenciar si existe diligencia en su implementación y si la empresa efectivamente está cumpliendo con sus obligaciones; en tal virtud abarca de forma genérica al cumplimiento de los deberes de supervisión y control y, además, de manera puntual y específica se centra también en la actividad empresarial concreta en la que se han dado los hechos considerados como posibles delitos.

II. ABORDAJE MULTIDISCIPLINAR Y TRANSDISCIPLINAR

Aproximarse de manera correcta a una institución compleja como el *compliance* requiere integrar –y poner en diálogo– saberes y expertos de distintas disciplinas y ámbitos de conocimiento, por mucho que la socialización y divulgación de la cultura del *compliance* se haya llevado a cabo por mor del empuje de áreas jurídicas y, entre ellas, con claro liderazgo de la rama penal. En España, y en otros muchos países, podríamos preguntarnos qué habría sido del forjamiento de esa cultura si en tiempos recientes no se hubieran reformulado postulados penales clásicos –*v. gr.*,

32. *Vid*. NAVARRO, J. (dir.), *El compliance officer, ¿un profesional en riesgo? Perspectiva penal, empresarial, procesal, de la fiscalía y jurisprudencial*, Profit Editorial, Barcelona, 2018.

33. *Vid*. BOLDOVA PASAMAR, M. A., "Naturaleza jurídica de los programas de cumplimiento", *Revista General de Derecho Penal*, núm. 37, 2022, pp. 18 y ss.; NEIRA PENA, A. M., *La defensa penal de la persona jurídica. Representante defensivo, rebeldía, conformidad y compliance como objeto de prueba*, Aranzadi, Cizur Menor, 2018, pp. 194 y ss.

el *"societas delinquere non potest"*– y cambiado el articulado de normas sancionatorias de referencia para dar cabida a manifestaciones de una "justicia colaborativa"[34] –no sólo penal–, que a día de hoy tiene como un claro exponente a los programas de cumplimiento.

Ahora bien, una vez construida en conjunto la "teoría general" del *compliance*, su aplicación se lleva a cabo de manera particularizada en sectores de actividad, tanto del tradicional ámbito privado como del más novedoso público[35] –en el que la ética institucional del Estado se presupone[36]–, en campos variopintos donde puede actuar la persona jurídica (tributario, penal, medioambiental, competencia, bancario, laboral, urbanismo, contratación, comunicación, tercer sector…) y sin que importe en demasía el tamaño que tenga[37], salvo en casos extremos[38]. Por tanto, el *compliance* involucra diversos ámbitos y distintas áreas del conocimiento que debemos entender a la luz de los tiempos a los que corresponde la creación de esta figura y en el contexto dentro del que ha surgido y se ha desenvuelto en el que la nota distintiva es la falta de certeza, acrecentada por un generalizado desarrollo tecnológico y digital. Una sociedad, caracterizada por los riesgos y las inseguridades[39], puede experimentarlo como un fenómeno natural pero también como fruto del actuar humano que da lugar a amenazas o peligros de diversas clases, intensidades y efectos.

Además, se requiere hacer un enfoque transdisciplinar de la figura del *compliance* que pueda permitir sostenerlo como elemento transversal que

34. *Vid.* RODRÍGUEZ-GARCÍA, N., RODRÍGUEZ LÓPEZ, F. (coords.), *Compliance y justicia colaborativa en la prevención de la corrupción*, Tirant lo Blanch, Valencia, 2020.

35. *Vid.* CASTILLO BLANCO, F. A. (coord.), *Compliance e integridad en el sector público*, Tirant lo Blanch, Valencia, 2019; CAMPOS ACUÑA, M. C. (dir.), *Guía práctica de Compliance en el sector público*, El Consultor de Los Ayuntamientos, Madrid, 2020; SUBIRANA DE LA CRUZ, S., FORTUNY CENDRA, M. (dirs.), *Compliance en el sector público*, Aranzadi, Pamplona, 2020.

36. FERRÉ OLIVÉ, J. C., "Compliance anticorrupción", *Revista Penal*, núm. 50, 2022, p. 99.

37. *Vid*. VV. AA., *Guía de implementación de compliance para pymes. Manual práctico de implementación*, Sepin, Madrid, 2019; SÁNCHEZ MACÍAS, J. I., LEO CASTELA, J. I., *Compliance tributario para pymes según la Norma UNE 19602*, AENOR Ediciones, Madrid, 2020; SERRANO DE NICOLÁS, Y., CONESA ALAGARDA, M., ALBALÁ GONZÁLEZ, A., *Compliance penal para pymes según la Norma UNE 19601*, AENOR Ediciones, Madrid, 2020.

38. Eso sucede cuando a consecuencia del tamaño tan reducido de la estructura corporativa carece de sentido exigir en paralelo responsabilidades al gestor y a la sociedad por ausencia de mecanismos internos de control. Con relación a ello véase la STS 264/2022, de 18 de marzo.

39. *Vid*. RAMOS TORRE, R., *De la sociedad del riesgo a la sociedad de la incertidumbre*, en LUJÁN LÓPEZ, J. L., ECHEVERRÍA, J. (coords.), *Gobernar los riesgos: ciencia y valores en la sociedad del riesgo*, Biblioteca Nueva, Madrid, 2009, pp. 35 y ss.

debe estudiarse en clave de "sistema", para con ello generar una visión holística del mismo debido a la implicación de diferentes campos en torno a sujetos de derecho como las personas jurídicas, en las que se cataloga a todo tipo de entidades colectivas con estructuras organizacionales, dimensiones, características, actividades y propósitos distintos; inclusive, en el campo penal español, si así se hubiera procedido no se habrían generado las disonancias, inconsistencias y urgencias legislativas a partir de la reforma penal de 2010 a consecuencia del "olvido" legal de que la decisión de sumar a las personas jurídicas al elenco de posibles sujetos responsables penales requería, en paralelo, definir su estatuto jurídico-procesal[40].

El *compliance* es una figura concebida para alcanzar a todas las organizaciones a partir del presupuesto de que la esencia misma –variopinta y compleja de las personas jurídicas y el entorno que las acompaña– es todo menos homogéneo, y ese es uno de los retos de la complianza: implantar desde raíz una cultura organizacional –extendida entre todos los miembros de la organización– apegada al comportamiento ético, operando con estructuras que hagan posible el buen gobierno corporativo, en un entorno de detección y prevención de posibles riesgos en distintos ámbitos entre los que destaca especialmente la comisión de conductas delictivas.

Uno de los elementos que más destaca es precisamente la cultura organizacional debido al papel fundamental que desempeña, inclusive cuando hablamos de cumplimiento normativo, pues es el ecosistema dentro del cual se traza un parámetro estandarizado de acciones que se encuentran previamente estipuladas y difundidas entre todos los miembros de la organización, que no se circunscriben exclusivamente a conductas delictivas y orientan el comportamiento colectivo e individual en la actividad –estructura, gestión y operación– de la empresa en todas sus dimensiones y ámbitos.

Podemos encontrar las directrices sobre el *compliance* en el campo penal a partir de organismos como la OCDE, específicamente a través del Convenio de lucha contra la corrupción de agentes públicos extranjeros en las transacciones comerciales internacionales de 1997, y Naciones Unidas, con la Convención contra la corrupción de 2004. Estos instrumentos hallan eco en los sistemas de normalización dedicados al *compliance* y que podemos observar, por ejemplo, en los estándares de las normas ISO *(International Organization for Standardization)* y UNE (Una Norma Española), creados

40. *Vid.* RODRÍGUEZ-GARCÍA, N., "Adecuación del proceso penal español a la fijación legal de la responsabilidad criminal de las personas jurídicas", *Revista Penal*, núm. 35, 2015, pp. 139 y ss.; GIMENO BEVIÁ, J., *Compliance y proceso penal. El proceso penal de las personas jurídicas*, Civitas, Madrid, 2016; NEIRA PENA, A. M., *La instrucción de los procesos penales frente a las personas jurídicas*, Tirant lo Blanch, Valencia, 2017, pp. 131 y ss.

con la finalidad de ayudar a las empresas a establecer unos niveles de homogeneidad en relación con la gestión, la prestación de servicios y el desarrollo de productos en la industria. Sin embargo, las organizaciones resultan tan diversas y complejas que no es posible establecer un parámetro capaz de abarcar todo lo relativo al cumplimiento legal y, en tal virtud, las normas que existen actualmente se han decantado por dedicarse especialmente a la promoción de principios o protocolos básicos de actuación que puedan tener cabida en todas las empresas sin importar su estructura o dimensiones a través de las cuales se pueda llevar a cabo la promoción de los sistemas de *compliance* y lograr que efectivamente se realice la evaluación continua.

Existen otras tendencias enfocadas en la gestión del riesgo, como la que proviene del Comité de las Organizaciones Patrocinadoras de la Comisión Treadway (COSO) y que proporciona una categorización de elementos esenciales para realizar el control interno: *(i)* existencia de un ambiente de control en el que todos los integrantes sepan y entiendan que sus actos son sometidos a control; *(ii)* evaluación del riesgo en la que se determinan los objetivos y tolerancias ante los riesgos y se identifican las clases de amenazas que puedan surgir; *(iii)* actividades de control que abarcan no solo el diseño sino además la implementación de las mismas; *(iv)* información y comunicación bidireccional entre los miembros de la organización al interior, junto con un contacto con el exterior; y *(v)* actividades de supervisión cuyo propósito radica en la evaluación de los problemas y en la posibilidad de corregir las deficiencias.

A partir del conjunto de directrices y parámetros establecidos en los distintos instrumentos, los legisladores nacionales han edificado el marco normativo –y político– del *compliance*[41]. En este sentido, debemos tener presente que no existe un modelo único de abordaje del *compliance* y, además, las tradiciones y los sistemas jurídicos en los que se va a insertar son distintos y de seguimiento disforme[42]. No hay unidad doctrinal en cuanto a la esencia del *compliance* y menos en cuanto a la forma en que debe realizarse, lo que ha contribuido a dar lugar a una diversidad de sistemas de implementación en las legislaciones de los distintos países que han acogido esta figura, sin que ni tan siquiera podamos colegir grandes patrones

41. *Vid*. SÁIZ PEÑA, C. A., *Compliance. Cómo gestionar los riesgos normativos en la empresa*, Cizur Menor, Aranzadi, 2015.

42. *Vid.* GÓMEZ COLOMER, J. L., "Introducción: La responsabilidad penal de las personas jurídicas y el control de su actividad: Estructura jurídica general en el Derecho Procesal Penal español y cultura de cumplimiento *(Compliance Programs)*", en GÓMEZ COLOMER, J. L. (coord.), *Tratado sobre compliance penal. Responsabilidad penal de las personas jurídicas y modelos de organización y gestión*, Tirant lo Blanch, Valencia, 2019, pp. 27 y ss.

comunes entre regiones[43], ni en su tratamiento general[44] ni vinculado a la responsabilidad –penal, o no– de las personas jurídicas[45].

Al lado de los modelos internacionales encontramos en España instrumentos surgidos en el seno de la Comisión Nacional del Mercado de Valores que a partir de 1998 en su informe para el estudio de un código ético de las consejos de administración de las sociedades –Comisión Olivencia– y del informe para el fomento de la transparencia y seguridad en los mercados y sociedades cotizadas –Comisión Aldama–, han dado lugar a diversos códigos éticos a través de los cuales se han adentrado los programas de cumplimiento, de forma voluntaria, para las empresas cotizadas. La última versión del Código de Buen Gobierno de las Sociedades Cotizadas de 2020, que conserva la voluntariedad sujeta al principio de "cumplir o explicar" de sus antecesores, los dota de una flexibilidad que puede calificarse de extrema. Lo cierto es que sirve de complemento a las normas legales de obligado cumplimiento previstas en las distintas ramas en las que se disponen de cuestiones de obligado cumplimiento[46].

---

43. Bien es verdad que el liderazgo en la definición y actualización de la estrategia –*a seguir*– en materia de responsabilidad de las personas jurídicas, no sólo penal, siempre procede de Estados Unidos y de su Departamento de Justicia. De hecho, este 15 de septiembre de 2022 la Fiscal General Lisa O. Monaco ha hecho público un memorándum *(Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group)* con el nuevo enfoque que han de seguir los fiscales estadounidenses en la depuración de responsabilidades por hechos delictivos cometidos por empresas, manteniéndose la prioridad de identificar y responsabilizar a las personas físicas, tanto a consecuencia del desarrollo de procesos completos como de la suscripción de acuerdos negociados, en los que los programas de cumplimiento desempeñan un papel fundamental, al ser esencial en las organizaciones tener una cultura corporativa que disuada el comportamiento ilegal e incentive –y recompense– las acciones éticas. Sobre ello véase MACHADO DE SOUZA, R., RODRÍGUEZ-GARCÍA, N., *Justicia negociada y personas jurídicas. La 'modernización' de los sistemas penales en clave norteamericana*, Tirant lo Blanch, Valencia, 2022, pp. 144 y ss.
44. *Vid*. RODRÍGUEZ-GARCÍA, N. (dir.), *Tratado angloiberoamericano sobre compliance penal*, Tirant lo Blanch, Valencia, 2021; SANTANA LORENZO, M. (dir.), *Guía práctica de compliance internacional*, Aranzadi, Pamplona, 2020; GÓMEZ COLOMER, J. L. (coord.), *Tratado sobre compliance penal. Responsabilidad penal de las personas jurídicas y modelos de organización y gestión*, Tirant lo Blanch, Valencia, 2019; LACERDA DA COSTA PINTO, F. de, LLEDÓ BENITO, I., PEREIRA COUTINHO, F. (dirs.), *Compliance y lucha contra la corrupción en España, Portugal e Iberoamérica*, Dykinson, Madrid, 2022.
45. *Vid*. WORLD COMPLIANCE ASSOCIATION, *Guía de Legislación comparada en materia de responsabilidad penal*, WCA Internacional, Madrid, 2022 [*https://worldcomplianceassociation.com/documentacion/Guia_de_legislacion_comparada_en_materia_de_responsabilidad_penal_2022.pdf*].
46. Por la actualidad de los datos aportados con relación al sector privado español, y la relevancia que tiene el "cumplimiento normativo" en su organización y actuaciones, trascendiendo de su concepción como una cultura –abstracta– dando paso a un elenco de pautas de actuación que puedan guiar el correcto proceder en la actividad

Nos enfrentamos, entonces, a la multiplicidad de normas aplicables y al desafío que supone hacerse una idea completa de las previsiones relativas a la empresa que tengan relación o impacto con el ejercicio de *compliance* que ésta debe llevar a cabo, situación que supone la necesidad del desarrollo de una buena técnica legislativa y aplicación de principios de mejora regulatoria para evitar fragmentaciones, disposiciones que se solapan o contradicen, tratándose de evitar la utilización de conceptos que puedan resultar indeterminados o que den margen a la posibilidad de distintas interpretaciones.

Y es que dentro de los textos legales podemos ver la figura del *compliance* aderezada con diversos términos (eficacia, gravedad, adecuación, seguridad, idoneidad…) que pueden dar lugar a dudas y divergencias, no solo en cuanto a la adopción de procesos, procedimientos y asignación de funciones dentro de la organización que *ex ante* los satisfagan, sino en relación a su implementación, ejecución y, especialmente, en el momento –*ex post*– en que se requiera acreditar que se han verificado positivamente esas adjetivaciones que acompañan y deben integrar el cumplimiento normativo[47], que también hace uso del desarrollo digital –con sus propias limitaciones y riesgos[48]–, las cuales requieren de específicas reglas para su valoración judicial[49]. Entrados en este punto, conviene destacar la necesi-

empresarial –en concreto–, véase TRANSPARENCY INTERNATIONAL ESPAÑA, *Transparencia de la Información Corporativa. TRAC-España 2022. Índice de Transparencia Corporativa en Integridad, Cumplimiento y Derechos Humanos de las Empresas del IBEX-35*, Transparency International España, Madrid, 2022 *[https://transparencia.org.es/wp-content/uploads/2022/04/TRAC-ESPANA-2022-TI-E.pdf]*.

47. Es decir, un satisfactorio ciclo completo, continuo y efectivo de las tres "C": "Comunicación" –*from top to bottom*–, "Confirmación" –*right or wrong*– y "Corrección" –*effective*–. Véase WALLACE, L., LIN, H., CEFARATTI, M. A., "Information Security and Sarbanes-Oxley Compliance: An Exploratory Study", *Journal of Information Systems*, vol. 25, núm. 1, 2011, pp. 185 y ss.

48. *Vid.* MESEGUER YEBRA, J., "Más transparencia para una Administración algorítmica", *Diario El País*, 14 de septiembre de 2022 *[https://elpais.com/tecnologia/2022-09-14/mas-transparencia-para-una-administracion-algoritmica.html]*; FUENTES SORIANO, O., "El valor probatorio de la información digital captada por el empresario: grabaciones y comunicaciones electrónicas", en FUENTES SORIANO, O., *Tecnología y proceso. Problemas procesales en un mundo digital*, Aranzadi, Pamplona, 2022, pp. 20 y ss.; GÓMEZ COLOMER, J. L., "Derechos fundamentales, proceso e Inteligencia Artificial: una reflexión", en CALAZA LÓPEZ, S., LLORENTE SÁNCHEZ-ARJONA, M., *Inteligencia artificial legal y la administración de justicia*, Aranzadi, Cizur Menor, 2022, pp. 264 y ss.; LLORENTE SÁNCHEZ-ARJONA, M., "Inteligencia artificial, valoración del riesgo y derecho al debido proceso", en CALAZA LÓPEZ, S., LLORENTE SÁNCHEZ-ARJONA, M., *Inteligencia artificial legal…, cit.*, pp. 373 y ss.; BARONA VILAR, S., *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021, pp. 390 y ss.

49. *Vid.* NEIRA PENA, A. M., "La prueba pericial en los delitos económicos. De la pericial contable al perito de *compliance*", *Estudios Penales y Criminológicos*, vol. XL, 2020, pp. 705 y ss.

dad de preparación y formación de los distintos operadores jurídicos en el dominio de los asuntos relacionados con el *compliance* y que implican necesariamente a grupos profesionales como los abogados de empresa, peritos y oficiales de cumplimiento, que van a requerir que indispensablemente existan procesos de formación reglada y de acreditación oficial de conocimientos que aporten los elementos necesarios para la correcta comprensión, construcción, implementación y evaluación de las actividades vinculadas al *compliance* desde distintas perspectivas y de acuerdo al rol que desempeñen las personas involucradas[50]. Específicamente, cabe resaltar la cualificación que deberá tener el oficial de cumplimiento y los alcances de su responsabilidad dentro y fuera de la organización[51].

Con carácter previo ya hemos alertado de la necesidad de que los oficiales de cumplimiento que sean elegidos reúnan las exigencias de independencia, autonomía y neutralidad, que sean conocedores del *compliance* y de todos los elementos esenciales que lo componen, pero que al mismo tiempo sean conocedores de la actividad y el sector en el que se desenvuelve la empresa para que tenga la posibilidad de generar un programa específico y *ad hoc* en la organización con la que colabora, que sea adecuado para desarrollar toda una cultura organizacional del cumplimiento a través de la implementación de protocolos y procedimientos aplicados por todos los miembros de la entidad y aplicables a terceros y que resulten eficaces en la medida en que logren adecuarse a la prevención y detección de la comisión de ciertos delitos.

El dinamismo, por ende, resulta una nota distintiva de los programas de cumplimiento, rechazándose de plano los *"paper compliance"* –programas cosméticos–, lo que supone que, en la medida de lo posible, todos los esquemas de cumplimiento deben mantenerse actualizados, ser pertinentes y estar vigentes permanentemente. Así, nunca se puede perder de vista que entre sus propósitos se encuentra el de identificar en todo momento riesgos de toda índole que permita a la organización prevenirlos *pro futuro*, organizando barreras tempranas en su detección y actuación[52], en muchas ocasiones enmendando y corrigiendo fallos ínsitos en su estructura, organización y recursos humanos.

---

50. *Vid*. LEO CASTELA, J. I., *El perito en Compliance. La ineludible intervención del experto en la administración de justicia penal frente a organizaciones y empresas*, Aranzadi, Pamplona, 2022, pp. 15 y ss.
51. *Vid*. LIÑÁN LAFUENTE, A., *La responsabilidad penal del compliance officer*, Aranzadi, Pamplona, 2019; TURIENZO FERNÁNDEZ, A., *La responsabilidad penal del compliance officer*, Marcial Pons, Madrid, 2021; VELASCO PERDIGONES, J. C., *La responsabilidad civil del Compliance Officer*, Aranzadi, Pamplona, 2022.
52. RODRÍGUEZ-GARCÍA, N., "Las investigaciones internas corporativas", en ROCA MARTÍNEZ, J. (dir.), *Procesos y prueba prohibida*, Dykinson, Madrid, 2022, pp. 205 y ss.

III. DISONANCIAS A SUPERAR

La posibilidad de que pueda atribuirse responsabilidad penal a una empresa entraña un riesgo que puede tener efectos colaterales de distinta índole (laborales, económicos, reputacionales…), pudiendo condicionar en gran medida la supervivencia de la entidad. Esta amenaza que se ciñe sobre la organización actúa como un poderoso incentivo en pro de la autorregulación; visto así, se percibe no tanto como un "fin" en sí mismo sino más bien como un "medio": verse exonerada o atenuada la persona jurídica con relación a las eventuales consecuencias jurídicas penales –¿y civiles?[53]– que le puedan ser impuestas por una resolución judicial. Tal circunstancia ha evidenciado nítidamente la imperiosa necesidad de la profesionalización y especialización del sector y sus operadores para evitar inercias, automatismos y soluciones coyunturales que no responden a una planificación estratégica tributaria de la nueva cultura ética y responsable exigible en una sociedad de riesgos.

En materia de *compliance*, la normativa aplicable y las tendencias se mantendrán en evolución y constante modificación por tratarse de una institución demasiado novel que guarda un estrecho vínculo con las empresas, en la medida en que éstas son personas jurídicas que implican una ficción legal que hace posible su ciclo vital normativizado, es decir que en la ley encuentran las condiciones para su nacimiento y existencia en la vida jurídica y cuya actividad se desenvuelve en el tráfico jurídico, económico, social y laboral en los que pueden proliferar delitos graves que cuenten con una estructura compleja y que además tengan la característica de ser transfronterizos que sean cometidos en la empresa o desde esta, para obtener un beneficio.

El reto de los diferentes países consiste en la construcción de la normativa relacionada con el *compliance* debidamente estructurada y sistematizada en clave de sistema, partiendo de la Constitución y asumiendo debidamente los compromisos internacionales con relación a algunos de sus elementos esenciales; *v. gr.*, los contenidos en la Directiva de 2019 de protección de alertantes[54], controvertida en su gestación europea y dilatada en su implementación por muchos de los países de la Unión, como es el caso de España[55].

---

53. *Vid.* SÁNCHEZ-VERA GÓMEZ-TRELLES, J., "La desobjetivización de la responsabilidad civil *ex delicto*: los programas de cumplimiento", *InDret: Revista para el Análisis del Derecho*, núm. 3, 2022, pp. 117 y ss.

54. Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, *relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión [https://www.boe.es/doue/2019/305/L00017-00056.pdf]*.

55. Deuda que se ha intentado subsanar recientemente con la presentación en el Congreso de los Diputados del "Proyecto de Ley reguladora de protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción"

El marco normativo del *compliance* penal en España nos remite necesariamente al Código Penal, que como ya sabemos ha tenido múltiples reformas y que, como se menciona al inicio de este trabajo a partir de 2010 introdujo la responsabilidad penal de la persona jurídica y en 2015 la figura del *compliance*. De la misma manera debemos centrar nuestra atención en la Ley de Enjuiciamiento Criminal, que suscita más dudas que certezas pues nos encontramos ante un proceso penal que nunca fue concebido para enjuiciar a personas jurídicas y que las nimias reformas de urgencia actuadas en 2011 y 2015 ni de lejos han generado un adecuado y completo estatuto procesal de éstas, manteniéndose dudas transcendentales; por ejemplo, si pueden concurrir en un mismo procedimiento personas físicas y jurídicas o lo más conveniente es separar los procedimientos penales para juzgarlas aisladamente, tanto si hay juicio como si el mismo se ve truncado por una declaración de conformidad[56], sobrevolando siempre un doble temor: impedir que pueda haber un desplazamiento –"malicioso"– de responsabilidades entre personas jurídicas y físicas[57] y que el contenido de la sentencia dé un tratamiento lo más igualitario posible e imponga consecuencias jurídicas adecuadas y proporcionadas en función de los hechos delictivos y de clase de persona que los ha cometido[58], pero sin que se puedan dar –en conjunto– desproporciones punitivas[59] ni vulneraciones del *non bis in idem*[60].

Más allá del texto legal podemos tomar en consideración dos circulares de la Fiscalía General del Estado emitidas a consecuencia de las

---

[https://www.congreso.es/public_oficiales/L14/CONG/BOCG/A/BOCG-14-A-123-1.PDF], la cual, desde un inicio, tiene el cuestionamiento de la sociedad civil, que a través de las veinticinco asociaciones más significadas en la materia han hecho públicas y trasladado al Gobierno y a los Grupos Parlamentarios un decálogo de mejoras *[https://www.access-info.org/es/2022-09-14/sociedad-civil-proteccion-informantes/]*.

56. *Vid*. RODRÍGUEZ-GARCÍA, N., "La conformidad en el proceso penal de las personas jurídicas", PÉREZ-CRUZ MARTÍN, A. J. (dir.), *Proceso penal y responsabilidad penal de personas jurídicas*, Aranzadi, Pamplona, 2017, pp. 177 y ss.
57. La Fiscalía General del Estado, en la Circular 1/2011, de 1 de junio, *relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 5/2010 [https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2011-00001.pdf*], llama a la atención a los fiscales para que se cuiden "[…] de que la instrucción judicial no se cierre en falso o en su fase embrionaria como consecuencia de la formalización de acuerdos de conformidad que constituyan mecanismos de deslizamiento de la responsabilidad desde la persona jurídica a la individual y viceversa".
58. *Vid*. BARKOW, R. E., "Using the Corporate Prosecution and Sentencing Model for Individuals: The Case for a Unified Federal Approach", *Law and Contemporary Problems*, vol. 83, núm. 4, 2020, pp. 160 y ss.
59. *Vid*. la STS 36/2022, de 20 de enero.
60. *Vid*. la STS 320/2022, de 30 de marzo.

dos reformas penales relativas a la responsabilidad penal de las personas jurídicas y el valor jurídico a dar al cumplimiento de los deberes de supervisión, vigilancia y control[61]. Contamos, además, con cada día más sentencias del Tribunal Supremo que han planteado diversas cuestiones nucleares en esta temática como aquellas referidas al respeto a los principios generales del Derecho Penal y Procesal penal que tienen carácter de irrenunciables también cuando se vean encausadas personas jurídicas o las que han abordado con especial dedicación sobre quién debe recaer la carga probatoria sobre la existencia del programa de cumplimiento; esto es, si la Fiscalía, en el papel de acusación, es quien debe acreditar la inexistencia en la organización de alguna medida de control eficaz ante la posible comisión de delitos en la empresa o cometidos a título de la misma, o si, por contra, ante la posibilidad de paliar los efectos jurídicos de la responsabilidad de la organización, ésta sería la más interesada en acreditar ya no la existencia del programa de cumplimento sino la forma, características y alcances de su implementación.

Actualmente en la legislación penal española la imputación de las personas jurídicas se sostiene en la omisión del debido control para evitar el delito y específicamente cuando la comisión del mismo se haya atribuido a un empleado que no ejerza funciones de representación, decisión, organización y control, consideradas como "alta dirección" será necesario acreditar que el cumplimiento al que alude la norma sea "grave". Al lado de estas dos formas de imputación, nuestra primera norma penal contempla supuestos de exención encaminados a mitigar los efectos de la comisión del delito que encuentran su fundamento en la prueba pericial de *compliance* cuyo propósito consiste en acreditar el cumplimiento normativo.

No podemos pasar por alto que a día de hoy carecemos de una especialidad o titulación en materia de *compliance*, por lo que esta tarea puede encargarse a economistas, expertos en riesgos, auditores o incluso equipos combinados entre economistas y abogados, lo que evidencia la falta de estandarización y de unificación de opiniones, dando lugar a discusiones que han hecho surgir distintas alternativas para abordar esta situación tales como la creación de cursos de formación reglada específicos y la fundación de colegios o asociaciones de profesionales en *compliance*. Como se puede observar, la profesionalización no solo se refiere a las personas en las que se deposita el cumplimiento de las obligaciones de *compliance* dentro de la empresa, sino que también se requiere especialización en materia de peritajes.

61. Las ya citadas Circulares 1/2011 y 1/2016.

El sistema de control debe establecerse adecuadamente para evitar la comisión de delitos en el seno de la empresa e incluso podrá servir de paliativo de la pena impuesta por una autoridad jurisdiccional –atenuación que solo podrá operar en situaciones en las que el programa y sus protocolos hayan funcionado inadecuadamente o en los casos en que la empresa los establezca mientras se desarrolla el proceso penal–, sin dejar de lado que, además, se deberán reconocer los hechos criminales, colaborar con la investigación y reparar el daño sufrido. En este ejercicio de prevención del delito es preciso tener en cuenta variables clasificatorias que atiendan, entre otras cuestiones, a la naturaleza y tipología de la organización, a su estructura organizativa y al sector de actuación[62].

La norma establece los requisitos para desarrollar el *compliance*, razón por la que precisa el modelo de organización y gestión que debe implementar la persona jurídica, así como los principios en torno a los que debe organizarse el sistema de prevención, que requiere *(i)* identificar las actividades susceptibles a la comisión de los delitos y por ende contar con un mapa de riesgos, *(ii)* implementar protocolos de actuación ante tales riesgos, *(iii)* poseer un canal de denuncias que pueda ser anónimo y libre de represalias y *(iv)* contar con un sistema disciplinario. Este conjunto de medidas y principios solamente puede resultar efectivo si se acompaña de la evaluación continua y promueve la mejora permanente.

Por otro lado, se debe admitir que a pesar de que la doctrina no es unánime en cuanto a la responsabilidad penal de la persona jurídica, lo cierto es que su incursión y aplicación en la legislación penal es ya un hecho consumado. Actualmente se contempla una lista de delitos –"controvertida", en especial por las ausencias– por los que pueden ser imputadas las personas jurídicas, lo que permite a éstas últimas la claridad necesaria para dotarse de una protección o blindaje frente a esas conductas delictivas específicas y, al hacerlo, pueden revestirse de la tendencia al cumplimiento, al tiempo que asumen una cultura organizacional de comportamiento ético y adoptan los principios elementales del buen gobierno corporativo.

A pesar del escudo de protección que significa el *compliance* en las organizaciones, no existe una armonización internacional en este ámbito, misma que resultaría clave para contar con un criterio universal en cuanto a los delitos que deben prevenir las empresas en aras de promover y fortalecer la eficacia en la lucha contra la delincuencia organizada transnacional.

62. *Vid*. BUZÓ OLIVÉ, J., GÓMEZ I CASALTA, G., "Sobre la configuración de un Sistema de Compliance: algunas variables a tener en consideración", *La Ley Compliance Penal*, núm. 9, 2022.

Sabido es que los instrumentos jurídicos supranacionales e internacionales se limitan a exigir a los países que legislen para que las personas jurídicas puedan ser responsables, por lo que les podrán ser impuestas sanciones eficaces, proporcionadas y disuasorias, las cuales sean consecuencia de actuaciones administrativas y jurisdiccionales no necesariamente de naturaleza penal. Siendo así, actualmente podemos encontrar diversos sistemas de responsabilidad de la empresa a nivel mundial que podemos agrupar entre los que son de naturaleza penal, aquellos que se inclinan por el ámbito administrativo, otros que sientan sus bases en las consecuencias accesorias y aquellos que son híbridos; y, además, en todos ellos conviven los distintos modelos de imputación: autorresponsabilidad, vicarial y mixto[63]. Por ello, las respuestas y tendencias ante el régimen de la responsabilidad penal de la persona jurídica y la manera de llevar a cabo el *compliance*, tendrían que emerger del ámbito internacional para asegurar la estandarización y asegurar mayor eficacia en su aplicación para evitar el riesgo de solapamientos o colisión de principios que los sostengan, dando lugar en todo caso a situaciones de impunidad.

IV. EPÍLOGO

En un mundo cada día más "global", "complejo" y "líquido", lleno de "riesgos" y "miedos" –en los sujetos participantes, en las actividades que se desarrollan y en la regulación que de todo ello se intenta–[64], es utópico pretender que los problemas que se generan puedan ser resueltos con los mismos patrones que han venido sirviendo para afrontar una realidad institucional, política, social, económica y jurídica menos intrincada, difusa y cambiante.

En este escenario y con esta premisa hay que reconocer que el *compliance* ha venido para quedarse: ha dejado de ser una opción para convertirse en un presupuesto de la estrategia de las organizaciones, por lo que para los aprendices en la materia resulta enormemente conveniente autoconvencerse a partir de la observación de las externalidades positivas que del mismo se han extraído en países que vienen transitando en la cultura del cumplimiento de manera más temprana. Entre ellas, el *compliance (i)* posibilita el acceso a nuevos sectores de actividad y mercados, en particular el extranjero, en que cada día más se da importancia al *compliance* como elemento reputacional positivo, contrastable, confiable

63. *Vid*. RODRÍGUEZ-GARCÍA, N. (dir.), *Tratado angloiberoamericano…, cit*.; GÓMEZ COLOMER, J. L. (coord.), *Tratado sobre compliance penal. Responsabilidad…, cit.*

64. *Vid*. BAUMAN, Z., *Miedo líquido*, Paidós, Barcelona, 2021.

y diferenciable de la competencia; *(ii)* refuerza la imagen corporativa; contribuye a conocer mejor los riesgos a los que se enfrenta la entidad; *(iii)* proporciona mayor transparencia y seguridad jurídica los integrantes de la organización y para externos, como proveedores y clientes; *(iv)* genera un ahorro de costes; *(v)* contribuye a depurar responsabilidades pasadas por la comisión de hechos ilegítimos, y a prevenir las futuras; e *(vi)* inocula la variable ética en la gestión de la organización y en el exigible cumplimiento legal de la misma.

Como hemos dejado constancia, la cultura del cumplimiento es un terreno muy fecundo para que, junto a otros muchos juristas y profesionales, los procesalistas –y los penalistas, *de la mano*– analicemos y debatamos las correlaciones o disonancias entre el *"law in books"* y el *"law in action"* en esta materia, tanto desde la "filosofía del lenguaje"[65] como desde la práctica forense, guiados y estimulados por sentencias y votos particulares de la Sala Segunda del Tribunal Supremo; *v. gr.*, las sentencias 154/2016, de 29 de febrero de 2016, y 668/2017, de 23 de octubre[66]. Un quehacer en el que tenemos que poner coto a la inercia, cada día más errada, de actuar siempre en tono negativo (represivo, retribucionista, cortoplacista) ante la eventualidad de que se produzcan hechos desviados cometidos por unas –pocas– personas –físicas y jurídicas–, auto justificándose en el hecho de que los mismos generan letales consecuencias con relación a la integridad pública, al desarrollo del país y a los pilares esenciales de un país democrático. En la práctica, y tal y como se viene impulsando en la región europea, se debe apostar por hacer primar un enfoque preventivo, sin descuidar obviamente la detección y corrección, como tampoco la persecución[67].

Surge la ocasión e imperiosa necesidad de considerar que en un futuro –no muy lejano– el desenvolvimiento y la expansión de las distintas formas de *compliance* en los diferentes sistemas estatales alcanzarán tal dimensión que nos encontraremos en un escenario fragmentado en el Derecho interior y plagado de enfoques de diversa naturaleza. Esta circunstancia –que supone gran incertidumbre– obliga a considerar seriamente la pertinencia

65. *Vid*. GONZÁLEZ CUSSAC, J. L., "Responsabilidad penal de las personas jurídicas: una mirada desde la filosofía del lenguaje", *Revista Penal México*, núm. 19, 2021, pp. 32 y ss.

66. *Vid*. GÓMEZ-JARA DÍEZ, C., *El Tribunal Supremo ante la Responsabilidad Penal de las Personas Jurídicas. El inicio de una larga andadura*, 2.ª ed., Cizur Menor, 2019, pp. 65 y ss.; ARES GONZÁLEZ, B., "El contenido del compliance penal en España según la jurisprudencia del Tribunal Supremo", RODRÍGUEZ-GARCÍA, N., RODRÍGUEZ LÓPEZ, F., *Compliance y justicia colaborativa en la prevención de la corrupción*, Tirant lo Blanch, Valencia, 2020, pp. 34 y ss.

67. JIMÉNEZ ASENSIO, R., "Integridad pública…", *cit.*, pp. 93 y ss.

de contar con una directriz estandarizada –original o bien "copiada"–, en la que habiéndose partido de las actuaciones y regulaciones del ámbito privado se alcance, para intentar cerrar el círculo del control ético, jurídico y judicial, al público[68], dejando a un lado disquisiciones y visiones reduccionistas de herramientas jurídicas tales como los programas de cumplimiento.

Evidentemente, disponer de un *"pack compliance"*, aunque en un inicio pueda ser visto como un "gasto" a realizar en las empresas –desde las pymes hacia las de mayor entidad–, variable en función de su tamaño, necesidad y ámbito de actuación, las experiencias habidas en los últimos lustros, en nuestro país y en casos significados extranjeros (Walmart, Petrobras, Volkswagen, Boing, etc.)[69] nos enseñan que a medio y largo plazo es una "inversión"[70] que tiene que suponer "beneficios", también evidenciables y cuantificables desde una óptica económica[71]. Una idea que gráficamente los estadounidenses resumen en la expresión *"if you think compliance is expensive, try non-compliance"*. Por tanto, con programas de cumplimiento normativo a pleno rendimiento tendremos una "ética rentable", que permite vislumbrar a todos como se anticipa la tutela jurídica del Estado en los mercados de bienes, recursos y trabajadores de toda índole.

La madurez en la utilización de este instrumento jurídico vendrá cuando cuaje en las organizaciones la idea de que ver reducida o eliminada una posible sanción tiene que ser la consecuencia de haber hecho

68. *Vid*. VALGAS DOS SANTOS, R., *Direito Administrativo do medo. Risco e fuga da responsabilição dos agentes públicos*, 2.ª ed., Revista dos Tribunais, São Paulo, 2022.

69. Véase DILORENZO, T. J., *Crimen organizado. El Estado: la verdad sin maquillaje*, Unión Editorial, Madrid, 2022, pp. 319 y ss., quien tamiza la utilidad y enseñanza de la "ética de los negocios" y las estigmatizaciones derivadas de generalizar y amplificar la presencial y efectos en una sociedad de las conductas deshonestas, fraudulentas y corruptas.

70. Entre los muchos datos interesantes contenidos en el informe "Barómetro de Empresas 51" elaborado por Deloitte Legal, el 68% de las empresas indicaban que para ellas entre los principales retos legales que tenían se encontraba el asegurar el cumplimiento normativo por parte de las asesorías internas, haciendo los ajustes necesarios con relación a la legislación sobre cumplimiento normativo *[https://www2.deloitte.com/content/dam/Deloitte/es/Documents/acerca-de-deloitte/Deloitte-ES-informe-barometro-empresas-51.pdf]*.

71. *Vid.* GOLDMAN, D. H., "Bases para el análisis económico de los sistemas de *compliance* penal", *Ius et Veritas*, núm. 57, 2018, pp. 2 y ss.; JOPPERT RAGAZZO, C. E., "Compliance concorrencial: relação de custos e benefícios pós Lava-Jato", *Quaestio Iuris*, vol. 11, núm. 2, 2018, pp. 1142 y ss.; ONTIVEROS ALONSO, M., "Noncompliance", en RODRÍGUEZ-GARCÍA, N., RODRÍGUEZ LÓPEZ, F. (coords.), Compliance *y justicia colaborativa en la prevención de la corrupción*, Tirant lo Blanch, Valencia, 2020, pp. 14 y ss.

bien las cosas en el pasado o, cuando menos, de tener la decidida voluntad de cambiar las cosas para que hechos similares y todos aquellos otros que se prevea que se puedan dar en función del ámbito de actuación propio tengan más difícil su concreción. Si así se hiciera por la mayoría de las organizaciones, aunque fuera con la intermediación de la amenaza penal impulsora de la autorregulación, el *compliance* sería una herramientas estratégica generadora de un *win-win* irrechazable en cualquier sector, ahuyentando los iniciales escepticismos –y grandes rechazos– colectivos, generando, además, atrayentes y fecundos escenarios laborales aptos para muchos profesionales resilientes golpeados en tiempos postpandémicos (certificadores, auditores, abogados de empresa, peritos, inspectores, delegados de protección de datos, gestores de canales de denuncias, responsables de recursos humanos… y responsables del cumplimiento regulatorio organizacional), los cuales tienen que interactuar durante y después de las actuaciones jurisdiccionales con fiscales y magistrados. Y en su formación y reciclaje, que no puede depender exclusivamente de cursos, conferencias, jornadas, foros y congresos, tiene que estar la Universidad, con sus titulaciones oficiales y enseñanzas propias, haciendo que esas personas más que desempeñar un "oficio" lo hagan de una "profesión" próspera y necesaria acorde a los tiempos que se viven y los que se avecinan.

Capítulo 12

Regulación, autorregulación y responsabilidad de las personas jurídicas

Paulo de Sousa Mendes*

Profesor Catedrático de la Facultad de Derecho
Universidad de Lisboa (FDUL)

I. INTRODUCCIÓN

El cumplimiento normativo (*compliance*)[1] ganó una enorme visibilidad desde que las empresas comenzaron a adoptar programas y sistemas de cumplimiento normativo, encaminados a aminorar significativamente los riesgos de responsabilización de las sociedades mercantiles y de sus respectivos directivos en los ámbitos civil, administrativo e incluso penal y, con ello, defender no sólo a los propietarios del negocio sino también, genéricamente, a los diferentes interesados[2]. El cumplimiento normativo consistió inicialmente en una autorregulación voluntaria (*voluntary self-regulation*)[3] de las empresas o grupos de empresas, extendiéndose a veces a nichos o sectores enteros de actividad económica[4]. Del interés

* Trabajo realizado en el marco del del proyecto de investigación "Proceso penal y Unión Europea. Análisis y propuestas" (Ref. PID2020-116848GB-I00). Traducido al español por José Carlos Medina Sagrario.

1. *Cf.* ROTSCH, T. (Dir.), *Criminal Compliance – Handbuch*, Nomos, Baden-Baden, 2015, § 1, n.os ms. 1-16 (pp. 35-45).
2. *Cf.* SIEBER, U. y ENGELHART, M., *Compliance Programs for the Prevention of Economic Crimes: An Empirical Survey of German Companies*, Duncker & Humblot, Berlín, 2014, pp. 1-2. También *Cf.* GÓMEZ-JARA DÍEZ, C., *Autorregulación y Responsabilidad Penal de las Personas Jurídicas*, ARA Editores, Perú, 2015, p. 76.
3. El concepto de autorregulación voluntaria se debe a BRAITHWAITE, J., "Enforced Self-Regulation: A New Strategy for Corporate Crime Control", *Mich. L. Rev.*, núm. 80, 1982, (pp. 1466-1507) p. 1469.
4. Braithwaite pone como ejemplo el programa de autorregulación sectorial creado por la Asociación Nacional de Intermediarios Financieros (*National Association of Securities*

manifestado por los reguladores públicos en relación con las ventajas del cumplimiento normativo adoptado por la propia industria, fue emergiendo la autorregulación regulada o impuesta (*enforced self-regulation*)[5]. La autorregulación impuesta significa que las empresas pasaron a ser obligadas a redactar sus propios programas de cumplimiento normativo, que fueron siendo sucesivamente ratificados por las entidades públicas competentes, como eran las agencias reguladoras sectoriales (mercados financieros y de crédito, mercado eléctrico, mercado de comunicaciones, etc.) o transversales (competencia). Ante la detección de fallos en el cumplimiento de tales normas escritas y públicamente ratificadas, tales defectos debían ser colmados por medio de la intervención efectiva de las agencias públicas[6]. La autorregulación regulada se sitúa así en un término medio entre la autorregulación pura y el control estatal directo, lo que fue posible gracias a que el cumplimiento normativo se hizo eco de la regulación de las actividades económicas. La regulación clásica se mostraba distante de la industria y adoptaba una posición formalista de mando y control (*command and control regulation*)[7]. Es decir, a cada pedido de información, auditoría o inspección del que se derivase el descubrimiento de un incumplimiento de deberes por parte de las empresas auditadas, respondía el regulador con la instauración de procedimientos de naturaleza sancionadora y la eventual aplicación de las correspondientes sanciones. Por lo contrario, la regulación responsiva (*responsive regulation*)[8] se adecúa simbióticamente a las mejoras en el cumplimiento normativo por parte de la industria, escogiendo de esta forma la oportunidad y la intensidad de la actuación, no solo supervisora, sino también sancionadora. La actuación de los reguladores, en ambos dominios, es así calibrada y dosificada de forma que permite ajustarse al comportamiento de las empresas y a su contexto. Los reguladores prefieren, así, aplicar medidas persuasivas y, en caso de ineficacia de las mismas, ir escalando sucesivamente hacia

---

Dealers – NASD), al amparo de lo dispuesto en la Sección 15A de la Ley del Mercado de Valores Mobiliarios (*Securities Exchange Act*), de 1934. Dicho programa confería a aquella entidad asociativa privada auténticos potestades inspectoras en lo tangente a instalaciones, libros y registros de los respetivos miembros para la confirmación del cumplimiento o eventual violación de los reglamentos de la autoridad reguladora del mercado de valores mobiliarios (*Cf.* BRAITHWAITE, *Mich. L. Rev.*, núm. 80, 1982, *cit.*, p. 1468).

5. El concepto de autorregulación impuesta se debe a BRAITHWAITE, *Mich. L. Rev.*, núm. 80, 1982, *cit.*, p. 1470.
6. La definición de autorregulación impuesta utilizada en el texto puede verse en AYRES, I. y BRAITHWAITE, J., *Responsive Regulation – Transcending the Deregulation Debate*, Oxford University Press, Oxford / New York, 1992, p. 6.
7. *Ibidem*.
8. El concepto de regulación responsiva se debe a AYRES y BRAITHWAITE, *Responsive Regulation*, *cit.*, p. 4 y *passim*.

medidas más severas, ya sean de aviso, tales como las cartas de advertencia, ya sean de resarcimiento de daños y perjuicios, de sanción administrativa o incluso penal, o ya sean, cuando todo falla, de suspensión o incluso revocación de licencias, siguiendo un esquema que, en sentido figurado, es designado como pirámide de la intervención regulatoria (*enforcement pyramid*)[9]. A pesar de que los conceptos de regulación responsiva y de autorregulación regulada tienen un origen doctrinal, no surgieron como meras propuestas de modelos de actuación para los reguladores y las empresas, sino más bien como el resultado de un análisis empírico de la evolución del mundo de los negocios en las sociedades desarrolladas[10]. Siendo así, revelan tendencias que tienen expresión en la realidad económica, política y social de las sociedades desarrolladas trascendiendo ya del amplio espacio anglosajón en el que surgieron.

En el presente estudio procuraremos encuadrar sumariamente las dificultades que plantea la necesidad de articulación de la regulación responsiva con la autorregulación regulada, e intentaremos dar respuesta a las siguientes cuestiones: I. ¿Cómo evitar que el regulador tenga una visión excesivamente optimista sobre la eficacia real de un programa de cumplimiento normativo que es, a fin de cuentas, impuesto? II. ¿Cómo evitar que el regulado se limite a ostentar un programa de fachada, declinando de este modo la asunción de responsabilidades al mismo tiempo que las descarga sobre los individuos de la empresa? III. ¿Como convertir a la regulación responsiva y la autorregulación regulada en una relación virtuosa?

De las respuestas a estas cuestiones que acabamos de formular genéricamente extraeremos consecuencias que nos sirvan para enfrentar otros problemas jurídicos cruciales en esta materia, a saber: IV. ¿Por qué motivo la regulación responsiva depende del marco legal vigente y no solo de la actitud simbiótica del regulador para con el regulado? V. ¿Cómo evitar que el regulador simbiótico se convierta en un blanco de captura por parte del regulado? VI. ¿Cómo evitar que las investigaciones internas en la empresa sean, en la práctica, desincentivadas por la posibilidad de que el regulador y las autoridades judiciales tengan acceso a las mismas y puedan utilizarlas para incoar procedimientos sancionadores contra el regulado?

En estas lides trataremos de algunas cuestiones más técnico-jurídicas de derecho material, fundamentalmente aquellas cuestiones relativas a la

9. El concepto de pirámide de la intervención regulatoria se debe igualmente a AYRES y BRAITHWAITE, *Responsive Regulation*, *cit.*, pp. 4, 35-38 y *passim*.

10. La formación de Braithwaite como criminólogo contribuye a este tipo de abordaje de los fenómenos estudiados.

imputación de responsabilidades, a saber: VII. ¿Cuál es la relevancia del cumplimiento normativo para la responsabilidad de las empresas en los planos administrativo y penal? VIII. ¿Cuál es la relevancia del cumplimiento normativo para la responsabilidad de los directivos y trabajadores en los planos administrativo y penal? IX. ¿Cuál es el título de imputación de responsabilidad al oficial de cumplimiento en los planos administrativo y penal?

Trataremos aún de cuestiones técnicas de derecho procesal y probatorio, tales como: X. ¿Quién tiene la carga de la prueba sobre la existencia de programas y sistemas efectivos de cumplimiento normativo?

Dejaremos para el final la respuesta a la cuestión más conceptual de todas, a saber: XI. ¿Corresponderán la regulación responsiva y la autorregulación regulada a la esfera del derecho administrativo, a la del derecho penal o a una rama emergente de derecho regulador?

II. DE LA AUTORREGULACIÓN VOLUNTARIA A LA AUTORREGULACIÓN IMPUESTA

1. Estados Unidos de América: El cumplimiento normativo tiene su origen en los Estados Unidos de América, aproximadamente a partir del año 1909, o sea, el año en el que el Tribunal Supremo Federal (*Supreme Court*) reconoció por primera vez que las sociedades mercantiles podían ser responsabilizadas por los ilícitos penales de sus agentes[11]. A partir de ese momento comenzó una paulatina toma de conciencia sobre el hecho de que litigios, sanciones, restricciones regulatorias y daños de reputación, podrían ser evitados mediante la concepción y puesta en práctica de programas de cumplimiento normativo por parte de las empresas. En la secuencia de la crisis financiera de 1929, el cumplimiento normativo pasó por una fase de gran incremento, aunque solo fuese como forma de que los hombres de negocios pudiesen reconstruir la perjudicada reputación de las empresas. El cumplimiento normativo era encarado entonces como una cuestión de autorregulación voluntaria de las empresas y de sus negocios[12].

En 1961, comenzó a producirse un drástico cambio de perspectiva en el cumplimiento normativo, desencadenado por el escándalo de las empresas de electricidad que afectó a decenas de empresas norte-americanas involucradas en prácticas colusorias de fijación de precios. Un cambio que

11. New York Central R. Co. v. United States, 212 U.S. 481 (1909).
12. *Cf.* HAUGH, T., "Criminalized Compliance", en SOKOL, D. y VAN ROOIJ, B. (Dir.), *The Cambridge Handbook of Compliance*, Cambridge University Press, Cambridge, 2021, (pp. 133-144) p. 135.

se fue acentuando a lo largo de décadas, a medida que se iban sumando escándalos de cartelización, abuso de información privilegiada y corrupción internacional[13]. Las grandes áreas de la economía fueron así sometidas a investigaciones penales. A ello siguió la producción de una amplia legislación destinada a cohibir infracciones de las empresas, lo que, a su vez, provocó que las empresas en todo el país incorporasen a sus respectivos códigos de conducta reglas específicas de prevención del crimen corporativo y promoviesen una adecuada instrucción de sus colaboradores. Este fue el inicio de la era moderna de la conformidad normativa, un período dominado por una espiral sin fin de escándalos corporativos, clamor público, legislación aplicable y multiplicación de reglas específicas de cumplimiento normativo por parte de las empresas[14].

Pero el verdadero momento de cambio cualitativo en el cumplimiento normativo llegó en 1991 con la publicación de las Directrices de Dictado de Sentencias de Organizaciones (*Organizational Sentencing Guidelines*)[15]. La innovación que trajeron estas Directrices consistió en dejar de encarar la punición de las empresas como un mero procedimiento reactivo por medio del cual las penas son fijadas en función del número y la gravedad de los ilícitos practicados para pasar a ser un procedimiento de disminución gradual por medio del cual las penas son dosificadas en función de las medidas de prevención de ilícitos ya implementadas por las empresas con anterioridad a la práctica de los propios ilícitos, enfocándose así en el propósito de inducir a las empresas a mejorar sus sistemas de conformidad normativa. Una empresa sometida a los criterios de las Directrices comienza por ser objeto de una sanción pecuniaria basada en el delito (*offense-based fine*), pero el importe de la sanción puede ser reducido en hasta un 95 por ciento si la empresa hubiese implementado un programa de conformidad eficaz operando antes del delito. La cuestión central de esta perspectiva basada en el deber (*duty-based approach*) pasó entonces a consistir en la identificación de los aspectos que hacen que un programa de conformidad sea satisfactoriamente eficaz (*effective*) para la prevención de ilícitos y la promoción de la cultura ética (en especial porque el programa obviamente falló en el caso concreto, como mínimo en alguno de esos aspectos), justificando, por eso mismo (a pesar del fallo en el caso concreto), una reducción acentuada de las sanciones aplicadas[16].

13. *Cf*. HAUGH, T., *The Cambridge Handbook of Compliance, cit*., p. 135.
14. *Cf*. HAUGH, T., *The Cambridge Handbook of Compliance, cit*., pp. 135-136.
15. Disponible online: https://www.ussc.gov/guidelines/organizational-guidelines (consultado el 14.06.2022).
16. *Cf.* HAUGH, T., *The Cambridge Handbook of Compliance*, *cit.*, p. 136. Los criterios para la evaluación de la efectividad de los programas de cumplimiento normativo están

Las Directrices desencadenaron, no sólo una explosión de conformidad por parte de las empresas, sino también una nueva actitud por parte de jueces, promotores públicos y autoridades reguladoras, dado que las Directrices se convirtieron en elementos fundamentales para cualquier tema relacionado con los ilícitos de origen empresarial. Si una empresa fuese realmente condenada, las Directrices determinarían la medida concreta de su culpabilidad. Si no llegase a verificarse una acusación, las Directrices no dejarían de ser fundamentales porque orientarían seguramente a los promotores públicos a la celebración de acuerdos de suspensión o no prosecución del procedimiento penal (*deferred or non-prosecution agreements*), naturalmente porque los elementos de un programa de conformidad eficaz fueron incorporados en el Manual de Justicia (*Justice Manual* – JM). En último análisis, cada memorando del Departamento de Justicia (*Justice Department* – DOJ) y cada informe de la Comisión del Mercado de Valores Mobiliarios (*Securities and Exchange Commission* – SEC) o de cualquier otra agencia reguladora independiente sobre la determinación del comportamiento ilícito corporativo, son decididamente influenciados por las Directrices[17].

Las Directrices también provocaron un efecto secundario imprevisto, pues llevaron a los reguladores a entrometerse en las empresas con miras a influenciar la cultura corporativa y el diseño de los programas de cumplimiento normativo[18].

Las tendencias señaladas aumentaron exponencialmente a partir de los años 2000 y durante la era de la crisis financiera de 2007-2008, cuando las principales leyes – la Ley Sarbanes-Oxley (*Sarbanes-Oxley Act* – SOX), de 2002, y la Ley Dodd-Frank (*Dodd-Frank Act* – DFA), de 2010 – criminalizaron la falta de programas de conformidad en las empresas. Ya simplemente el hecho de no cumplir correctamente, podía constituir una violación sustantiva por sí misma. La expansión legislativa relacionada con el cumplimiento normativo coincidió con la expansión del derecho penal de forma general. Actualmente, existen más de 5.000 leyes federales y, aproximadamente, 300.000 reglamentos administrativos federales que pueden ser aplicados penalmente, muchos de los cuales controlan conductas relacionadas con la economía y los negocios. No es una sorpresa, por tanto, que los crímenes corporativos y de cuello blanco hayan pasado a ser el foco de la mayor expansión de la ley federal en tres de las últimas

definidos en el Manual sobre las Directrices Sentenciadoras de los Estados Unidos (*United States Sentencing Guidelines Manual*), § 8B2.1(a)–(b) (2018).

17. *Cf*. HAUGH, T., *The Cambridge Handbook of Compliance, cit*., p. 137.
18. *Cf*. HAUGH, T., *The Cambridge Handbook of Compliance, cit*., p. 139.

cinco décadas. En gran parte, esto se derivó de la espiral, y a cada nuevo escándalo corporativo seguía la promulgación de una nueva legislación penal destinada a combatirlo[19].

2. España: El modelo norteamericano influyó en la evolución de muchos ordenamientos jurídicos nacionales. El derecho español es uno de los que más directamente refleja dicha influencia. Con la reforma del Código Penal español – CPe[20], en 2010[21], fue establecida la obligación de que las personas jurídicas tuviesen un modelo de prevención de riesgos criminales, aunque fue con la reforma de 2015[22] cuando se desarrolló la forma en que esta obligación debe ser implantada y la exención de la responsabilidad de la persona jurídica en caso de que se verifique una correcta implementación anterior a la comisión del delito o la atenuación de la pena que le es aplicada en caso de que se verifique una implementación tan solo parcial (artículo 31 bis, n.º 2, del CPe).

3. Alemania: La situación en el derecho alemán es algo diferente. En la ley alemana no existe la responsabilidad penal de las personas jurídicas, ya que el Código Penal alemán (*Strafgesetzbuch* – StGB) se aplica solamente a las personas físicas. Al no existir la responsabilidad penal de las personas jurídicas, tampoco habrá lugar, en sede de derecho penal, al establecimiento de premios para aquellas personas jurídicas que hayan adoptado programas de conformidad antes de la comisión del delito por parte de alguno de sus directivos o trabajadores.

La situación estuvo a punto de cambiar. Cuando los partidos que integraban el anterior Gobierno Federal[23] firmaron el acuerdo de coalición de 12 de marzo de 2018, estuvieron de acuerdo en la creación de un sistema de sanciones penales contra personas jurídicas. No obstante, los partidos de la anterior coalición de gobierno no fueron capaces de resolver las divergencias pendientes, lo que dio lugar, al final, al fracaso de la Propuesta de Ley de las Sanciones para Organizaciones (*Verbandssanktionsgesetz*–VerSanG),

19. *Cf*. HAUGH, T., *The Cambridge Handbook of Compliance, cit*., pp. 137-138.
20. Ley Orgánica 10/1995, de 23 de noviembre.
21. Ley Orgánica 5/2010, de 22 de junio.
22. El Código Penal español de 1995 sufrió innumerables modificaciones a lo largo de los años (treinta y dos modificaciones, incluyendo la última introducida por la Ley Orgánica 2/2019 de 1 de marzo), siendo la última de las grandes reformas la del año 2015 (Ley Orgánica 1/2015, de 30 de marzo).
23. El 4.º Gabinete de Merkel fue el 24.º Gobierno Federal de la República Federal de Alemania y estaba compuesto por una coalición entre la Unión Democrática Cristiana de Alemania (*Christlich Demokratischen Union Deutschlands* – CDU), la Unión Social Cristiana de Baviera (*Christlich-Sozialen Union in Bayern* – CSU) y el Partido Social Demócrata de Alemania (*Sozialdemokratischen Partei Deutschlands* – SPD).

de 16 de junio de 2020[24]. Por primera vez en Alemania, el VerSanG habría permitido que las personas jurídicas fuesen penalmente sancionadas y, entre otros aspectos, habría definido los requisitos legales de las investigaciones internas (*verbandsinterne Untersuchungen*). Se espera que, tras las elecciones federales de 26 de septiembre de 2021 y con el nuevo Gobierno Federal[25], sea abordada una nueva tentativa de promulgación de sanción penal de las personas jurídicas.

La inexistencia de sanciones penales para las personas jurídicas es, sin embargo, una cuestión de importancia menor o, si se quiere, un mero tecnicismo en lo tangente al binomio de la regulación responsiva y autorregulación regulada, pues basta con que existan reguladores con poderes sancionadores, por un lado, y empresas, por otro, para que se haga posible replicar la actual tendencia a una utilización responsiva de los poderes sancionadores y al fomento de la conformidad de las actividades económicas con las buenas prácticas.

Las potestades sancionadoras de las autoridades reguladoras son ejercidas en el marco del derecho de las contravenciones (*Ordnungswidrigkeitenrecht*)[26]. La posibilidad de aplicación de sanciones a empresas actualmente está garantizada por la vía del derecho de las contravenciones, que es una especie de derecho administrativo sancionador cuyas sanciones pecuniarias (*Geldbußen*), cuando son aplicadas a las empresas, pueden alcanzar valores muy significativos, en los términos del § 30 de la Ley de las Contravenciones (*Gesetz über Ordnungswidrigkeiten* – OWiG).

Es posible configurar la regulación responsiva a la luz del derecho de las contravenciones porque el § 47 OwiG deja a las autoridades administrativas la decisión de promover o no un procedimiento sancionador, en

24. Para una lectura crítica de la VerSanG, *Cf.* SCHWEIGER, T., "Quo vadis Verbandssanktionenrecht? Eine Stellungnahme im Anschluss an die Äußerungen des Bundesrates und der Bundesregierung zum Regierungsentwurf eines Verbandssanktionengesetzes", *ZIS*, núm. 2, 2021, pp. 137-154.

25. El gabinete de Scholz es el 25.º Gobierno Federal de la República Federal de Alemania y está compuesto por una coalición entre el Partido Socialdemócrata Alemán (*Sozialdemokratischen Partei Deutschlands* – SPD), Alianza 90/Los Verdes (*Bündnis 90/Die Grünen*) y el Partido Democrático Libre (*Freie Demokratische Partei* – FDP). Ver el acuerdo de coalición de 12/07/2021 (*Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands, Bündnis 90/Die Grünen und den Freien Demokraten*).

26. A excepción de Alemania y Portugal, este último influenciado por el derecho alemán, la denominación derecho de las "contraordenaciones" no existe en otros países. La comparación debe pues ser realizada con los regímenes sancionadores no penales en los que la titularidad de los procesos sancionadores pertenece a las autoridades administrativas. Itália tiene un régimen jurídico específico para el ilícito administrativo y las sanciones administrativas (*Legge 24 novembre 1981, n. 689*).

el ejercicio de una potestad que el mismo precepto designa como discrecionalidad vinculada (*pflichtgemäßes Ermessen*). La jurisprudencia y la doctrina se ocupan de la definición de los criterios a que se debe circunscribir el ejercicio de dicha potestad, atendiendo al riesgo de que las decisiones discrecionales normalmente comportan un trato desigual a las personas en situaciones equivalentes. El debate se centra, fundamentalmente, en la cuestión de saber si son o no aplicables los parámetros contemplados en el § 153 del Código del Proceso Penal (*Strafprozessordnung* – StPO) relativos a la posibilidad de no promover el procedimiento penal. De acuerdo con lo dispuesto en el § 152 StPO, salvaguardadas las excepciones previstas en ese mismo cuerpo legal, la Fiscalía (*Staatsanwaltschaft*) debe promover los procedimientos dirigidos a obtener conocimiento sobre infracciones criminales. Con todo, el § 153 StPO contempla la posibilidad de que la Fiscalía pueda no incoar el procedimiento en caso de insignificancia (*Geringfügigkeit*). De este modo, la incoación del procedimiento no obedece al estricto principio de legalidad (*Legalitätsprinzip*), en la medida en que, ante la verificación de los presupuestos definidos en el § 153 StPO, la Fiscalía dispone de una verdadera potestad para la incoación, manifestada también en otros preceptos que contemplan soluciones procesales diversas, tales como el archivo de las causas mediante la imposición de reglas de conducta (*Einstellung nach Erfüllung von Auflagen*), en los términos del §153 StPO. El Tribunal Constitucional (*Bundesverfassungsgericht* – BverfG) se pronunció en el sentido de que el margen de decisión atribuido a la Fiscalía era conforme a la Ley Fundamental (*Grundgesetz* – GG), reconociendo que el deber del Estado de garantizar una tutela de derechos eficaz, no impone el deber de promover el procedimiento penal ante todas las noticias de infracción y que tal deber podría ser incluso contrario a los principios del Estado de Derecho (*Rechtsstaatsprinzip*)[27]. En Alemania hay Directrices para los Procedimientos Penales y Administrativos Sancionadores (*Richtlinien für das Strafverfahren und das Bußgeldverfahren* – RiStBV)[28] emitidas por el Ministerio de Justicia. De ahí se deriva que cualquier decisión de no promover el proceso deba ser motivada y que, de tal decisión, deba ser dado traslado al denunciante[29].

Es dudoso que aquellas situaciones en que se dispensa la incoación de un procedimiento sancionador por parte das autoridades administrativas,

27. BVerfG, 19/06/1979 – 2 BvR 1060/78.

28. *Cf. Richtlinien für das Strafverfahren und das Bußgeldverfahren* (RiStBV), de 01/01/1977, modificadas por última vez a nivel federal en 01/11/2007 (BAnz. Nr. 208).

29. *Cf*. BIBBO, S. M., *Kriterien zur Konkretisierung des Opportunitätsprinzips im Bussgeldverfahren*, Köhler, Tübingen, 2006, pp. 177-178, y MAIAZZA, R., *Das Opportunitätsprinzip im Bussgeldverfahren unter besonderer Berücksichtigung des Kartellrechts*, Centaurus, Herbolzheim, 2003, p. 192.

correspondan siempre a casos de insignificancia de la infracción descubierta o denunciada. Muy al contrario, cualquier estrategia de intervención basada en la pirámide regulatoria recomienda que las autoridades administrativas comiencen por adoptar medidas persuasivas con independencia de la gravedad de la infracción, aunque, a fin de cuentas, las medidas deban ser escogidas en función de las circunstancias del caso concreto. Hacen falta estudios empíricos sobre la actuación de los diferentes reguladores para percibir si prefieren el modelo de mando y control o el modelo de regulación responsiva[30]. Una cosa es cierta: hay ejemplos de mando y control que, en la práctica, acabaron por no funcionar, como fue el caso de Citigroup, en el que la Autoridad Federal de Supervisión Financiera (*Bundesanstalt für Finanzdienstleistungsaufsicht* – BaFin) denunció la situación a la Fiscalía de Frankfurt (Meno), con vistas a la incoación de un proceso penal relativo a la negociación que fue efectuada por Citigroup por sospechas de la comisión de un delito de manipulación del mercado. Dada la inexistencia de responsabilidad penal de las personas jurídicas en el ordenamiento jurídico alemán, la denuncia fue presentada contra los seis operadores del Citigroup que implementaron la estrategia de negociación en cuestión[31]. La Fiscalía archivó inmediatamente el procedimiento en fecha 21 de marzo de 2005. También en Alemania, el Eurex abrió una investigación sobre el mismo caso, pero llegó a la conclusión de que la negociación efectuada por el Citigroup no violaba ninguna de las reglas de aquel mercado. No obstante, el Citigroup, debido a las características transnacionales del caso[32], fue condenado en el Reino

30. No compensan esa falta los estudios empíricos ya realizados acerca de los programas de conformidad de las empresas alemanas, cuyo ejemplo de referencia es el estudio de SIEBER y ENGELHART, *Compliance Programs for the Prevention of Economic Crimes*, *cit.*, *passim*. Naturalmente, existen también informes de las grandes auditoras, tales como, por ejemplo: *PwC's Global Economic Crime and Fraud Survey 2020 – Wirtschaftskriminalität – Ein niemals endender Kampf*. Online: https://www.pwc.de/de/consulting/forensic-services/wirtschaftskriminalitaet-ein-niemals-endender-kampf.pdf (consultado el 14/06/2022). En el referido informe es de destacar la constatación de que las autoridades de supervisión y aplicación de la ley prestan cada vez más atención a los programas de conformidad de la empresa y solicitan evidencias de su eficacia.

31. *Cf.* DONALD, D. C., "Applying Germany's market manipulation rules to disruptive trades on the Eurex and MTS platforms", *German Law Journal*, núm. 3, 2005, (pp. 649-666) p. 650.

32. El caso Citigroup presentaba elementos de conexión con varios ordenamientos jurídicos europeos, a saber: el Citigroup tenía sede en Londres, el mercado de futuros Eurex tenía sede en Frankfurt (Meno), el MTS era un sistema de negociación italiano, pero era operado en diferentes plataformas nacionales por empresas filiales. No sorprende, pues, que el caso Citigroup haya originado investigaciones por parte de diversas autoridades nacionales de supervisión de los mercados financieros.

Unido por los mismos hechos[33]. La Autoridad de Servicios Financieros (*Financial Services Authority* – FSA)[34] del Reino Unido acabó por concluir que la estrategia de negociación del Citigroup puso en riesgo la negociación ordenada en la plataforma del MTS y, por consiguiente, le aplicó una sanción administrativa pecuniaria de cerca de 14 millones de libras (21 millones de euros) que, en aquella fecha, fue la segunda más elevada de siempre en el país, en materia de mercado de capitales[35]. La sanción fue pagada inmediatamente porque la decisión final de la FSA fue negociada con el Citigroup y, por tal motivo, fue descartada su impugnación judicial. Parece ser que la FSA fue la autoridad reguladora nacional más eficaz, pues consiguió que el Citigroup, no solo pagase la sanción pecuniaria que le fue aplicada, sino que también –lo que es aún más importante– reconociese que había transgredido algunos de los llamados principios de los negocios (*principles for businesses*) que constaban en el Manual de la FSA (*FSA Handbook*)[36].

La autorregulación regulada, por su parte, es una realidad legal y corporativa armónica con los muchos regímenes jurídicos especiales que convirtieron los programas de conformidad normativa en materia de obligatorio cumplimiento. Los mecanismos de autorregulación regulada y deberes de colaboración impuestos por el Estado aparecen, por primera vez, recogidos en los preceptos de los §§ 14 de la Ley del Blanqueo de Capitales (*Geldwäschegesetz* – GwG)[37], 25 da Ley de Instituciones de Crédito (*Kreditwesengesetz* – KWG)[38] y 33 de la Ley del Mercado de Valores Mobiliarios (*Wertpapierhandelsgesetz* – WpHG)[39/40]. Como último ejemplo, cabe aquí recordar que fue presentada por el anterior Gobierno Federal,

33. *Cf.* LUCHTMAN, M., "Choice of forum and the prosecution of cross-border crime in the European Union – What role for the legality principle?", en LUCHTMAN, M. (Dir.), *Choice of Forum in Cooperation against EU Financial Crime – Freedom, Security and Justice and the Protection of Specific EU-interests*, Eleven, The Hague, 2013, (pp. 3-61) pp. 7-8.
34. La FSA fue sustituida, en 2012, por la Autoridad Financiera Comportamental (*Financial Conduct Authority* – FCA).
35. *Cf.* HERBST, J. y RUTTER, M., "Why Citigroup was fined", *The Financial Regulator*, núm. 2, 2005, pp. 65-68.
36. *Cf.* DE SOUSA MENDES, P., "Was tun im Falle von transnationalem Marktmissbrauch? – Der Fall Citigroup", *ZIS*, núm. 2, 2009, pp. 55-58.
37. *Cf. Geldwäschegesetz*, de 23/06/2017 (BGBl. I S. 1822), modificada por última vez a través del artículo 92 de la Ley de 10/08/2021 (BGBl. I S. 3436).
38. *Cf. Kreditwesengesetz*, de 09/09/1998 (BGBl. I S. 2776), modificada por última vez a través del artículo 90 de la Ley de 10/08/2021 (BGBl. I S. 3436).
39. *Cf. Wertpapierhandelsgesetz*, de 09/09/1998 (BGBl. I S. 2708), modificada por última vez a través del artículo 56 de la Ley de 10/08/2021 (BGBl. I S. 3436).
40. *Cf.* SIEBER, U., "Programas de compliance en el derecho penal de la empresa: Una nueva concepción para controlar la criminalidad económica", en ARROYO

en 2020, el Proyecto de Ley de los Canales de Suministro, el cual, tras un intenso debate político, fue aprobado, aunque con profundas alteraciones, por el Parlamento Federal, el 11 de junio de 2021, y por el Consejo Federal, el 25 de junio de 2021. La nueva Ley de Defensa de la Integridad Empresarial en los Canales de Suministro (*Gesetz über unternehmerische Sorgfaltspflichten in Lieferketten* o, abreviadamente, *Lieferkettensorgfaltspflichtengesetz* – LkSG) tiene su inicio de vigencia previsto para el 1 de enero de 2023. Además de definir un cuadro de sanciones aplicables a las infracciones previstas en la propia ley, incluye reglas de atenuación en función de las medidas de conformidad implementadas en las empresas[41].

Al margen del encuadramiento arriba referido, existen ilícitos de disconformidad que tienen relevancia penal para las personas físicas. Como vimos, el derecho penal alemán se concentra en la responsabilidad de los administradores, directores, trabajadores y el resto de representantes de las empresas[42].

La transformación de los códigos de ética en materia de cumplimiento obligatorio cuyas infracciones son sancionadas penalmente ocurrió, en un primer momento, por imperativo del § 161 de la Ley de Sociedades Anónimas (*Aktiengesetz* – AktG)[43], precepto que, aun cuando califique a los preceptos del Código de Gobernación Corporativa Alemán (*Deutscher Corporate Governance Kodex* – DCGK)[44] como meras recomendaciones (tanto así que fue elaborado por representantes de la economía privada)[45], obliga a las sociedades admitidas a cotización en la Bolsa de Valores a declarar, en sus informes y cuentas anuales, cuáles son las recomendaciones que fueron ejecutadas y cuáles no y por qué.

Esta declaración debe ser publicada en el sitio web de la sociedad anónima en cuestión. Si la información no correspondiese a la verdad, este hecho es punible, como delito de informaciones falsas con pena de prisión de hasta 3 años o pena de multa, en los términos del § 331, n.º 1, del

ZAPATERO, L. y NIETO MARTÍN, A. (Dir.), *El Derecho Penal Económico en la Era de la Compliance*, Tirant lo Blanch, Valencia, 2013, (pp. 63-109) p. 99.

41. Del acuerdo de coalición entre el CDU/CSU y SPD, de 12/03/2018, formaba parte la promulgación de legislación para incrementar la eficacia en el combate a los ilícitos corporativos e incentivar a las empresas para que investigasen sus propios fallos de conformidad.
42. *Cf*. SIEBER, U., *El Derecho Penal Económico en la Era de la Compliance, cit*., p. 82.
43. *Cf. Aktiengesetz*, de 06/09/1965 (BGBl. I S. 1089), modificada por última vez a través la Ley de 07/08/2021 (BGBl. I S. 3311).
44. *Cf. Deutscher Corporate Governance Kodex*, de 26/02/2002, alterado pela última vez em 07/02/2017. El 20/03/2020, fue publicado un nuevo Código de Gobernación Corporativa Alemán, que entró en vigor inmediatamente.
45. *Cf*. SIEBER, U., *El Derecho Penal Económico en la Era de la Compliance, cit*., p. 79.

Código de Comercio (*Handelsgesetzbuch* – HGB)[46] o, eventualmente, como delito de infidelidad con pena de prisión de hasta 5 años o pena de multa en los términos del § 266 StGB)[47]. Pero la falsedad y la infidelidad tienen que ser imputadas a personas físicas[48].

4. Otros: En muchos otros países, se constata la misma transición paulatina desde la autorregulación voluntaria hacia la autorregulación regulada, acompañada tal vez de una mayor capacidad de los reguladores para ajustar su intervención a las características de la cultura empresarial instalada, si el marco jurídico global y sectorial así lo hiciese posible. Por mencionar algunos ejemplos recientes, tomados de las más diversas áreas, podemos considerar las siguientes normas nacionales: la inglesa Ley de la Moderna Esclavitud (*Modern Slavery Act* – MSA), de 2015[49], la francesa Ley Relativa al Deber de Vigilancia (*Loi sur le Devoir de Vigilance* – LDV), de 2017[50], o la a neerlandesa Ley de la Diligencia Debida en Relación con el Trabajo Infantil (*Child Labour Due Diligence Law* – WZK), de 2019[51]. Todas ellas son normas legales que obligan a las empresas, al menos a las de cierta dimensión, a adoptar planes efectivos de conformidad y a divulgarlos públicamente, conminándolas a ello bajo la advertencia de imposición de sanciones. En Portugal, el reciente paquete legislativo anticorrupción 2021/2022 impuso la adopción de programas de cumplimiento que deben incluir planes de prevención de riesgos, códigos de conducta, capacitación, canales de denuncia y designación de un oficial de cumplimiento. Se imponen sanciones administrativas por la no adopción, así como por los esfuerzos de adopción deficientes o incompletos, de programas de cumplimiento efectivo[52].

Algunos países de América Latina siguen la misma tendencia. En Chile, la Ley n.º 20.393, de 25/11/2009[53], establece la responsabilidad penal de las

46. *Cf. Handelsgesetzbuch*, del 10/05/1897, modificada por última vez a través de la Ley de 10/08/2021 (BGBl. I S. 3436).
47. *Cf.* SIEBER, U., *El Derecho Penal Económico en la Era de la Compliance, cit*., p. 80.
48. *Cf.* TIEDEMANN, K., "El derecho comparado en el desarrollo del derecho penal económico", en ARROYO ZAPATERO, L. y NIETO MARTÍN, A. (Dir.), *El Derecho Penal Económico en la Era de la Compliance*, Tirant lo Blanch, Valencia, 2013, (pp. 31-42) pp. 37-38.
49. *Cf. Modern Slavery Act*, del 26/03/2015.
50. *Cf. Loi n.° 2017-399 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre*, del 27/03/2017.
51. *Cf. Wet zorgplicht kinderarbeid*, del 01/05/2019.
52. *Cf. Decreto-Lei n.º 109-E/2021*, del 12/09/2021, *Lei n.º 93/2021*, del 20/12/2021, *Lei n.º 94/2021*, del 21/12/2021 y *Lei n.º 4/2022*, del 01/06/ 2022.
53. *Cf. Ley 20393 (Ley que establece la responsabilidad penal de las personas jurídicas en los delitos que indica)*, del 25/11/2009, modificada por última vez por Ley 21240, del 20/06/2020.

personas jurídicas en delitos de blanqueo de capitales, terrorismo y cohecho entre otros, al mismo tiempo que les concede la exención de responsabilidad para el caso en que hubiesen cumplido sus deberes de dirección y supervisión con anterioridad a la comisión del delito, de acuerdo con un modelo de prevención que incluye la designación de un encargado de prevención. En Perú, la Ley n.º 30.424, de 01/04/2016[54], establece la responsabilidad administrativa de las personas jurídicas por la comisión del delito de cohecho activo transnacional, al mismo tiempo que les concede la exención de responsabilidad siempre que hubiesen adoptado e implementado en su organización, con anterioridad a la comisión del delito, un modelo de prevención adecuado a su naturaleza, riesgos, necesidades y características, consistente en medidas de vigilancia y control idóneas para prevenir el delito de corrupción activa transnacional o para reducir significativamente el riesgo de su comisión, incluyendo la designación de una persona u órgano que ejerza la función de auditoría interna de prevención.

5. Síntesis comparada: Se ha producido una progresiva toma de consciencia sobre el hecho de que los litigios, restricciones regulatorias y daños a la reputación de las empresas, podrían ser evitados si fuesen concebidos y puestos en práctica programas de cumplimiento normativo por parte de las empresas[55]. La adopción de buenas prácticas y sistemas efectivos de control interno es indispensable para que las empresas no sucumban a sus propios fallos y pierdan, al final, la batalla de la competitividad. Los códigos de ética y programas de cumplimiento surgieron por iniciativa de las propias empresas, y en este sentido, se puede hablar de autorregulación voluntaria. Tal tendencia ganó una dimensión generalizada, como se puede colegir de la fijación y certificación privada de patrones universales de gestión de sistemas de cumplimiento normativo voluntario, a través de las Directrices para Sistemas de Gestión del Cumplimiento Normativo (*Compliance Management Systems – Guidelines*), ISO 19600, de 2014, de la Organización Internacional para la Estandardización (*International Organization for Standardization* – ISO)[56]. La

54. *Cf. Ley 30.424 (Ley que regula la responsabilidad administrativa de las personas jurídicas por el delito de cohecho activo transnacional)*, de 01/04/2016.

55. *Cf.* ENGELHART, M., *Sanktionierung von Unternehmen und Compliance – Eine rechtsvergleichende Analyse des Straf– und Ordnungswidrigkeitenrechts in Deutschland und den USA*, 2.ª ed., Duncker & Humblot, Berlin, 2012, pp. 285-289.

56. La ISO, como entidad internacional no gubernamental e independiente, fue fundada en 1946 por delegados de 25 países y congrega actualmente representantes de 165 países, desempeñando un papel de relieve en la fijación y certificación de patrones universales de gestión de sistemas de cumplimiento normativo voluntario, especialmente a través de las Diretrices para los Sistemas de Gestión del Cumplimiento Normativo, actualmente en versión: ISO 37301:2021(en). Online: https://www.iso.org/obp/ui/#iso:std:iso:37301:ed-1:v1:en (consultado el 14/06/2022).

norma ISO 37001, de 2016, tiene objetivos similares, aunque orientados específicamente hacia la prevención de los crímenes de corrupción en el sector privado.

Mientras tanto se produjo, en varios países, una transición paulatina de la autorregulación voluntaria a la autorregulación regulada, acompañada o no de una mayor capacidad de los reguladores y otras autoridades públicas, para adecuar su intervención a las características de la cultura empresarial instalada.

Las medidas de autorregulación regulada o, si se quiere, de regulación compartida estatal y empresarial (incluyendo a las empresas privadas, públicas y semipúblicas) admiten distintos modelos conceptuales, que van desde meras estrategias de estímulo (como la exención de responsabilidad administrativa o penal de la persona jurídica en caso de comprobada implementación de mecanismos de conformidad, con anterioridad a la comisión del delito) hasta la imposición de sanciones, incluso penales, para la simple falta de adopción de medidas efectivas de prevención de delitos de empresa (como la sanción por falta de designación de persona u órgano encargado de la prevención).

La literatura refiere que en la autorregulación regulada pueden coexistir funciones de regulación compartida preventivas y represivas. Dependiendo del reparto de funciones que la autoridad pública y la empresa establezcan recíprocamente, son concebibles varios tipos de autorregulación regulada: la autorregulación delegada (*delegated self-regulation*), en la cual la regulación queda a cargo del Estado y la supervisión y sanción por cuenta de la empresa, o viceversa; la autorregulación transferida (*devolved self regulation*), en la cual el Estado devuelve la regulación, la supervisión y la sanción a la empresa, aunque se reserva la competencia de revisar y fiscalizar periódicamente los programas de conformidad y su aplicación efectiva; finalmente, la autorregulación cooperativa (*cooperative self-regulation*), en la cual el Estado trabaja al mismo tiempo que la empresa y recibe todas las informaciones solicitadas, a fin de incrementar conjuntamente un sistema de prevención individualizado, quedando la empresa sometida a la fiscalización de la autoridad competente[57]. Estas clasificaciones, sin embargo, solo tienen interés si tuviesen adherencia a los respectivos ordenamientos jurídicos concretos. De no ser así, los modelos conceptuales se transformarían en meros ejercicios de estilo. Más vale analizar el derecho comparado, en orden a percibir las tendencias que

57. *Cf.* COCA VILA, I., "Programas de cumplimiento como forma de autorregulación regulada?", en SILVA SÁNCHEZ, J.-M. y FERNÁNDEZ, R. (Dir.), *Criminalidad de Empresa y Compliance – Prevención y Reacciones Corporativas*, Atelier, Barcelona, 2013, (pp. 43-76), pp. 51-52.

tienen verdadera expresión en este campo y llevar a cabo una reflexión crítica sobre las mismas.

En lo sucesivo hablaremos, sobre todo, de los peligros que la regulación responsiva y la autorregulación regulada representan, ya sea para la misión de los reguladores y demás autoridades públicas, ya sea para la salvaguarda de un ambiente económico y social abierto, aunque regulado[58].

III. EL EXCESO DE CONFORMIDAD

La autorregulación regulada impuso un crecimiento exponencial de los departamentos y funciones de conformidad de las empresas, aunque de forma proporcional a la dimensión de cada una de ellas. A lo anterior se une que la autorregulación regulada expandió las propias áreas de prevención de ilícitos de la empresa, comenzando por la prevención del blanqueo de capitales –el área universalmente más regulada en cuanto a la imposición de deberes preventivos, no solo en relación con los bancos, sino con todas las entidades sujetas, financieras y no financieras– y terminando en la prevención de las prácticas restrictivas de la competencia.

Del mismo modo, la autorregulación regulada incitó a los reguladores a realizar inspecciones más frecuentes a las empresas, con miras a conocer los mecanismos de prevención instalados. Pero, al mismo tiempo, las inspecciones pasaron a ser más amigables para mejorar el diseño de los programas de conformidad y los mecanismos de su aplicación práctica. En principio, las inspecciones administrativas no persiguen el descubrimiento de ilícitos, a riesgo de convertirse en búsquedas encubiertas (en manifiesto fraude de ley), sino que persiguen, eso sí, el control del cumplimiento de la ley. Es natural, por tanto, que, en caso de detección de irregularidades o indicios de infracciones, los reguladores deban emitir preferentemente recomendaciones para la adopción de medidas de corrección y perfeccionamiento de los sistemas internos de cumplimiento de las obligaciones legales y reglamentarias de las empresas (aunque no queda necesariamente excluida la posibilidad de que ejerzan sus potestades sancionadoras, dependiendo de las circunstancias de la situación

58. En una visión muy crítica sobre la autorregulación regulada, *Cf.* BUSATO, P. C., "O que não se diz sobre o criminal compliance", en DE SOUSA MENDES, P. *et al.* (Dir.), *Estudos sobre Law Enforcement, Compliance e Direito Penal*, 2.ª ed., Almedina, Coimbra, 2018, pp. 21-55. Igualmente crítico, *Cf.* TAVARES LOBATO, J. D., "Considerações críticas sobre criminal compliance e corrupção", en DE SOUSA MENDES, P. *et al.* (Dir.), *Novos Estudos sobre Law Enforcement, Compliance e Direito Penal*, Almedina, Coimbra, 2020, pp. 25-57.

concreta)[59]. Hay quienes hablan incluso de una Administración simbiótica a propósito de esta casi osmosis entre los reguladores y las empresas[60].

La autorregulación regulada no solo se transformó en un mecanismo dominado por los reguladores, como también se transformó, de hecho, en un mecanismo mimético de la actuación de los propios reguladores, generalmente con la adhesión entusiasta de las propias empresas. Las empresas necesitan contratar empleados dedicados a las funciones de conformidad. Ahora bien, las contrataciones más buscadas tienden a ser las de juristas o abogados con experiencia adquirida en funciones de regulación pública. No es de extrañar que éstos reproduzcan en las empresas el modo de actuación aprendido en sus anteriores funciones de regulación. Este modo de actuar es realmente incentivado en las funciones de conformidad, tanto así que las empresas tienen interés en adiestrarse en los procedimientos de colaboración debida con los reguladores en caso de inspecciones anunciadas o incluso inspecciones sorpresa (*dawn raids*), según el régimen jurídico aplicable. Ante el temor a los riesgos de responsabilidad penal o por infracciones administrativas ligados a los respectivos ramos de negocio, las empresas exigen frecuentemente el máximo de proactividad y realismo en los procedimientos de conformidad, en especial en lo tangente a las investigaciones internas (*internal investigations*). No es de extrañar que los gabinetes de los colaboradores sean invadidos a la búsqueda de documentos, discos duros y e-mails, aprehendiéndose todo lo que pudiese ser exigido, por ejemplo, durante una investigación real de prácticas restrictivas de la competencia. Es frecuente también que tales diligencias lleven a la incoación de procedimientos disciplinarios y a la imposición de sanciones a directivos y trabajadores. Estos ejercicios de dramatización sirven, ciertamente, para que las empresas aleguen y prueben la implantación de robustos sistemas de cumplimiento normativo, si tuviesen que enfrentarse a procedimientos sancionadores[61].

La existencia de programas de clemencia (*leniency programmes*) que ofrecen inmunidad o reducción de las sanciones pecuniarias a las empresas que se autodenuncien, al mismo tiempo que denuncian a las otras involucradas en prácticas de cártel, es otro contexto que ha favorecido que las empresas lleven a cabo investigaciones internas agresivas. Los

59. *Cf.* DE SOUSA MENDES, P., "Die Finanzmarktaufsicht und der Transfer von Informationen aus dem Verwaltungsverfahren in das Strafverfahren", *GA*, núm. 6, 2016, (pp. 380-392) p. 383, n. 24.

60. *Cf.* HERMES, G., "Staat und Markt", en KEMPF, E., LÜDERSSEN, K. y Volk, K. (Dir.), *Die Finanzkrise, das Wirtschaftsstrafrecht und die Moral*, de Gruyter, Berlin / New York, 2010, (pp. 26-46) pp. 38-39.

61. *Cf.* HAUGH, T., *The Cambridge Handbook of Compliance, cit*., pp. 138-140.

programas de clemencia persiguen desestabilizar los pactos de silencio, ofreciendo incentivos a las empresas del cártel para que colaboren con las autoridades. En los últimos veinticinco años fueron creados programas de clemencia en más de ochenta países[62]. Desde 1996, la Comisión Europea ha promovido un programa de clemencia en la lucha contra los cárteles. Desde el punto de vista de la Dirección General de la Competencia (DG Comp) de la Comisión Europea y de las Autoridades Nacionales de la Competencia (ANC), la principal ventaja de un programa de clemencia es la reducción de la complejidad, la demora y los costes de la instrucción y obtención de pruebas en prácticas de cártel. Desde el punto de vista de las empresas, la inmunidad que es concedida a la primera solicitante de clemencia y la reducción de las sanciones pecuniarias concedidas a las siguientes, pueden constituir un incentivo suficiente para la autodenuncia y la colaboración, aunque solo sea por el recelo a que las otras empresas del cártel puedan ofrecer informaciones y medios de prueba. A la vista de esto, se entiende que los programas de clemencia hayan contribuido al incremento de la conformidad en las empresas[63].

Todo esto puede afianzar las funciones de conformidad como una *longa manus* de los reguladores y demás autoridades públicas o como un instrumento de transferencia de culpas de las empresas a sus propios colaboradores, intentando así transformar los delitos de empresa en delitos de los colaboradores contra la empresa. Ambos escenarios, que no son necesariamente alternativos, son –en nuestra opinión– contraproducentes para la consecución del cumplimiento normativo.

En cuanto al primero de los escenarios cabe, desde luego, señalar que la conformidad, incluso cuando es impuesta, no es una finalidad en sí misma, sino más bien una limitación a las finalidades de la empresa. La empresa, como organización de medios humanos, técnicos y financieros, opera para satisfacer los intereses de sus múltiples beneficiarios, desde los dueños del negocio o accionistas (a través de la realización del lucro que remunera el riesgo asumido), pasando por sus colaboradores (a través del empleo y del salario) y clientes (a través de la oferta de bienes o servicios), hasta los acreedores (a través del reembolso del capital y sus respectivos intereses) y los proveedores (a través de la búsqueda de bienes no servicios). No está de más incluir al Estado entre los beneficiarios (a través del cumplimiento da las obligaciones fiscales). En el sentido más amplio del concepto de beneficiario, aún se podría decir, en buena lógica, que la autorregulación transformada en obligación legal, correspondería incluso

62. *Cf.* WILS, W., "The Use of Leniency in EU Cartel Enforcement: An Assessment after Twenty Years", *World Competition*, núm. 3, 2016, pp. 327-388.

63. *Cf*. HAUGH, T., *The Cambridge Handbook of Compliance, cit*., pp. 138-140.

a una operación de la empresa para satisfacer el interés de la comunidad jurídica (a través de su contribución a la economía competitiva y regulada). Pero sería un paso de gigante deducir de ahí que la empresa se convertiría en una *longa manus* de los reguladores y otras autoridades públicas, ejecutando órdenes o directivas, en vez de colaborar con dichas entidades públicas, bajo el cumplimiento de deberes de colaboración (*Mitwirkungspflichten*)[64]. Esta distinción puede parecer solo un matiz, pero es, al final, una diferencia esencial de perspectiva al respecto de la autorregulación regulada. Nótese que fueron las divergencias sobre esta aparente diferencia de matiz las que provocaron el reciente fracaso de la VerSanG, en Alemania. En especial, el régimen propuesto para las investigaciones internas fue la piedra angular de la discordia entre los partidos de la coalición de gobierno. La proposición de ley preveía una separación total entre los investigadores internos y los abogados de empresa, lo que significaba que los resultados de las investigaciones internas no quedarían resguardados por la prohibición de aprehensión (*Beschlagnahmeverbot*) establecida por el § 97 StPO y podrían, así, ser utilizados por los reguladores y la Fiscalía para la instauración y la instrucción de procedimientos sancionadores públicos (administrativos y penales)[65]. No fue considerado admisible –afortunadamente, en nuestra opinión– este elevado grado de intrusión, como si no existiesen barreras de ningún tipo a los poderes de las autoridades públicas frente a las empresas.

En cuanto al segundo de los escenarios, la conformidad como instrumento de transferencia de culpabilidad de la empresa a sus colaboradores, acompañada de investigaciones internas que violan sus derechos[66],

64. Sobre los deberes de colaboración, BÖSE, M., *Wirtschaftsaufsicht und Strafverfolgung – Die verfahrensübergreifenden Verwendung von Informationen und die Grund– und Verfahrensrechte des Einzelnen*, Mohr Siebeck, Tübingen, 2005, p. 5. Igualmente, *Cf*. WOHLERS, W., "Selbstregulierung – Aufsichtsrecht – Strafrecht: (Ziel–)Konflikte und Interdependenzen", en ACKERMANN, J.-B. y WOHLERS, W. (Dir.), *Finanzmarkt ausser Kontrolle? Selbstregulierung – Aufsichtsrecht – Strafrecht: 3. Zürcher Tagung zum Wirtschaftsstrafrecht*, Schulthess, Zürich / Basel / Genf, 2009, (pp. 267-314) p. 285.

65. Online: https://www.noerr.com/en/newsroom/news/corporate-sanctions-act-dropped (consultado el 14/06/2022).

66. *Cf.* ARLEN, J. y BUELL, S. W., "The Law of Corporate Investigations and the Global Expansion of Corporate Criminal Enforcement", *Southern California Law Review*, núm. 93, 2020, (pp. 697-762) pp. 719-720. Igualmente, *Cf.* REEB, P., *Internal Investigations – Neue Tendenzen privater Ermittlungen*, Duncker & Humblot, Berlin, 2011, pp. 95-108. También *Cf.* ANTUNES, M. J., "Privatização das investigações e compliance criminal", *Revista Portuguesa de Ciência Criminal*, núm. 1, 2018, (pp. 119-127) p. 124. Finalmente, *Cf.* LEITE FILHO, José Raimundo, *Corrupção Internacional, Criminal Compliance e Investigações Internas – Limites à Produção e Valoração dos Interrogatórios Privados*, Lumen Juris, Rio de Janeiro, 2018, pp. 153-156.

solo puede –como es fácil de entender– contribuir a la creación de una cultura de escapismo y fingimiento por parte de los colaboradores, en vez de estimular el compromiso con las buenas prácticas, la asunción de los propios errores y la voluntad colectiva de corregirlos. A fin de cuentas, en vez de una verdadera cultura de conformidad, se abre la puerta a la creación de una cultura soterrada de disimulación de los delitos de empresa.

IV. EL OFICIAL DE CUMPLIMIENTO COMO PARARRAYOS DE LA EMPRESA

No hay mejor ejemplo del riesgo de transferencia de culpa de la empresa a sus colaboradores que la discusión en torno a la responsabilidad administrativa y penal del director del departamento de cumplimiento (*Head of Compliance* o *Chief Compliance Officer*).

En este contexto, son frecuentemente citados varios casos emblemáticos de derecho comparado. En los Estados Unidos de América, se refiere, por ejemplo, el caso de Peter Madoff, director ejecutivo y director de conformidad de la sociedad Bernard L. Madoff Investment Securities (BLMIS), que fue condenado, en 2012, a 10 años de prisión por la práctica de varios crímenes, principalmente fraudes mediante falsificación de libros y registros de la empresa de consultoría de inversión en activos de su hermano Bernie Madoff[67]. En Alemania, se menciona la sentencia de la 5.ª Sección Penal del Supremo Tribunal Federal (*Bundesgerichtshof* – BGH), que declaró, en *obiter dictum*, que un oficial de cumplimiento tiene, por regla general, un deber de garante jurídico-penal, en los términos del § 13 Abs. 1 StGB (comisión por omisión), que lo obliga a evitar los delitos de los trabajadores de la empresa relacionados con la actividad empresarial (BGH 5 StR 394/08, 17/07/2009). En realidad, el BGH dictaminó la responsabilidad penal por comisión por omisión de un director del departamento interno de revisión de una empresa pública, cuya función era equiparada a la del responsable de un sector de conformidad[68].

En la generalidad de las órdenes jurídicas nacionales, falta una regulación detallada y legalmente vinculante de las funciones del oficial de cumplimiento. Siendo así, la delimitación de su competencia en el ámbito de la empresa constituye el único fundamento de su posición de garante, con base en la cual se pueda imputar después una eventual

67. Online: https://www.nbcnews.com/business/peter-madoff-sentenced-10-years-role-ponzi-scheme-1C7660243 (consultado el 14/06/2022).
68. Online: https://dejure.org/dienste/vernetzung/rechtsprechung?Text=5%20StR%20394/08 (consultado el 14/06/2022).

responsabilidad penal por comisión por omisión. Para fundamentar una posición de garante del oficial de cumplimiento, es necesario partir de la posición de garante de los órganos de gobierno de la sociedad comercial (en especial, el órgano de administración). La doctrina dominante ha atribuido a la administración una posición de garante que la obliga a evitar la práctica de delitos de empresa[69]. La posición de garante del oficial de cumplimiento corresponde a un deber derivado y no originario. El deber de conocimiento originario del órgano de administración (o del administrador con las competencias en conformidad) es complementado por el deber de reportar del oficial de cumplimiento, al mismo tiempo que el deber de fiscalización originario del órgano de administración es complementado por un deber de vigilancia derivado del oficial de cumplimiento[70]. La designación de un oficial de cumplimiento a través de una suficiente *diligentia in delegando* no exonera, no obstante, al órgano de administración (o de sus miembros), pues el deber originario permanece en el órgano de liderazgo[71]. Es importante, pues, impedir que haya una descarga total de responsabilidades en el oficial de cumplimiento, ya sea por parte de las empresas (cuando exista responsabilidad penal de las personas jurídicas), ya sea por parte de los directivos de las empresas (en cualquiera de los casos), como si el oficial de cumplimiento fuese el pararrayos de todos los fallos de la empresa y fuese remunerado para eso[72].

La posibilidad de atribución de responsabilidad penal no debe hacer olvidar que los oficiales de cumplimiento no forman parte de la estructura operativa de las empresas y que, por eso mismo, dependen de la información que les es transmitida por los departamentos operativos. Su capacidad de interferencia en las operaciones de las empresas es indirecta y depende en gran medida de la confianza que les sea otorgada por todos los colaboradores. Por su parte, tal confianza solo se mantendrá incólume

69. *Cf*. KONU, M., *Die Garantenstellung des Compliance-Officers – Zugleich ein Beitrag zu den Rahmenbedingungen einer Compliance-Organisation*, Duncker & Humblot, Berlin, 2014, pp. 91-143. Igualmente, Cf. DEMETRIO CRESPO, E., "Sobre la posición de garante del empresario por la no evitación de delitos cometidos por sus empleados", en SERRANO-PIEDECASAS, J. R. y DEMETRIO CRESPO, E. (Dir.), *Cuestiones Actuales de Derecho Penal Económico*, COLEX, Madrid, 2008, (pp. 61-87) p. 64.

70. *Cf*. SCANDELARI, G. B., "As posições de garante na empresa e o *criminal compliance* no Brasil: Primeira abordagem", en DAVID, D. F. (Dir.), *Compliance e Direito Penal*, Atlas, São Paulo, 2015, (pp. 158-199) pp. 174-176.

71. *Cf*. CARRIÓN ZENTENO, A. y URQUIZO VIDELA, G., "La responsabilidad penal del oficial de cumplimiento en el ámbito empresarial: Un breve análisis comparativo entre Alemania-Perú y *EEUU*", en AMBOS, K., CARO CORIA, D. C. y MALARINO, E. (Dir.), *Lavado de Activos y Compliance – Perspectiva Internacional y Derecho Comparado*, Jurista Editores, Lima, 2015, (pp. 371-401) p. 383.

72. *Cf*. SCANDELARI, G. B., *Compliance e Direito Penal*, *cit*., p. 191.

si los oficiales de cumplimiento no son vistos como elementos extraños al ambiente empresarial, sino como agentes de las buenas prácticas. De ahí se debería derivar que reportasen internamente (al órgano de administración) las anomalías y fallos de conformidad, a fin de que sean corregidas, pudiendo esto implicar, según los casos, la imposición de sanciones internas a los colaboradores que las cometieron. Por eso, sorprende que algunos ordenamientos jurídicos nacionales impongan a los oficiales de cumplimiento deberes de denuncia a las autoridades públicas competentes de los ilícitos que ellos mismos detecten en las empresas. Aquello que se pueda ganar con la denuncia de un solo ilícito ante la Justicia, de nada valdría frente a todo el capital de confianza derrochado en un instante, comprometiéndose así, para el futuro, el éxito de las funciones de conformidad.

Pero aún más sorprende que haya ordenamientos jurídicos nacionales, aunque pocos, que criminalicen la omisión de comunicación de operaciones y transacciones sospechosas específicamente por parte del oficial de cumplimiento[73], tal y como está previsto y punido por el artículo 5.º do DL No. 1106 peruano[74].

Sea como fuere, la omisión de comunicación a las autoridades competentes (por parte de los oficiales de cumplimiento) de operaciones y transacciones sospechosas ha ido configurándose como categoría de ilícito administrativo en muchos ordenamientos jurídicos nacionales, de hecho integrada en el rol de deberes preventivos del blanqueo de capitales cuyo incumplimiento es sancionado directamente por los reguladores financieros. Es, por tanto, muy dudoso que este tipo de ilícito administrativo contribuya a la eficacia de las funciones de conformidad. Por el contrario, produce un efecto de aislamiento de los oficiales de cumplimiento de los restantes colaboradores.

V. LA CARGA DE LA PRUEBA DE LA CONFORMIDAD EMPRESARIAL

En principio, la posición de los reguladores y demás autoridades públicas frente a los programas de conformidad en las empresas debe ser neutral. No deben ser extraídas conclusiones inmediatas sobre la existencia

73. *Cf.* REYNA ALFARO, L. M., "La responsabilidad penal del *compliance officer*: Algunas consideraciones iniciales sobre el nuevo delito de omisión culposa de comunicación de operaciones sospechosas", *ADPE*, núm. 3, 2015, (pp. 273-287) p. 277.

74. *Cf.* DL 1106, publicado em 19 de abril de 2012, in: *Diario Oficial "El Peruano"*, que modifica la disciplina prevista por la Ley Penal contra el blanqueo de capitales (*Ley Penal contra el lavado de activos* – LPLA), o sea, la *Ley No.* 27765.

de tales programas para eximir a las empresas o al menos mitigar las sanciones o cualesquiera otras consecuencias jurídicas[75]. Tomado en serio, el cumplimiento normativo tiene que perseguir la prevención de varios tipos de ilícitos, incluyendo los ilícitos penales (*e.g.*, delitos ambientales, delitos contra los consumidores, delitos fiscales, corrupción activa y blanqueo de capitales), en vez de apostar primordialmente en la exención de responsabilidades empresariales o en la atenuación de sanciones. En caso contrario, los programas de conformidad se vuelven meras estratagemas de encubrimiento de las malas prácticas de las empresas. Como cautela ante tales estratagemas, el legislador y los reguladores no deberían consagrar regímenes de responsabilidad empresarial que reconociesen efectos premiales automáticos ante la existencia de programas de conformidad, por lo menos hasta cerciorarse de si son realmente tomados en serio en la práctica.

En los Estados Unidos de América, la evaluación de la efectividad del programa de conformidad obedece a una lista exigente y bastante estructurada de requisitos, de acuerdo con lo que fue establecido por la Comisión Sentenciadora (*Sentencing Commission*), a saber:

(1) Patrones y procedimientos para prevenir y detectar la conducta ilícita;

(2) Responsabilidad en todos los niveles del programa, junto con recursos adecuados y empoderamiento del personal directivo;

(3) Diligencia debida en la contratación y asignación de los recursos humanos para cargos con empoderamiento sustancial;

(4) Patrones y procedimientos de comunicación, incluyendo un requisito específico para el adiestramiento a todos los niveles;

(5) Monitorización, auditoría y sistemas de orientación y reporte internos no sancionadores, incluyendo la evaluación periódica de la efectividad del programa;

(6) Promoción y aplicación de la conformidad y conducta ética; y

(7) Adopción de medidas razonables para responder de forma adecuada y prevenir futuras malas conductas al detectar una violación.

La verificación en la práctica de todos los puntos relacionados en la lista anterior no es una cuestión trivial, pero lo que verdaderamente importa es que el estabelecimiento de tales requisitos originó un recrudecimiento

75. *Cf.* ROTSCH, T., "Compliance und Strafrecht – Fragen, Bedeutung, Perspektiven Vorbemerkungen zu einer Theorie der sog. 'Criminal Compliance' ", *ZStW*, núm. 3, 2013, (pp. 481-498) pp. 483-484.

masivo de la conformidad porque las empresas pasaron a tener una noción clara (o por lo menos más clara) sobre lo que podrían hacer para mitigar su responsabilidad. En vez de conformidad enfocada a un determinado sector o reglamentación, ahora hay un instrumento para disminuir la culpabilidad por cualquier delito corporativo en potencia[76].

En Alemania, la sentencia de la 1.ª Sección Penal del Supremo Tribunal Federal (BGH 1 StR 265/16, de 09.05.2017) decidió que la conformidad podría llevar a una reducción de la multa (*Geldbuße*) aplicada a una sociedad mercantil, en sede de responsabilidad administrativa (*Verantwortlichkeit für Ordnungswidrigkeiten*), aunque no existan leyes o reglamentos estrictos en ese sentido, pues las empresas están obligadas a implementar un sistema de conformidad capaz de evitar la conducta impropia o incluso ilícita por parte de sus colaboradores[77]. El BGH estableció dos criterios relevantes para la determinación del valor de la multa: (i) saber si existía un sistema de conformidad efectivo y adecuado a la prevención de los riesgos de la práctica de la infracción en causa; (ii) saber si la administración societaria reaccionó con prontitud, identificó las lagunas de conformidad y las corrigió inmediatamente en el sistema para prevenir infracciones similares en el futuro[78].

Dicho esto, importa ahora saber quién tiene la carga de alegar y producir prueba en el procedimiento sancionador sobre la verificación en la práctica de los requisitos mencionados.

En los sistemas jurídicos anglosajones (*common law*), cuya matriz de proceso penal es antagonista (*adversarial*), es aceptada la existencia de diversos tipos de carga de la prueba, entre las cuales destacan las siguientes: (i) la carga de la alegación (*burden of pleading*); (ii) la carga de la producción de medios de prueba (*burden of production* o *evidential burden*); (iii) la carga de la persuasión (*burden of persuasion*) y (iv) la carga táctica (*tactical burden of proof*).

La defensa por impugnación y la defensa por excepción no son diferentes, en tanto en cuanto, ambas se dirigen a saber a quién cabe la iniciativa de producir medios de prueba con miras a introducir la cuestión planteada en la instrucción del proceso penal. Una defensa negativa

76. *Cf*. HAUGH, T., *The Cambridge Handbook of Compliance, cit*., pp. 136-137.

77. *Cf.* BGH 1 StR 265/16, del 09/05/2017, p. 456.

78. *Cf*. NIENABER, L. C., *Umfang, Grenzen und Verwertbarkeit compliance basierter unternehmensinterner Ermittlungen*, Nomos, Baden-Baden, 2019, p. 42. También *Cf*. ABENDROTH, C., *Prolegomena einer strafrechtlichen Bewertung von Corporate Governance, Compliance und Business Ethics – Eine Untersuchung unter Berücksichtigung der Besonderheiten der Kreditwirtschaft*, WVB, Berlin, 2011, pp. 140-142.

impugna uno o más de los elementos del caso de la acusación (por ejemplo, defensa de coartada). Una defensa afirmativa va más allá de una simple negación de los hechos en la medida en que proporciona hechos adicionales que evitan las consecuencias jurídicas buscadas por la acusación (por ejemplo, legítima defensa, estado de necesidad, coacción moral, error de prohibición, intoxicación y trastorno mental). En caso de defensa negativa, corresponde al acusado alegar y aportar pruebas para sustentar la negación de uno o más elementos del delito. Sin embargo, esta carga del acusado de alegar y producir evidencia que acredite una coartada no significa que la Fiscalía no tenga que soportar la carga final de persuadir al investigador de hechos (juez o jurado) de la culpabilidad del acusado para ganar el caso. El riesgo de condena explica por qué a la defensa le conviene hacer algo más que reclamar justicia y, por lo tanto, también tendrá sentido hablar de una carga táctica de la prueba sobre los hombros del acusado, dados los giros y vueltas del caso. Con respecto a la defensa afirmativa, los distintos tipos de carga de la prueba no se distribuyen de manera diferente.

Todavía no hay ideas claras o procedimientos establecidos sobre cómo montar una defensa eficaz en un caso de cumplimiento normativo. La discusión de las cargas de prueba podría agudizar el punto de que, dado que la ocasión del caso es una falta de cumplimiento, tiene sentido que la persona jurídica demuestre que el programa de cumplimiento fue efectivo a pesar del incumplimiento (a menos que la ocasión del caso sea simplemente sobre si hubo un programa de cumplimiento o no). ¿Debe la acusación probar la ausencia de un programa de cumplimiento efectivo o la persona jurídica en cuestión necesita probar su efectividad incluso si la acusación tiene, por alguna razón, la carga de investigar tales programas? En términos prácticos, sería muy difícil para un fiscal probar la total ineficacia de un programa dado que toda la información clave está en el dominio de la empresa y solo ella conocerá todos los detalles de las fallas. Como tal, se podría argumentar que una persona jurídica entonces solo necesita negar el cargo o hacer una defensa afirmativa, es decir, ¿presentar evidencia de la efectividad del programa? Sin embargo, esto conlleva el riesgo de que el programa quede expuesto a las críticas de la Fiscalía por sus deficiencias y, en última instancia, la persona jurídica pueda revelar más hechos de los que se investigaron originalmente. En cualquier caso, parece justo que una persona jurídica en esta situación tenga que asumir ese riesgo si quiere afirmar la defensa del cumplimiento.

A ello se suma la evidencia de que la medida de la prueba es diferente para los elementos constitutivos del delito, de la medida de la prueba de la concurrencia de circunstancias eximentes de la pena. El Tribunal

Supremo de los Estados Unidos (*United States Supreme Court* – SCOTUS), imponiendo que todos los hechos necesarios para la configuración del delito tengan que ser probados por la acusación más allá de toda duda razonable (*beyond any reasonable doubt* – BARD)[79], aún así considera que los hechos que integran las defensas afirmativas tienen que ser probados por la defensa, según la regla de la prueba preponderante (*preponderance of the evidence*), que termina siendo más exigente para la defensa porque no desencadena el requisito constitucional de refutación (por parte de la acusación) más allá de una duda razonable[80]. De hecho, al clasificar la efectividad de un programa de cumplimiento como una defensa afirmativa, se aplicaría el estándar de la prueba preponderante. Sin embargo, esto todavía constituye una carga alta y explica por qué las personas jurídicas tengan que reunir los máximos elementos posibles para probar el cumplimiento de los requisitos establecidos por la Comisión Sentenciadora. En este escenario, es la defensa la que tiene que alegar y producir la prueba sobre la efectividad de un programa de cumplimiento y no la acusación.

En los sistemas jurídicos romano-germánicos (*civil law*), cuya matriz del proceso penal es de estructura acusatoria, e integrada por un principio de investigación (principio inquisitorio)[81], la perspectiva de la literatura más clásica sobre la carga de la prueba es muy diversa. En lo que atinente a la carga de la prueba, la doctrina alemana de finales del siglo XIX solía distinguir entre la carga de introducir prueba en el juicio y el riesgo de no persuasión[82]. A lo primero la doctrina lo llamaba carga de la prueba

79. A partir de la regla establecida en el precedente *In re Winship*, 397 U.S. 358, 1970.

80. Por ejemplo, en el caso *Dixon vs. US*, 548US___(2006), la acusada Keshia Dixon alegó haber actuado bajo coacción moral (*duress*), pero el Tribunal de Distrito (*District Court*), en *Dixon*, 126 S. Ct. At 2440, consideró no probada tal coacción moral por la medida de la prueba de la probabilidad preponderante, lo que fue confirmado por el Tribunal de Apelación (*Court of Appeals*), en vía de recurso ordinario, en *United States vs. Dixon*, 413 F.3d 520, 522, United States Court of Appeals, Fifth Circuit (2005),y por la propia Corte Suprema (*U. S. Supreme Court*), en vía de recurso extraordinario para la fijación de jurisprudencia (*Writ of Certiorari*). *Cf. Supreme Court of the United States: Keshia Cherie Ashford Dixon, petitioner v. United States – On writ of certiorari to the United States Court of Appeals for the Fifth Circuit*. Online: https://www.supremecourt.gov/opinions/05pdf/05-7053.pdf (consultado el 14/06/2022). También *Cf.* KAMISAR, Y., LaFAVE, W. R., ISRAEL, J. H. y KING, N. J., *Modern Criminal Procedure – Cases-Comments-Questions*, 10.ª ed., West Group, St. Paul, MN, 2003 (1.ª ed., 1965), pp. 1511-1517.

81. Otras denominaciones frecuentemente utilizadas para designar al principio inquisitorio (*Aufklärungsgrundsatz*) son principio de la instrucción (*Instruktionsmaxime*) o principio de la investigación (*Untersuchungsgrundsatz*).

82. *Cf.* FLETCHER, G. P., "Two Kinds of Legal Rules: A Comparative Study of Burden-of-Persuasion Practices in Criminal Cases", *The Yale Law Journal*, núm. 5, 1968, (pp. 880-935) p. 904, n. 82.

formal (*formelle Beweislast*)[83] y a lo segundo carga de la prueba material (*materielle Beweislast*)[84]. En el proceso penal no existiría la carga de la prueba formal o fáctica, ya fuese porque el promotor tenía que colaborar con el tribunal en el descubrimiento de la verdad y en la realización de la justicia, tanto produciendo pruebas incriminatorias como exculpatorias (*à charge et à décharge*), ya fuese porque el juez de la causa (*Tatrichter*) tenía poderes-deberes autónomos de investigación (*Aufklärungspflichten*), ordenando así, de oficio, la producción de todos los medios de prueba cuyo conocimiento considerase necesario para el descubrimiento de la verdad y la buena decisión de la causa[85]. Esta posición se consolidó en la doctrina hasta tal punto que actualmente ya ni siquiera se encuentran referencias a la carga de la prueba en los tratados y manuales alemanes consagrados de derecho procesal penal[86]. A ello se une que la estructura tripartita de la responsabilidad penal fijada por la clásica monografía de Ernst Beling (1866-1932), *La Teoría del Delito* (*Die Lehre vom Verbrechen*)[87], especialmente en lo que respecta a la tipicidad, la ilicitud y la culpabilidad (*Tatbestand*, *Rechtswidrigkeit* y *Schuld*), proporciona un esquema para organizar todas las cuestiones sustantivas relacionadas con la culpabilidad o inocencia del imputado. Al formular una serie de tres preguntas: –¿El imputado causó un resultado prohibido por el legislador?– ¿El hecho causa repulsa social (es injustificado)? –¿El imputado es personalmente culpable (es indisculpable)?– el juez del caso alemán progresa a través de una ordenación amplia y unificada de las cuestiones atinentes a la atribución de responsabilidad penal al imputado. Y la conclusión de la culpabilidad requiere una constatación afirmativa de estas tres categorías de la indagación judicial. Las tres categorías tienen un peso equivalente en la carga del Estado, consistente en establecer la punibilidad del imputado y, por eso mismo, el fiscal alemán es quien soporta el riesgo de duda residual del juez del caso sobre las cuestiones sustantivas de las tres categorías[88]. Esta perspectiva de la literatura clásica no puede dejar de traer consecuencias para la prueba de la conformidad efectiva en la determinación de la responsabilidad empresarial, ya sea encarando la conformidad efectiva como

83. *Cf.* GLASER, J., *Beiträge zur Lehre vom Beweis im Strafprozess*, Duncker & Humblot, Leipzig, 1883, pp. 99-103.
84. *Cf.* GLASER, *Beiträge zur Lehre vom Beweis im Strafprozess, cit*., pp. 85-98.
85. *Cf.* GLASER, *Beiträge zur Lehre vom Beweis im Strafprozess, cit*., pp. 100.
86. *Cf.* ROXIN, C. y SCHÜNEMANN, B., *Strafverfahrensrecht – Ein Studienbuch*, 30.ª ed., Beck, München, 2022 (1.ª ed., 1949), pp. 412-413 (§ 45., n.os ms. 2-4). La doctrina portuguesa más clásica siguió la misma tendencia. Por todos, *Cf.* DE FIGUEIREDO DIAS, J., "Anotação – Ónus de alegar e provar em processo penal?", *Revista de Legislação e Jurisprudência*, núm. 105, 1972, (pp. 125-128 y 139-143) pp. 139-140.
87. *Cf.* BELING, E., *Die Lehre vom Verbrechen*, J. C. B. Mohr (Paul Siebeck), Tübingen, 1906.
88. *Cf*. FLETCHER, G. P., *The Yale Law Journal*, núm. 5, 1968, *cit*., pp. 913-915.

elemento negativo del tipo delictivo, o ya sea vista más bien como una eximente en el plano de la ilicitud o incluso de la culpabilidad.

Esta línea de pensamiento es seguida en otros países europeos continentales, lo que nos permite aplicarla a aquellos ordenamientos jurídicos que admiten la responsabilidad penal de las personas jurídicas, como es el caso, a título de ejemplo, de España. Con la reforma de 2010 del Código Penal español[89], fue impuesta a las personas jurídicas la obligación de contar con un modelo de prevención de riesgos penales, aunque no fue hasta la reforma de 2015 del Código Penal[90] cuando realmente se desarrolló la forma en que esta obligación debe ser implementada y se decretó la exención de la responsabilidad de la persona jurídica en caso de correcta implementación. El actual n.º 2 del artículo 31 bis del Código Penal decreta que la persona jurídica quedará exenta de responsabilidad si cumple un conjunto especificado de requisitos, los cuales están claramente inspirados en los que estableció la Comisión Sentenciadora norte-americana. El punto crítico aquí es la cuestión de saber a quién incumbe alegar y reunir pruebas del cumplimiento, total o parcial, de tales requisitos. No habiendo una distribución de la carga de la prueba, la conclusión lógica debería ser que el fiscal español es quien soporta el riesgo de la duda residual del juez del caso sobre el incumplimiento, total o parcial, de los requisitos de la conformidad efectiva en la determinación de la responsabilidad empresarial. Si así fuese, la omisión de los defectos de conformidad en el escrito de acusación a cargo de la Fiscalía acabaría por hacer operar una presunción judicial de conformidad en la decisión del juez del caso[91]. A esto se une que los fallos y defectos concretos de conformidad que, eventualmente, sean atribuidos a las personas jurídicas en el escrito de acusación, tienen que generar una convicción próxima a la certeza en el juez del caso sobre su verificación, lo que significa, al mismo tiempo, que las personas jurídicas investigadas tendrán solo que suscitar una duda razonable en relación con las pruebas reunidas por la acusación para conseguir sacar partido de la presunción judicial de conformidad.

89. *Cf.* Nuevo Código Penal español (reformado por Lei Orgânica 5/2010), en vigor desde el 24/12/2010.

90. *Cf.* Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, del 23 de noviembre, del Código Penal.

91. Las presunciones judiciales (*praesumptio judicis*), simples, naturales, de hombre, de hecho o de experiencia (por todas estas denominaciones se hicieron conocidas) son aquellas que no están establecidas en la ley, pero se basan exclusivamente en la experiencia de vida o, si se prefiere, en las llamadas reglas de la experiencia (*Erfahrungssätze*). Sobre las reglas de la experiencia, *Cf.* AROSO LINHARES, J. M., "Regras de experiência e liberdade objetiva do juízo de prova", *Boletim da Faculdade de Direito de Coimbra*, núm. XXXI, 1988, (pp. 1-364) p. 14.

En nuestra opinión, lo anterior supone un esfuerzo absurdo de recogida de pruebas a cargo de la acusación, que, además, se aproxima a una prueba negativa o diabólica (*probatio diabolica*) precisamente en aquellos casos en los que las personas jurídicas no alegan nada en su defensa, o sea, los casos en que las empresas probablemente no practican ningún tipo de conformidad. En estas circunstancias, la autorregulación regulada acabaría por provocar el resultado opuesto al pretendido. O sea, la autorregulación regulada, así interpretada, haría más difícil de fundamentar y probar la responsabilidad de la persona jurídica.

Pero esto no tiene por qué ser así. Hay ordenamientos jurídicos inspirados en el modelo europeo continental que contienen una regla de distribución de la carga de la prueba en el proceso penal equiparable, salvo en los poderes subsidiarios de investigación del juez del caso, a la del modelo antagonista norte-americano, como es el caso de Brasil. En el artículo 156 del Código del Proceso Penal brasileño[92] se dispone que: "La prueba de la alegación incumbirá a quien la hiciere estando, no obstante, facultado el juez de oficio: […] determinar, en el transcurso de la instrucción, o antes de dictar sentencia, la realización de diligencias para dirimir dudas sobre puntos relevantes"[93]. Esta regla permite la interpretación de que la alegación de la prueba de la conformidad efectiva corresponderá a la empresa, especialmente en el único caso en que el legislador brasileño admite la atribución de responsabilidad penal a las personas jurídicas, o sea, en los términos del artículo 3.º de la Ley de Delitos Ambientales[94].

Ni si quiera es necesario que exista una regla para la distribución de la carga de la prueba en el proceso penal para llegar a la misma conclusión. Si preferimos una teoría procesal del delito, inspirada en la retórica antagonista, en vez de la teoría meramente sustantiva del delito de Beling, inspirada en el principio inquisitorio, entonces se hace posible una distribución eficiente y eficaz de la carga de la prueba entre las partes procesales. Citando al filósofo portugués Fernando Gil (1937-2006): "[…] el proceso es una argumentación racional contradictoria, que se inspiró en los procedimientos retóricos de la prueba y que, al mismo tiempo, los marcó también. La teoría […] del *onus probandi* interviene también en toda la controversia […]. Finalmente, el proceso se articula con el establecimiento y la evaluación neutra, imparcial, del hecho, que también representa una exigencia epistemológica fundamental […]"[95].

92. *Cf. Decreto-Lei n.º 3.689*, del 3 de octubre de 1941.
93. Incluido por *Lei n.º 11.690*, de 2008.
94. *Cf. Lei n.º 9.605*, del 12 de febrero de 1998.
95. GIL, F., *Provas*, Lisboa: INCM, 1986, pp. 35-36.

El derecho norte-americano ha producido un análisis asaz sofisticado de los distintos tipos de carga de la prueba que debería servir –y está sirviendo de forma creciente– como referencia también para los sistemas jurídicos romano-germánicos[96].

Todo ello visto y ponderado, los programas, los mecanismos y las medidas de conformidad podrán, en la práctica, tener impacto en la evaluación de la responsabilidad empresarial y en la determinación de las sanciones aplicables[97].

VI. UN NUEVO DERECHO REGULADOR

La contraposición clásica entre el derecho administrativo y el derecho penal es una disyuntiva superada en la regulación de las actividades económicas, así como en el derecho de la competencia. Asistimos al surgimiento de una nueva rama del Derecho, que aglutina aspectos del derecho administrativo, de derecho sancionador público, e incluso penal.

La aparición de las autoridades independientes subvirtió el clásico modelo de separación de poderes, por eso mismo fueron dotadas de tres tipos de poderes públicos, tradicionalmente separados, a saber: poderes normativos, ejecutivos y (para) judiciales. Las modernas autoridades independientes dictan reglamentos de carácter general y abstracto, acompañan e inspeccionan la actividad de las empresas y, por fin, aplican sanciones pecuniarias y sanciones accesorias, si detectan infracciones. A este respecto es, pues, difícil sostener la contraposición clásica entre el derecho administrativo y el derecho penal, más si tenemos en cuenta que el

96. *Cf.* PRAKKEN, H. y SARTOR, G., "A logical analysis of burdens of proof", in: KAPTEIN, H., PRAKKEN, H. y VERHEIJ, B. (Dir.), *Legal Evidence and Proof: Statistics, Stories, Logic*, Ashgate, Farnham, 2009, pp. 223-253.

97. En Portugal, *Cf.* QUINTELA DE BRITO, T., "*Compliance*, cultura corporativa e culpa penal da pessoa jurídica", en DE SOUSA MENDES, P. *et al.* (Dir.), *Estudos sobre Law Enforcement, Compliance e Direito Penal*, 2.ª ed., Almedina, Coimbra, 2018, (pp. 57-100) p. 89. También *Cf.* MIRANDA RODRIGUES, A., *Direito Penal Económico – Uma Política Criminal na Era Compliance*, Almedina, Coimbra, 2019, pp. 65-70. Igualmente, *Cf.* AIRES DE SOUSA, S., *Questões Fundamentais de Direito Penal da Empresa*, Almedina, Coimbra, 2019, pp. 128-135. Véase la jurisprudencia portuguesa citada por LEITE BAPTISTA, A., "*Compliance* em processo contraordenacional: Da alegação à decisão através da prova", en DE SOUSA MENDES, P. *et al.* (Dir.), *Estudos sobre Law Enforcement, Compliance e Direito Penal*, 2.ª ed., Almedina, Coimbra, 2018 (pp. 345-384) pp. 378-379, n. 83. En Brasil, *Cf.* MACHADO SARAIVA, R., *Criminal Compliance como Instrumento de Tutela Ambiental – A Propósito da Responsabilidade Penal de Empresas*, LiberArs, São Paulo, 2018, pp. 61-68. También *Cf.* SCANDELARI, G. B., *Compliance e Prevenção Corporativa de Ilícitos – Inovações e Aprimoramentos para Programas de Integridade*, Almedina, Coimbra, 2022, pp. 151-212.

Tribunal Europeo de los Derechos Humanos, en jurisprudencia reiterada, ha fijado que las infracciones típicamente administrativas deben ser consideradas infracciones penales para efectos de la aplicación del artículo 6.º de la Convención Europea de los Derechos Humanos, que consagra el derecho a un proceso equitativo y a la presunción de inocencia.

El contexto social del derecho regulador obliga a un cambio de paradigma en la aplicación del derecho y la interacción con los agentes económicos. La experiencia apunta generalizadamente a las ventajas de un abordaje basado en los principios de la regulación responsiva y de la autorregulación regulada. El balance entre ambas exige, no obstante, un delicado equilibrio entre las exigencias de una regulación eficaz y las ventajas de colaboración con las empresas en el desempeño de esta misión de derecho público. De hecho, los riesgos de esta articulación son enormes y solo pueden ser aminorados a través de la consagración de mecanismos que garanticen la independencia y la rendición de cuentas (*accountability*) de los reguladores e impidan la captura (*regulatory capture*)[98] por innumerables intereses, que van de los intereses partidistas a los empresariales, a lo que contribuye también la imposición de obligaciones de transparencia y restricciones a las puertas giratorias (*revolving doors*) entre el ejercicio de funciones de regulación, funciones gubernativas y funciones de gestión de empresas públicas, mixtas o privadas.

VII. CONCLUSIÓN

De todo lo aquí expuesto resulta que la regulación responsiva y la autorregulación regulada son una buena idea, pero puede tener resultados insatisfactorios por muchas y variadas razones y en múltiples circunstancias, a menos que sean creados mecanismos de independencia efectiva, rendición de cuentas, anti captura y autorreflexión crítica de los reguladores.

Los conceptos de regulación responsiva y de autorregulación regulada son indisociables entre sí, porque el cumplimiento normativo por parte de la industria solo puede mejorar si se tienen debidamente en cuenta las potestades de reglamentación, supervisión y aplicación de sanciones administrativas por parte de las autoridades independientes, así como las competencias de investigación y acusación de la Fiscalía en materia penal. El papel de los agentes de aplicación del Derecho (*law enforcement*)

98. *Cf.* POSNER, R. A., "The Concept of Regulatory Capture: A Short, Inglorious History", en CARPENTER, D. y MOSS, D., *Preventing Regulatory Capture – Special Interest Influence and How to Limit It*, Cambridge University Press, Cambridge, 2013, pp. 49-56.

mejorará también si éstos adoptan modelos de regulación responsiva, adecuándose empáticamente a las mejoras de cultura corporativa de la industria y escogiendo, de esta forma, la oportunidad y la intensidad de sus respectivas actuaciones supervisora y sancionadora.

Por la parte que toca a la industria, los desafíos son esencialmente de conformación y (re) definición de la cultura de las empresas, articulando y conciliando la dimensión económica y financiera del negocio con los riesgos de su actividad, especialmente los riesgos legales, siguiendo la máxima de que más vale prevenir que curar.

El alcance y detalle de una política de conformidad es más exigente cuando se trata de una empresa que desarrolla su actividad en un sector regulado. Por una simple razón: el marco legal y reglamentario en dichos sectores es siempre de mayor alcance, y también más denso y minucioso, que en los restantes sectores de actividad, además de ser más propenso a su evolución y revisión como marco normativo.

Capítulo 13

Pessoas colectivas e direitos de defesa – alguns aspectos do regime processual português[1]

Vânia Costa Ramos

Advogada
Assistente-Convidada na Faculdade de Direito da Universidade de Lisboa

I. A LACUNA NA REGULAMENTAÇÃO LEGAL DOS ASPECTOS PROCESSUAIS DA RESPONSABILIDADE PENAL DAS PESSOAS COLECTIVAS EM PORTUGAL (1984-2021)

Desde 1984 que está consagrada, embora com carácter excepcional até 2007, a responsabilidade penal das pessoas colectivas no ordenamento jurídico português.

No âmbito dos diplomas que consagraram a responsabilidade das pessoas colectivas com carácter excepcional[2] não foram consagradas disposições processuais para as pessoas colectivas. A omissão poderia ter sido, nessa fase, "desculpável", por tratar-se de regimes excepcionais. O mesmo não poderá dizer-se, no entanto, relativamente às alterações de 2007, 2010 e 2013 ao Código Penal (CP).

Com efeito, a reforma penal de 2007 introduziu a responsabilidade das pessoas colectivas no Código Penal, estendendo-a a um amplo número de

1. Este trabalho foi elaborado no âmbito do projecto de investigação do Ministério da Ciência e Inovação: "O Processo Penal e a União Europeia". Análise e propostas" –PID2020-116848GB-100–, bem como do Grupo de Investigação Reconhecido "Garantias Processuais e União Europeia", da Universidade de Valladolid.

2. Designadamente, o Decreto-Lei n.º 28/84, de 20 de Janeiro, o Regime jurídico das infracções fiscais não aduaneiras (RJIFNA) (Decreto-Lei n.º 20-A/90, de 15 de Janeiro), Regime jurídico das infracções fiscais aduaneiras (RJIFA) (Decreto-Lei n.º 376-A/89, de 25 de Outubro) e o Regime geral para as infracções tributárias (RGIT) (Lei n.º 15/2001, de 05 de Junho).

condutas penalmente relevantes. Da mesma forma, deveria ter procedido à adaptação das normas processuais penais para aplicação às pessoas colectivas[3].

Em 2010 e 2013 foram efectuadas alterações de necessidade duvidosa (por exemplo, relativamente às medidas de coacção e ao regime da prescrição) e, ainda assim, este problema, que nos parece de maior importância, continuou a ser ignorado.

Também do ponto de vista do seu tratamento doutrinário, os problemas processuais da responsabilidade penal das pessoas colectivas não vinham, até certa altura, merecendo qualquer destaque, com honrosas excepções[4].

---

3. Neste sentido, v.g., SILVA, G.M., «Questões processuais na responsabilidade cumulativa das empresas e seus gestores», in MONTE, M.F. (et al.) (coord.), *Que futuro para o direito processual penal?: simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, Coimbra Editora, Coimbra, 2009, págs. 789-803; BRITO, T.Q., «Processo contra pessoas colectivas: algumas propostas de adaptação (urgente) do Código de Processo Penal português», in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág. 477 e ss. TEIXEIRA, C.A., «A pessoa colectiva como sujeito processual; ou a "descontinuidade" processual da responsabilidade penal», *Revista do CEJ*, núm. 8 (especial), 2008, pág. 100. Referindo a total omissão de disposições processuais, que também caracteriza como surpreendente, BRAVO, J.R., «Incidências processuais da punibilidade de entes colectivos», *RMP*, núm. 105, 2006, págs. 50-52, advertia já que, «no contexto de um processo legislativo em que […] um regime geral de responsabilidade criminal de entes colectivos tende a ser aprovado […], seria curial que se acautelasse, também no âmbito legislativo, a dimensão adjectiva de tal realidade», explicitando os motivos pelos quais a utilização da analogia ou de mecanismos do processo civil é inadequada. MEIRELES, M.P., «A responsabilidade penal das pessoas colectivas ou entidades equiparadas na recente alteração ao Código Penal ditada pela Lei 59/2207, de 4 de Setembro: algumas notas», *JULGAR*, núm. 5, 2008, págs. 123-124 e 133.

4. SILVA, G.M., «Questões processuais na responsabilidade cumulativa das empresas e seus gestores», in MONTE, M.F. (et al.) (coord.), *Que futuro para o direito processual penal?: simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, Coimbra Editora, Coimbra, 2009, págs. 789-803; ALBUQUERQUE, P.P., *Comentário do Código de Processo Penal,* 4.ª Ed., Universidade Católica Editora, Lisboa, 2011; BRAVO, J.R., «Incidências processuais da punibilidade de entes colectivos», *RMP*, núm. 105, 2006, págs. 45-99. TEIXEIRA, C.A., «A pessoa colectiva como sujeito processual; ou a "descontinuidade" processual da responsabilidade penal», *Revista do CEJ*, núm. 8 (especial), 2008, pág. 99-166; MEIRELES, M.P., «A responsabilidade penal das pessoas colectivas ou entidades equiparadas na recente alteração ao Código Penal ditada pela Lei 59/2207, de 4 de Setembro: algumas notas», *JULGAR*, núm. 5, 2008, págs. 121 e ss; REGO, C.L. «Constitucionalidade do artigo 40 do Código de processo penal; intervenção no julgamento de arguida (pessoa colectiva) do juiz que na fase de inquérito decretou a prisão preventiva de outro co-arguido (pessoa singular)», *RMP,* núm. 71, 1997, págs.123-127. DIAS, A.S./RAMOS, V.C., *O Direito à não auto-inculpação (nemo tenetur seiIpsum accusare) no*

Dever-se-ia tal facto à, porventura, menor dignidade dogmática do tema? Não pensamos que tal possa afirmar-se, sobretudo porque, como refere GERMANO MARQUES DA SILVA[5], o tema é de importância prática mor. Não nos parece por este motivo viável o desenvolvimento de uma dogmática penal da responsabilidade das pessoas colectivas alheada dos problemas da sua concretização processual, sob pena de aquela ser político-criminalmente ineficiente[6]. Nos últimos anos, todavia, a doutrina tornou-se mais activa no que diz respeito a este tema, o que poderá eventualmente tido influência na reforma operada em 2021[7].

A omissão de disposições processuais penais específicas para aplicação à pessoa colectiva resultava assim na existência de múltiplas lacunas que, de um ponto de vista prático, dificultavam a tarefa da interpretação e aplicação do direito nos casos concretos, obrigando os sujeitos processuais a procederem, ou a interpretação extensiva, ou à analogia para integração de lacunas caso-a caso. Tudo com prejuízo para a eficiência processual e para a segurança jurídica, bem como para a igualdade na aplicação do direito e a condução de um processo justo e equitativo[8]. Além do mais,

---

processo penal e contra-ordenacional português, Coimbra Editora, Coimbra 2009, págs. 39-42, tratam, muito embora não desenvolvidamente, a questão da aplicação deste direito às pessoas colectivas, resolvendo-a no sentido afirmativo.

5. SILVA, G.M., «Questões processuais na responsabilidade cumulativa das empresas e seus gestores», in MONTE, M.F. (et al.) (coord.), *Que futuro para o direito processual penal?: simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, Coimbra Editora, Coimbra, 2009, pág. 789.
6. TEIXEIRA, C.A., «A pessoa colectiva como sujeito processual; ou a "descontinuidade" processual da responsabilidade penal», *Revista do CEJ*, núm. 8 (especial), 2008, pág. 166, questiona se, face à inexistência de disposições processuais penais específicas, no final do "calvário processual", a responsabilidade penal das pessoas colectivas não será apenas direito penal simbólico.
7. V.g. BRITO, T.Q., «Processo contra pessoas colectivas: algumas propostas de adaptação (urgente) do Código de Processo Penal português», in ALBUQUERQUE, P.P./CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, 2021, pág. 477-514; ANTUNES, M.J., *Processo Penal e pessoa colectiva arguida,* Almedina, Coimbra, 2020; LOUREIRO, F.N., «A insustentável ausência de normas processuais penais para pessoas colectivas», in MOUTINHO, J.L./SALINAS, H./SEQUEIRA, E.V./MARQUES, P.G. (coord.), *Homenagem ao Professor Doutor Germano Marques da Silva,* vol. II, Universidade Católica Editora, Lisboa, 2020, pág. 896; ANTUNES, M.J., «A posição processual da pessoa colectiva constituída arguida», *JULGAR*, núm. 38, 2019, págs. 17-29; SILVA, G.M., «Questões processuais da responsabilidade penal das empresas e seus gestores», in PALMA, M.F./DIAS, A.S./MENDES, P.S. et al. (coord.), *Law enforcement, compliace e direito penal*, 2.ª Ed., Almedina, Coimbra, 2018, págs. 151-159, SILVA, G.M., «Sobre a representação das pessoas coletivas constituídas arguidas no processo criminal», *Católica Law Review,* núm. 3, 2018, págs. 103-111.
8. MEIRELES, M.P., «A responsabilidade penal das pessoas colectivas ou entidades equiparadas na recente alteração ao Código Penal ditada pela Lei 59/2207, de 4 de

nem todas as lacunas que existiam eram susceptíveis de integração através do recurso ao disposto no art. 4.º do Código de Processo Penal (CPP), dando origem a omissões de regulamentação que, em última análise, poderiam ser susceptíveis de obstaculizar a finalidade político-criminal da consagração da responsabilidade penal das pessoas colectivas.

II. A REGULAMENTAÇÃO LEGAL DOS ASPECTOS PROCESSUAIS DA RESPONSABILIDADE PENAL DA PESSOA COLECTIVA NO CPP ATRAVÉS DA LEI N.º 94/2021, DE 21 DE DEZEMBRO

A Lei n.º 94/2021, de 21 de Dezembro[9], veio, finalmente, colocar termo a esta situação insustentável. É perfeita, a solução legislativa adoptada? Poderá não o ser[10], mas teve, pelo menos, o condão de introduzir uma

---

Setembro: algumas notas», *JULGAR*, núm. 5, 2008, pág. 138, refere que sem alterações legislativas, a «concretização da responsabilidade penal das pessoas colectivas ou entidades equiparadas no Código Penal pode não passar, na prática, de uma fonte interminável de problemas, que tornem o processo criminal insusceptível de conduzir a um julgamento justo». SILVA, G.M, «A pessoa colectiva como arguida no processo penal», conferência proferida no âmbito do I Curso de Outono sobre Direito Penal das Pessoas Colectivas, FDL, Outubro de 2014, disponível em https://carlospintodeabreu.com/public/files/a_pessoa_colectiva_como_arguida_no_processo_penal.pdf (consulta em 05.10.2022), págs. 1-2, afirma que é criticável a ausência de soluções legais para os problemas processuais da pessoa colectiva como arguida, alertando que a «mera circunstância de ter de ser construído em grande parte por interpretação extensiva ou integração acarreta dificuldades e divergências porque as soluções normativas não estão ainda consolidadas pela jurisprudência». Mais recentemente, e ainda nesse sentido, SILVA, G.M, «Processo contra pessoas coletivas» in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág. 466.

9. Lei n.º 94/202, de 21.12, disponível em https://files.dre.pt/1s/2021/12/24500/0000300049.pdf (consulta em 05.10.2022). O texto da alteração provém de uma proposta do PSD – cf. ANTUNES, M.J., «A pessoa coletiva arguida no processo penal. O que muda?», *RPCC*, núm. 31, 2021, págs. 1-9.

10. Cf. por exemplo algumas críticas de SILVA, G.M, «Responsabilidade penal das pessoas coletivas questões processuais», conferência proferida no Centro de Estudos Judiciários, 14.01.2022 (*texto gentilmente cedido pelo autor*): ausência de ponderação da admissibilidade do recurso para o STJ relativamente às penas de multa aplicadas às pessoas coletivas, pondo termo ao desfasamento dos recursos em matéria cível e em matéria penal, conforme consta do nº 2 do artigo 400º; não regulamentação da representação da pessoa colectiva após liquidação; desfasamento ou contradição entre o artigo 359.º, nº 3, do Código Penal, e o artigo 342.º, n.º 4, do Código de Processo Penal; a aplicação do instituto da contumácia no caso de não nomeação de representante pela pessoa colectiva; inexistência de obrigação de comunicar a ausência do representante ao abrigo do TIR; falta de critérios para aplicação de medidas de coacção às pessoas colectivas que poderão significar o mesmo que a «morte» destas, caso não seja especialmente ponderada e conhecida a vida das empresas, «o que não acontece com frequência» (por exemplo, o controlo de contas bancárias); falta

primeira regulamentação dos aspectos processuais da responsabilidade penal das pessoas colectivas, o que, desde logo, é de aplaudir.

Em concreto, foram introduzidas normas sobre os seguintes aspectos[11]:

a) conexão de processos (art. 24.º, n.º 1, alínea f));

b) constituição de arguido (arts. 57.º, n.º 4, 58.º, n.º 3 e 59.º, n.º 3);

c) representação da pessoa coletiva arguida (art. 57.º,n.ºs 4, 5, 6, 7, 8 e 9);

d) direitos e deveres (arts. 61.º e 196.º, n.º 5);

e) assistência obrigatória por defensor (art. 64.º, n.º 5);

f) notificações (arts. 113.º, n.ºs 16 e 17, 196.º, n.º 5, alínea c), 313.º, n.º 2, e 335.º, n.º 6)

g) impedimentos e recusa de depoimento (art. 133.º, n.º 1, alínea e), e 134.º, n.º 1, alínea c);

h) medidas de coação (art. 196.º, n.ºs 4 a 6, 197.º, n.º 4, 199.º, n.º 3, 200.º, n.º 7, e 204.º, n.º 2 e 3);

i) caução económica e arresto preventivo (art. 227.º, n.º 6, e 228.º, n.º 7);

j) suspensão provisória do processo (art. 281.º, n.ºs 3 e 11[12]);

k) declaração de contumácia (art. 335.º, n.º 6);

l) declarações da arguida (arts. 342.º, n.ºs 3 e 4, e 344.º, n.º 5);

m) processo abreviado (art. 391.º-A, n.º 4);

n) processo sumaríssimo (art. 392.º, n.º 3);

o) responsabilidade de terceiros pelo pagamento de multas e indemnizações aplicados à pessoa colectiva (art. 491.º-B).

Algumas das normas introduzidas limitaram-se a consagrar explicitamente a aplicabilidade às pessoas colectivas arguidas das normas

---

de definição do que deve ser um programa de *compliance* e dos termos da vigilância judiciária, no âmbito da suspensão provisória do processo, abrindo um campo de vasta discricionariedade.

11. Excluímos o art. 174.º, n.º 5, do CPP, pois este não visa a situação da pessoa colectiva arguida, mas, genericamente, a regulamentação da legitimidade para consentir em caso de busca a pessoa colectiva, seja esta ou não arguida, clarificando que apenas o respectivo representante pode consentir.

12. Cf., ainda, no artigo 9.º, n.º 3, da Lei n.º 36/94, de 29.09.

previstas para as pessoas singulares arguidas. Exemplo destas normas são as referentes à assistência obrigatória por defensor (art. 64.º, n.º 5); caução económica e arresto preventivo (art. 227.º, n.º 6, e 228.º, n.º 7); processo abreviado (art. 391.º-A, n.º 4); processo sumaríssimo (art. 392.º, n.º 3).

As demais normas procuraram adaptar à realidade da pessoa colectiva o regime processual penal originalmente concebido para as pessoas singulares.

III. ASPECTOS SELECCIONADOS DO DIREITO DE DEFESA DAS PESSOAS COLECTIVAS

1. O ESTATUTO DE ARGUIDA E A SUA AQUISIÇÃO

A Constituição e a lei processual penal consagram uma série de direitos de que é titular a pessoa arguida em processo penal, designadamente nos arts. 29.º e 32.º da Constituição da República Portuguesa (CRP), e nos arts. 60.º e 61.º, n.º 1, do CPP. O CPP consagra também, ainda que de forma limitada, deveres que recaem sobre o arguido, designadamente os constantes do art. 61.º, n.º 3, do CPP. Antes da Lei n.º 94/2021, de 21.12, inexistia qualquer referência expressa às pessoas colectivas naquelas normas, o que poderia levar à dúvida sobre se esses direitos e deveres eram aplicáveis às arguidas pessoas colectivas.

O art. 12.º, n.º 2, da CRP dispõe que «as pessoas colectivas gozam dos direitos e estão sujeitas aos deveres compatíveis com a sua natureza». Se a natureza das pessoas colectivas não obsta à sua responsabilização criminal, impõe tal natureza que, excepcionadas as limitações dela mesma decorrentes, as pessoas colectivas gozem do respectivo estatuto processual de arguido, idêntico ao das pessoas singulares[13]. Neste sentido decidiu o Tribunal Constitucional, referindo especificamente o direito

13. Neste sentido, *Bravo, Jorge dos Reis*, Incidências processuais da punibilidade de entes colectivos, RMP 105 (2006), 45, 62, "dir-se-á, portanto, que nenhuma restrição de direitos, no plano do estatuto processual enquanto arguidas, lhes poderá ser assinalada. Significa isto que não se poderá defender qualquer distinção de estatuto processual das pessoas colectivas, relativamente aos indivíduos, para alem daquelas que resultem da sua própria natureza". Dando como exemplo da diferença de incidência dos direitos em causa, no campo do direito à não auto-inculpação, a inaplicabilidade deste às pessoas colectivas nos casos de colheita de ar expirado ou de material orgânico, DIAS, A.S./RAMOS, V.C., *O Direito à não auto-inculpação (nemo tenetur se ipsum accusare) no processo penal e contra-ordenacional português*, Coimbra Editora, Coimbra 2009, pág. 42.

à presunção de inocência e a ser julgado por um tribunal imparcial[14]. A conclusão neste sentido não poderia ser outra, tendo em conta a decorrência da consagração constitucional de um processo penal de estrutura acusatória, com garantias de defesa constitucionalmente ancoradas e que se aplicarão a qualquer arguido, seja pessoa colectiva ou singular. O CPP estabelece agora, no art. 57.º, n.º 4, que a «pessoa coletiva ou entidade equiparada pode ser constituída arguida […]», tornando-lhe aplicáveis os direitos e deveres do arguido constantes do CPP.

Tal como a pessoa singular, a pessoa colectiva assumirá a posição de arguida, o mais tardar, nos termos do art. 57.º, n.º 1, do CPP, com a dedução de acusação ou requerimento de instrução contra si apresentado. Ou, nos termos do art. 58.º, n.º 1, als. *a), b)* e *d)*, do CPP, quando (i) correndo inquérito contra pessoa colectiva determinada relativamente à qual exista suspeita fundada da prática de crime, um seu representante preste declarações; (ii) seja necessário aplicar-lhe medida de coacção ou de garantia patrimonial; (iii) lhe for comunicado auto de notícia que a dê como agente de um crime, salvo se a notícia for manifestamente infundada.

Poderá ainda questionar-se se a pessoa colectiva deveria ser constituída arguida quando seja detido um seu representante legal também suspeito, nos termos da al. *c)*, do n.º 1, do art. 58.º, do CPP. Neste caso não nos parece ser necessária a constituição de arguido da pessoa colectiva, uma vez que a natureza da constituição de arguido tem que ver com a situação de detenção que, por natureza, é incompatível com a natureza da pessoa colectiva. Em todo o caso, se essa pessoa detida prestar declarações e o fizer também na qualidade de representante da pessoa colectiva, por actos praticados nessa qualidade, no interesse e por conta da sociedade, esta deverá também ser constituída arguida, já nos termos do art. 58.º, n.º 1, al. *a*), do CPP.

O artigo 59.º, n.º 3, do CPP prevê (tal como para as pessoas singulares, ao abrigo do artigo 59.º, n.º 1, que se «durante a inquirição de um seu representante como arguido ou testemunha, surja a fundada suspeita da prática de um crime pela pessoa coletiva ou entidade equiparada que ainda não seja arguida», a entidade que procede ao acto suspende-o imediatamente e procede à constituição de arguido, nos termos do art. 58.º, n.º 2. Desta norma, conjugada com o art. 58.º, n.º 1, al. *a*), do CPP, se retira que a constituição de arguido de pessoa colectiva

14. Acórdão do Tribunal Constitucional n.º 656/97, de 04.11, proc. n.º 126/97 (Relator: Ribeiro Mendes), disponível em http://www.tribunalconstitucional.pt/tc/acordaos/19970656.html (consulta em 05.10.2022). Em idêntico sentido, ANTUNES, M.J., «A pessoa coletiva arguida no processo penal. O que muda?», *RPCC*, núm. 31, 2021, págs. 3-4.

não sucede *sempre* que o seu representante seja ouvido como arguido, mas tão só e apenas quando tal aconteça *e* exista suspeita fundada da prática de crime pela pessoa colectiva. Crime esse que possa ter sido praticado por quem nela ocupe posição de liderança, ou por qualquer funcionário, com violação dos deveres de vigilância por quem nela ocupe a primeira posição, desde que por todos praticado no seu âmbito funcional e no interesse directo ou indirecto da pessoa colectiva – cf. art. 11.º, n.º 2, do CP.

A pessoa colectiva pessoa sobre quem recair suspeita de ter cometido um crime tem ainda direito a ser constituída, a seu pedido, como arguida sempre que estiverem a ser efectuadas diligências, destinadas a comprovar a imputação, que pessoalmente a afectem (art. 59.º, n.º 2, do CPP). Em minha opinião, esta norma permite que a pessoa colectiva adquira também a qualidade de arguida, por exemplo no âmbito de uma busca na sua sede social, se desta decorrer que existe suspeita da prática de infracção por parte da pessoa colectiva. A redacção do artigo 59.º, n.º 3, poderá, no entanto, suscitar dúvidas sobre a inclusão de tais diligências, pois remete a aplicabilidade dos «números anteriores», aos casos da «inquirição de um seu representante como arguido ou testemunha» em que «surja a fundada suspeita da prática de um crime pela pessoa coletiva ou entidade equiparada que ainda não seja arguida». Parece-me, no entanto, que esta norma deve ser interpretada não no sentido da exclusão de demais diligências que possam, nos termos do n.º 2, conferir o direito à constituição de arguida da pessoa colectiva, mas antes no sentido de clarificar a aplicação dos números anteriores no caso das inquirições, já que para as pessoas singulares é sempre coincidente o inquirido com o suspeito, enquanto nas pessoas colectivas existe por natureza alteridade, justificando a previsão específica consagrando a adaptação da norma. No caso da busca à pessoa colectiva não arguida, inexiste essa alteridade, sendo aplicável directamente o art. 59.º, n.º 2, do CPP. Parece ficar de fora o caso da busca contra pessoa singular que seja representante da pessoa colectiva, quando do mandado ou da própria busca decorra também a existência de suspeita contra a pessoa colectiva, por não serem «diligências, destinadas a comprovar a imputação, que *pessoalmente* a afectem». No entanto, tenho dúvidas neste ponto.

Veremos de seguida algumas normas consagradas no CPP, com a Lei n.º 94/2021, de 21 de Dezembro, sobre o estatuto processual da pessoa colectiva arguida, seus direitos e deveres, em particular sobre: (i) a representação da pessoa colectiva e (ii) o direito à não auto-inculpação.

2. REPRESENTAÇÃO

Tal como um arguido pessoa singular a pessoa colectiva tem o direito (e por vezes o dever) de estar presente nos actos processuais que lhe digam directamente respeito, bem como o direito a ser ouvida antes de serem tomadas decisões que a afectem pessoalmente (art. 61.º, n.º 1, als. *a)* e *b)*, do CPP). Coloca-se, porém, o problema de saber *como* podem ou devem as pessoas colectivas estar presentes. O art. 61.º, n.º 7, do CPP, introduzido com a Lei n.º 94/2021, de 21.12, adianta que «os direitos e os deveres previstos nos números anteriores são exercidos e cumpridos pela pessoa coletiva ou entidade equiparada, *através do seu representante*».

Antes das alterações ao CPP, GERMANO MARQUES DA SILVA defendia que a representação da pessoa colectiva devia ser feita pelo representante legal à data do acto processual[15]. Não foi esta integralmente a opção do legislador que, na Lei n.º 94/2021, de 21 de Dezembro, admite a nomeação de um terceiro para representar a pessoa colectiva arguida, sendo essa a solução a título principal para as pessoas colectivas e a título subsidiário para as entidades sem personalidade jurídica.

A matéria vem regulada no artigo 57.º do CPP, onde se lê, logo no n.º 4, que «[a] pessoa coletiva ou entidade equiparada pode ser constituída arguida, *sendo representada por quem a pessoa coletiva designar ou, na ausência de tal designação, por quem a lei designar*». Igualmente, no n.º 5 prevê-se que «[a] entidade que careça de personalidade jurídica é representada pela pessoa que aja como diretor, gerente ou administrador e, *na sua falta, por pessoa escolhida pela maioria dos associados*».

GERMANO MARQUES DA SILVA[16] defende que o art. 57.º, n.º 4, apenas deveria permitir que a administração designasse um representante quando este possa «sê-lo nos termos da lei, ou seja, quando os estatutos ou o regime legal aplicável à pessoa coletiva arguida permita a sua representação por terceiro». No entanto, não é o que decorrerá do texto, segundo o autor, o que levará a ter «muito provavelmente, nas médias e grandes empresas, um funcionário com a função de representar a pessoa coletiva nos processos criminais, o que se me não afigura compatível com o princípio de que o arguido deve estar pessoalmente no processo quando

15. SILVA, G.M., «Processo contra pessoas coletivas» in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág. 468; SILVA, G.M., «Sobre a representação das pessoas coletivas constituídas arguidas no processo criminal», *Católica Law Review,* núm. 3, 2018, págs. 107-108.

16. SILVA, G.M, «Responsabilidade penal das pessoas coletivas questões processuais», conferência proferida no Centro de Estudos Judiciários, 14.01.2022 (*texto gentilmente cedido pelo autor*), II.

o representante não tenha cobertura estatutária ou legal». Questão que, como o autor alerta «não é irrelevante» em termos de direito probatório, nomeadamente ao nível dos impedimentos para depor como testemunha, ou do direito à não auto-inculpação.

O regime proposto por GERMANO MARQUES DA SILVA seria similar ao do processo civil, nos arts. 25.º, n.º 1, do Código de Processo Civil (CPC), sendo as sociedades com personalidade jurídica representadas «por quem a lei, os estatutos ou o pacto social designarem», e 26.º do CPC, «os patrimónios autónomos são representados pelos seus administradores e as sociedades e associações que careçam de personalidade jurídica, bem como as sucursais, agências, filiais ou delegações, são representadas pelas pessoas que ajam como diretores, gerentes ou administradores».[17] Nos termos da lei, as pessoas colectivas são representadas por quem os estatutos determinarem ou, na falta de disposição estatutária, pela administração ou quem por ela for designado (art. 163.º do CC); as sociedades civis, pelos administradores, nos termos do contrato, ou do art. 985.º do CC, por todos os sócios (art. 996.º, n.º 1, do CC); as sociedades por quotas, pelos gerentes (art. 252.º do CSC); as sociedades anónimas pelo conselho de administração (art. 405.º do CSC); as sociedades em nome colectivo, pelos gerentes (art. 192.º do CSC); as associações de facto, por quem as administre ou dirija (art. 163.º do CC e 26.º do CPC). Se se tratar de uma sociedade de direito estrangeiro, haverá que recorrer a esse direito para determinar quem são os legais representantes.

As críticas do autor parecem ter tido eco no legislador, que, pouco tempo depois, através da Lei n.º 13/2022, de 1 de Agosto[18], veio novamente alterar o artigo 57.º do CPP. Este dispõe agora, no n.º 5, que «[a] pessoa coletiva é *representada por quem legal ou estatutariamente a deva representar*[…]». Claro que tal não excluirá, a meu ver, a escolha de um representante "processual" *ad hoc* que não pertença aos órgãos estatutários, com poderes de representação, quando tal seja permitido pelos estatutos da pessoa colectiva.

O que sucede quando são vários os representantes legais ou estatutários da pessoa colectiva? Quem pode escolher o representante para fins

17. SILVA, G.M., «Processo contra pessoas coletivas» in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág. 468; SILVA, G.M., «Questões processuais da responsabilidade penal das pessoas colectivas» in PALMA, M.F./ DIAS, A.S./MENDES, P.S. et al. (coord.), Estudos sobre *Law enforcement, compliace e direito penal*, Almedina, Coimbra, 2018, págs. 157 e 158.

18. Lei n.º 13/2022, de 01.08, disponível em https://dre.pt/dre/detalhe/lei/13-2022-186869046 (consulta em 05.10.2022).

processuais? GERMANO MARQUES DA SILVA sugeria que a escolha não pode ser feita pela entidade que presida ao acto, mas tem de ser feita pela própria pessoa colectiva que pode, aliás, mudar o seu representante[19]. Parece-me, porém, que, se no decurso de um acto processual, por exemplo uma busca, estiver presente um representante da pessoa colectiva, não pode esta impedir que seja este o representante que assine a constituição de arguido, sem que indique outro que, no momento, possa fazê-lo. Evidentemente tal não impede a pessoa colectiva de, posteriormente, indicar no processo outro representante.

A mudança de representante pode, aliás, decorrer da própria alteração do representante legal da sociedade, que deixa assim de ter poderes de representação, tendo aliás a nova redacção do artigo 196.º, n.º 5, do CPP, a propósito do Termo de Identidade e Residência (TIR), estabelecido que «[d] a obrigação de comunicar no prazo máximo de 5 dias as alterações da sua identificação social, nomeadamente nos casos de cisão, fusão ou extinção, ou quaisquer factos que impliquem a substituição do seu representante, sem prejuízo da eficácia dos atos praticados pelo anterior representante».

O próprio representante pode requerer a sua substituição, de acordo com o novo n.º 6, do artigo 196.º do CPP, «quando se verificarem factos que impeçam ou dificultem gravemente o cumprimento dos deveres e o exercício dos direitos da sua representada, sendo que a substituição do representante não prejudica o termo já prestado pela representada». Supomos que tal se verificará quando, por exemplo, um representante legal deixe de o ser, e a pessoa colectiva não comunique a alteração; quando exista risco de auto-inculpação ou de hetero-inculpação do representante pela pessoa colectiva (*que dificilmente o representante poderá crer admitir no respectivo requerimento…*); ou quando um representante *ad-hoc* designado para o efeito não consiga manter o necessário contacto com a pessoa colectiva, ou esta não cumpra o contrato de mandato celebrado com o representante, impedindo-o do cumprimento dos respectivos deveres (*o representante designado pode ser externo à empresa e colocar termo ao contrato celebrado para o efeito nos termos do mesmo ou da lei aplicável*).

O CPP regula agora também a representação das entidades fundidas ou cindidas. nos termos dos n.º 6 e 7 do artigo 57.º, dispondo que

19. SILVA, G.M, «Processo contra pessoas coletivas» in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, págs.468 e 469; SILVA, G.M., «A pessoa colectiva como arguida no processo penal», conferência proferida no âmbito do I Curso de Outono sobre Direito Penal das Pessoas Colectivas, FDL, Outubro de 2014, disponível em https://carlospintodeabreu.com/public/files/a_pessoa_colectiva_como_arguida_no_processo_penal.pdf (consulta em 05.10.2022), pág. 10.

a representação cabe aos representantes das pessoas coletivas cindidas ou da pessoa coletiva fundida (supomos que queira com esta expressão designar-se a pessoa colectiva resultante da fusão). Nos casos de cisão, poderia questionar-se se esta solução não deveria ser mitigada, permitindo-se a gestão das *liabilities* das empresas através da cisão, mediante, por exemplo, a sujeição a medidas de garantia patrimonial que acautelem as responsabilidades no âmbito do processo contra a *bad entity*. Se houver transformação da sociedade, também não se coloca qualquer problema, passando a responder como arguida a sociedade na sua nova forma (por exemplo, uma S.A., em vez de uma sociedade por quotas), podendo, porém, esta alteração reflectir-se nas regras sobre a representação processual.

O artigo 57.º, n.º 8, do CPP, vem agora dizer que «[n]o caso de extinção e quando tenha sido declarada a insolvência e até ao encerramento da liquidação, mantém-se o representante à data da extinção ou da declaração de insolvência». No caso particular das sociedades em liquidação no âmbito de processo de insolvência, a jurisprudência maioritária defendia já que estas eram representadas, não pelo administrador de insolvência (pois as suas funções se prendem apenas com a esfera patrimonial da pessoa colectiva), mas sim pelos representantes legais da pessoa colectiva (art. 82.º do CIRE)[20].

O art. 127.º, n.º 2, do Código Penal regula a extinção do processo no caso de «morte» da pessoa colectiva, prevendo que «no caso de extinção de pessoa colectiva ou entidade equiparada, o respectivo património responde pelas multas e indemnizações em que aquela for condenada». A jurisprudência maioritária, proferida em regra a propósito de situações cuja insolvência foi declarada, preconiza a extinção da responsabilidade criminal com o registo do encerramento da liquidação[21]. Nos casos de

20. Em sentido concordante SILVA, G.M., «Questões processuais da responsabilidade penal das pessoas colectivas» in PALMA, M.F./DIAS, A.S./MENDES, P.S. et al. (coord.), Estudos sobre *Law enforcement, compliace e direito penal*, Almedina, Coimbra, 2018, pág.160; SILVA, G.M, «A pessoa colectiva como arguida no processo penal», conferência proferida no âmbito do I Curso de Outono sobre Direito Penal das Pessoas Colectivas, FDL, Outubro de 2014, disponível em https://carlospintodeabreu.com/public/files/a_pessoa_colectiva_como_arguida_no_processo_penal.pdf (consulta em 05.10.2022), pág. 5.

21. *V.g.* Acórdão do Supremo Tribunal de Justiça, de 12.10.2006, Processo 06P2930 (Relator: Pereira Madeira), disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/74c2b0def7f436ff8025725d00560ccc?OpenDocument (consulta em 05.10.2022); Acórdão do Tribunal da Relação de Coimbra, de 04.03.2015, Proc. 6/05.3EDCBR-B.C1 (Relator: Alice Santos), disponível em http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/a51fb746ec05225780257e05004f3088?OpenDocument (consulta em 05.10.2022).

dissolução voluntária, nos termos do art. 160.º, n.º 2, do CSC, não ocorre extinção da responsabilidade criminal com o registo do encerramento da liquidação[22].

GERMANO MARQUES DA SILVA inclina-se a considerar, em sentido contrário, que o património da pessoa colectiva apenas pode responder enquanto não estiver registado o encerramento da liquidação[23]. A distinção jurisprudencial entre a dissolução voluntária e a insolvência parece ir no sentido da posição defendida por GERMANO MARQUES DA SILVA que refere a extinção da pessoa colectiva como irrelevante para a extinção da responsabilidade penal, por razões de necessidade da pena «porque a extinção voluntária da pessoa colectiva podia ser causada para evitar as sanções, nomeadamente as pecuniárias, em proveito de terceiros»[24].

Permanecendo a responsabilidade penal, também permanece a capacidade de responder como arguida em processo penal[25]. Suscitam-se, porém, problemas de representação da pessoa colectiva extinta, para além dos já tratados *supra*. É que, neste caso, a pessoa colectiva deixa de ter legais representantes. GERMANO MARQUES DA SILVA sugeria anteriormente[26] a representação da pessoa colectiva por curador especial, nos

22. Acórdão do Tribunal da Relação de Évora, de 02.05.2006, Proc. 394/06-1 (Relator: Pires da Graça), disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/6cb25eb2f91cf80480257de1005748f1?OpenDocument (consulta em 05.10.2022).

23. SILVA, G.M, «A pessoa colectiva como arguida no processo penal», conferência proferida no âmbito do I Curso de Outono sobre Direito Penal das Pessoas Colectivas, FDL, Outubro de 2014, disponível em https://carlospintodeabreu.com/public/files/a_pessoa_colectiva_como_arguida_no_processo_penal.pdf (consulta em 05.10.2022), pág. 6.

24. SILVA, G.M., «Questões processuais na responsabilidade cumulativa das empresas e seus gestores», in MONTE, M.F. (et al.) (coord.), *Que futuro para o direito processual penal?: simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, Coimbra Editora, Coimbra, 2009, pág. 800.

25. SILVA, G.M, «Processo contra pessoas coletivas» in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág.473; SILVA, G.M., «Questões processuais da responsabilidade penal das pessoas colectivas» in PALMA, M.F./DIAS, A.S./MENDES, P.S. et al. (coord.), Estudos sobre *Law enforcement, compliace e direito penal*, Almedina, Coimbra, 2018, pág.167; SILVA, G.M., «A pessoa colectiva como arguida no processo penal», conferência proferida no âmbito do I Curso de Outono sobre Direito Penal das Pessoas Colectivas, FDL, Outubro de 2014, disponível em https://carlospintodeabreu.com/public/files/a_pessoa_colectiva_como_arguida_no_processo_penal.pdf (consulta em 05.10.2022), pág. 4.

26. SILVA, G.M, «Processo contra pessoas coletivas» in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág. 473; SILVA, G.M., «Questões processuais da responsabilidade penal das pessoas colectivas» in PALMA, M.F./

termos do art. 25.º, n.º 2, do CPC[27]. A Lei 94/2021, de 21 de Dezembro, veio agora preconizar a solução idêntica à da insolvência, mantendo-se os representantes à data da extinção, mas não resolve o problema da representação nos casos em que a própria responsabilidade penal se tenha extinguido, mas o processo deva continuar para efeitos de responsabilização subsidiária pelo pagamento de multas ou indemnizações, ou para efeitos da perda de bens – lacuna identificada por aquele autor[28].

Os representantes para efeitos do processo não se confundem com os representantes à data da prática do facto, nem com os agentes do facto punível colectivo, sendo os representantes actuais quem representa processualmente a pessoa colectiva arguida[29]. Por vezes, poderia coincidir a pessoa singular que também é arguida a título individual e cujos actos servem para imputar o crime à pessoa colectiva, mas é mera coincidência e não se confundem a identidade e posição processual das duas, pessoa colectiva e singular[30].

O art. 57.º, n.º 9, do CPP, na redacção dada pela Lei n.º 94/2021, de 21 de Dezembro, introduziu inclusivamente, para esta situação, um impedimento à representação: «[e] m caso algum a pessoa coletiva ou entidade equiparada arguida pode ser representada pela pessoa singular que também tenha a qualidade de arguido relativamente aos factos que são objeto do processo».

A imposição desta distinção tinha uma vantagem prática: facilitaria processualmente a distinção entre pessoa colectiva e pessoa singular.

DIAS, A.S./MENDES, P.S. et al. (coord.), Estudos sobre *Law enforcement, compliace e direito penal*, Almedina, Coimbra, 2018, pág. 167.

27. Artigo 25.º, n.º 2, do CPC «[s]endo demandada pessoa coletiva ou sociedade que não tenha quem a represente, ou ocorrendo conflito de interesses entre a ré e o seu representante, o juiz da causa designa representante especial, salvo se a lei estabelecer outra forma de assegurar a respetiva representação em juízo».

28. SILVA, G.M, «Responsabilidade penal das pessoas coletivas questões processuais», conferência proferida no Centro de Estudos Judiciários, 14.01.2022 (*texto gentilmente cedido pelo autor*), II.

29. Neste sentido, também já a Circular n.º 4/2011, da Procuradoria Geral da República, de 10 de Outubro, disponível em https://www.ministeriopublico.pt/iframe/circulares (consulta em 05.10.2022).

30. SILVA, G.M, «Processo contra pessoas coletivas» in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág. 468; SILVA, G.M., «Questões processuais da responsabilidade penal das pessoas colectivas» in PALMA, M.F./ DIAS, A.S./MENDES, P.S. et al. (coord.), Estudos sobre *Law enforcement, compliace e direito penal*, Almedina, Coimbra, 2018, pág. 158; SILVA, G.M.,«A pessoa colectiva como arguida no processo penal», conferência proferida no âmbito do I Curso de Outono sobre Direito Penal das Pessoas Colectivas, FDL, Outubro de 2014, disponível em https://carlospintodeabreu.com/public/files/a_pessoa_colectiva_como_arguida_no_processo_penal.pdf (consulta em 05.10.2022), pág. 9.

Com efeito, os actos processuais referentes à pessoa colectiva e à pessoa singular têm de ser praticados distintamente, mesmo quando o representante é também arguido em nome individual. E a sua falta pode ter importantes repercussões processuais, nomeadamente em matéria de presença na audiência e de prescrição. Por exemplo «I – As sociedades arguidas num processo devem prestar termo de identidade e residência nessa qualidade, não podendo considerar-se que esse termo é implicitamente prestado quando os legais representantes dessas sociedades, que são também arguidos no processo, prestam esse termo a título pessoal. II – A ausência dessa prestação e da subsequente notificação da acusação a tais sociedades configura uma irregularidade de conhecimento oficioso. […]»[31]. GERMANO MARQUES DA SILVA – com quem concordamos – defendia aliás que não estando a sociedade devidamente representada num acto processual, estaríamos perante uma nulidade insanável, prevista no art. 119.º, al. *c)*, do CPP, porquanto estamos perante um verdadeiro caso de «ausência do arguido»[32], não sendo aplicável o regime do art. 47.º do CPC que prevê a sanação da irregularidade de representação[33].

Além de facilitar processualmente a distinção entre pessoa colectiva e pessoa singular, a distinção entre o arguido pessoa singular e o representante da pessoa colectiva arguida poderá prevenir eventuais conflitos de interesse. Poderá, no entanto, questionar-se essa teria de ser sempre a solução legal, ou deveria ser aferida caso-a-caso. Evidentemente, quanto mais se promove o «direito premial» e a colaboração que poderá constituir, precisamente, em investigar internamente e fornecer provas de uma infracção cometida pelo seu representante, maior é o potencial de conflito entre a defesa da pessoa colectiva arguida e a dos seus representantes. No entanto, nem sempre assim o é e poderá existir conveniência numa defesa

31. Acórdão do Tribunal da Relação do Porto, de 4 de Junho de 2014, Processo 35/13.3IDPRT-A.P1 (Relator: Pedro Vaz Pato), disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/918f481107e1645980257cfc003ab3b9?OpenDocument (consulta em 05.10.2022).

32. Assim SILVA, G.M, «Processo contra pessoas coletivas» in ALBUQUERQUE, P.P./CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, págs. 470 e 471; SILVA, G.M., «Questões processuais da responsabilidade penal das pessoas colectivas» in PALMA, M.F./DIAS, A.S./MENDES, P.S. et al. (coord.), Estudos sobre *Law enforcement, compliace e direito penal*, Almedina, Coimbra, 2018, pág.161; SILVA, G.M., «A pessoa colectiva como arguida no processo penal», conferência proferida no âmbito do I Curso de Outono sobre Direito Penal das Pessoas Colectivas, FDL, Outubro de 2014, disponível em https://carlospintodeabreu.com/public/files/a_pessoa_colectiva_como_arguida_no_processo_penal.pdf (consulta em 05.10.2022), pág. 12.

33. Em sentido idêntico, ALBUQUERQUE, P.P., *Comentário do Código de Processo Penal*, 4.ª Ed., Universidade Católica Editora, Lisboa, 2011, anotação ao art. 57.º, n.º 15.

conjunta[34]. Em todo o caso, na verdade essa «defesa» conjunta não tinha sido vedada pela Lei n.º 94/2021, de 21 de Dezembro, já que a pessoa colectiva arguida e o representante arguido em nome individual podiam ser representados pelo mesmo defensor (que deverá analisar caso-a-caso se existe conflito que o impeça de o fazer).

A solução legal introduzida pela Lei n.º 94/2021, de 21 de Dezembro, com esta separação, foi objecto de críticas por GERMANO MARQUES DA SILVA[35], uma vez que existem casos em que o representante legal é precisamente o arguido pessoa singular, ficando sem se saber como seria representada a pessoa colectiva. Caso esta seja representada por alguém nomeado por aquele representante legal, também arguido pelo mesmo crime, pergunta-se o autor, e com razão, se a separação não poderá ser uma «falácia». «E se o representante legal, sendo também arguido, não nomear representante para a pessoa coletiva? E se se tratar se uma sociedade unipessoal em que o único sócio seja também coarguido no processo?» (algo que, tendo em conta o nosso tecido empresarial, não será raro). E no caso das entidades sem personalidade jurídica, se ninguém actuar como director, gerente ou administrador, e ninguém for escolhido pelos associados? Segundo o autor, a lei não responde a estas questões, e pareceria sugerir uma «solução bizarra»: a declaração de contumácia (solução que, tendo sido consagrada, afasta claramente a aplicação subsidiária do regime do art. 21.º do CPC onde se prevê para o réu ausente a nomeação de defensor oficioso). Solução que, segundo o autor, é até um convite, no caso das entidades sem personalidade jurídica, a não nomear alguém para evitarem responder eventualmente por multas e indemnizações nos termos do art. 11.º, n.º 11, do CP. Tratava-se claramente de um ponto para o qual era necessário encontrar solução.

Mais uma vez, o legislador parece ter ouvido o eco da crítica e, também logo na Lei n.º 13/2022, de 1 de Agosto, revogou a proibição constante do artigo 57.º, n.º 9, do CPP, deixando de vedar que o representante da pessoa colectiva seja aquele representante que tenha também a qualidade de arguido como pessoa singular.

Fica em aberto a possibilidade de, em caso de claro conflito de interesses, saber se é possível aplicar subsidiariamente as normas do processo

34. ANTUNES, M.J., «A pessoa coletiva arguida no processo penal. O que muda?», *RPCC*, núm. 31, 2021, pág. 6, refere mesmo que o «legislador quis obviar a uma situação potencial de defesas conflituantes, esquecendo, contudo, as vantagens que poderiam advir para a defesa da pessoa coletiva se fosse deixado ao seu critério a avaliação dos conflitos potenciais».

35. SILVA, G.M, «Responsabilidade penal das pessoas coletivas questões processuais», conferência proferida no Centro de Estudos Judiciários, 14.01.2022 (*texto gentilmente cedido pelo autor*), 2.2. (VII).

civil, *ex vi* art. 4.º do CPP, em concreto as que consagram a representação da pessoa colectiva por curador especial, nos termos do art. 25.º, n.º 2[36]: «[…] sendo demandada pessoa coletiva ou sociedade que não tenha quem a represente, ou ocorrendo conflito de interesses entre a ré e o seu representante, o juiz da causa designa representante especial, salvo se a lei estabelecer outra forma de assegurar a respetiva representação em juízo». Anteriormente à Lei n.º 94/2021, de 21 de Dezembro, TERESA QUINTELA DE BRITO sugerira até a adopção de uma solução idêntica à da Lei francesa, que permitiria ao representante da pessoa colectiva, em caso de conflito de interesses, solicitar a designação de um curador *ad litem* para a pessoa colectiva[37]. A falta de regulamentação desta situação na reforma operada pela Lei 94/2021, de 21 de Dezembro, suscita dúvidas sobre a aplicabilidade desta solução do direito subsidiário, em particular face às normas sobre a contumácia. Admitimos que talvez seja possível a aplicação subsidiária. Mas neste caso, tratar-se ia de uma nomeação oficiosa que, a nosso ver, só deveria ocorrer caso a pessoa colectiva, notificada para indicar novo representante para o processo em substituição do representante também imputado a título individual, não o viesse fazer.

3. DIREITO À NÃO AUTO-INCULPAÇÃO

GASCÓN INCHAUSTI[38] considera que o direito à não auto-inculpação da pessoa colectiva abrangerá as seguintes condutas: (i) recusa da pessoa colectiva, enquanto tal, em fornecer informações e documentos que lhe sejam solicitados e tenham natureza incriminatória; (ii) recusa de

36. A solução não é desconhecida em termos de direito comparado, prevendo o direito italiano a incompatibilidade de representação da pessoa jurídica por parte da pessoa física a quem é imputado o delito que está na base do facto colectivo (art. 39.º, n.º 1, do Decreto Legislativo n.º 231/2001). No direito francês não se prevê a incompatibilidade absoluta de posições, porém permite-se ao representante legal, quando imputado pelos mesmos factos ou por factos conexos, que requeira ao tribunal a designação de um curador especial (mandatário *ad litem*) para representar a pessoa jurídica (art. 706-43 do CPP francês). Cf. BRITO, T.Q., «Processo contra pessoas colectivas: algumas propostas de adaptação (urgente) do Código de Processo Penal português», in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág. 496.

37. BRITO, T.Q., «Processo contra pessoas colectivas: algumas propostas de adaptação (urgente) do Código de Processo Penal português», in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág. 498.

38. GASCÓN INCHAUSTI, F., «Los desafíos del proceso penal frente a personas jurídicas en la legislación y en la praxis española: representación y derecho a no autoincriminarse», *RPCC*, núm. 29, pág. 105.

certas pessoas ligadas à pessoa colectiva em fornecer tais informações e documentos; (iii) recusa de certas pessoas ligadas à pessoa colectiva em responder a questões de conteúdo incriminatório para a pessoa colectiva no contexto de uma investigação ou processo penal.

Quanto à dimensão declarativa, o direito da pessoa colectiva a estar presente e ser ouvida é exercido através do seu representante processual (art. 61.º, n.º 1, als. *a*) e *b*), e n.º 7, do CPP). A este caberá também exercer o direito ao silêncio que assiste à pessoa colectiva (cf. art. 61.º. n.º 1, al. *d*), do CPP) nos mesmos termos do que a pessoa física[39]. No entanto, *o âmbito de aplicação pessoal direito ao silêncio* (e à não auto-inculpação) da pessoa colectiva não pode esgotar-se na pessoa do representante pessoal, tendo um âmbito de aplicação pessoal mais amplo.

Imaginemos que o Ministério Público ou o Tribunal pretendem ouvir outros representantes legais da pessoa jurídica que não sejam o seu representante para o processo. Em que qualidade serão ouvidos? Poderão estes invocar também o direito da pessoa colectiva à não auto-inculpação e recusar a prestação de declarações? E se forem os representantes legais à data da prática do facto, por exemplo, ex-administradores, mas que já não são actualmente representantes legais?

Anteriormente à reforma legislativa operada, perguntava-se: os representantes legais que não fossem o representante processual seriam ouvidos como meras testemunhas, com dever de responder com verdade aos factos imputados à pessoa colectiva – art. 132.º, n.º 1, al. *d)*, CPP? E, nesse caso, poderiam invocar o art. 132.º, n.º 2, analogicamente, relativamente às respostas das quais possa resultar a responsabilização da pessoa colectiva? Ou teriam um direito de recusar o testemunho nos termos do art. 134.º do CPP, aplicado analogicamente? Ou mesmo um direito ao silêncio amplo como o ente colectivo arguido? E as regras seriam diferentes para quem tenha sido, mas já não seja actualmente, representante legal?

A alínea *e*), do n.º 1, do art. 133.º do CPP, introduzida pela Lei n.º 94/2021, de 21 de Dezembro, dispõe agora que não pode depor como testemunha «[o] representante da pessoa coletiva ou entidade equiparada no processo em que ela for arguida», e a nova al. *c*), do n.º 1, do art. 134.º, veio estabelecer um direito de recusa a depor para "[o] membro do órgão da pessoa coletiva ou da entidade equiparada que não é representante da mesma no processo em que ela seja arguida». Esta previsão abrangerá

39. DIAS, A.S./RAMOS, V.C., *O Direito à não auto-inculpação (nemo tenetur se ipsum accusare) no processo penal e contra-ordenacional português*, Coimbra Editora, Coimbra 2009, págs. 39-42, tratam, muito embora não desenvolvidamente, a questão da aplicação deste direito às pessoas colectivas, resolvendo-a no sentido afirmativo.

qualquer dos actuais membros dos órgãos da pessoa colectiva porque todos fazem parte da sua estrutura e por isso que as razões que justificam o poder de recusa a depor são também válidas para todos, como ensina GERMANO MARQUES DA SILVA[40]. Já antes da reforma, o autor – com quem concordamos – expressara a posição de que aos demais titulares (actuais) de órgãos da pessoa colectiva, que não o representante no processo, também era aplicável o direito ao silêncio da pessoa colectiva, no que respeita aos factos imputados à pessoa colectiva, não podendo assim ser ouvidos como testemunhas, o que decorreria do princípio da protecção contra a auto-inculpação, na ausência de norma expressa[41]. Assim, deveriam ficar impedidos de depor como testemunhas, através da inclusão no artigo 133.º do CPP[42].

A clarificação legislativa quanto a este ponto é de saudar. No entanto, não foi regulado o direito de uma forma ampla, mas apenas a dimensão declarativa, do direito ao silêncio. Por exemplo, não se alterou o artigo 14.º, n.º 5, da Lei 109/2009, de 15 de Setembro, quanto às pessoas colectivas,

40. SILVA, G.M, «Processo contra pessoas coletivas» in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, págs. 472 e 473; SILVA, G.M., «Questões processuais da responsabilidade penal das pessoas colectivas» in PALMA, M.F./ DIAS, A.S./MENDES, P.S. et al. (coord.), Estudos sobre *Law enforcement, compliace e direito penal*, Almedina, Coimbra, 2018, pág. 166; SILVA, G.M., «Responsabilidade penal das pessoas coletivas questões processuais», conferência proferida no Centro de Estudos Judiciários, 14.01.2022 (*texto gentilmente cedido pelo autor*), 5.2. (I).

41. Neste sentido, SILVA, G.M., «Questões processuais na responsabilidade cumulativa das empresas e seus gestores», in MONTE, M.F. (et al.) (coord.), *Que futuro para o direito processual penal?: simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, Coimbra Editora, Coimbra, 2009, pág. 800; 2014, pág. 17. MEIRELES, M.P., «A responsabilidade penal das pessoas colectivas ou entidades equiparadas na recente alteração ao Código Penal ditada pela Lei 59/2207, de 4 de Setembro: algumas notas», *JULGAR*, núm. 5, 2008, pág. 136, também concorda que não podem ser ouvidos como testemunhas, mas sugere uma alteração legal que o permite.

42. MEIRELES, M.P., «A responsabilidade penal das pessoas colectivas ou entidades equiparadas na recente alteração ao Código Penal ditada pela Lei 59/2207, de 4 de Setembro: algumas notas», *JULGAR*, núm. 5, 2008, pág. 136, argumentava inclusivamente que esse impedimento já decorreria das regras do CPC (art. 496.º que determina que estão impedidos de ser ouvidos como testemunhas aqueles que sejam parte no processo, norma que se aplica aos representantes legais da pessoa jurídica). Porém, existindo norma expressa sobre os impedimentos no CPP, tornava-se difícil admitir a existência de lacuna a integrar pelas normas do processo civil. Assim, TEIXEIRA, C.A., «A pessoa colectiva como sujeito processual; ou a "descontinuidade" processual da responsabilidade penal», *Revista do CEJ*, núm. 8 (especial), 2008, págs. 112-113, considerava que os administradores que não são os designados no processo como representantes poderão ser ouvidos como testemunhas desde que não sejam eles próprios suspeitos da prática de crime e sugeria o aditamento de impedimento ao art. 133.º do CPP.

neste âmbito (*v. infra*). E mesmo quanto à dimensão declarativa, a alteração legislativa não esclareceu todas as questões pertinentes quanto ao âmbito de aplicação pessoal do direito da pessoa colectiva à não auto-inculpação.

Ficaram, por exemplo, por regular a extensão deste aos antigos membros dos órgãos, às pessoas com posição de liderança que não sejam representantes, ou aos simples funcionários, ou pessoas que ajam por conta da sociedade.

GERMANO MARQUES DA SILVA[43] defende que, quanto aos antigos membros dos órgãos, estes não estão impedidos de depor como testemunhas, mas deveria ter-se reconhecido um direito de recusa a depor quanto a factos ocorridos durante o período em que tenham sido representantes da pessoa colectiva, análogo ao estabelecido na al. *b*), do n.º 1, do art. 134.º, do CPP, para os ex-cônjuges. Uma interpretação literal do regime actual levará a concluir que aqueles não estão abrangidos pelo direito ao silêncio e terão de depor com verdade, não podendo recusar-se a depor (a não ser que das repostas resulte a autoincriminação própria)[44].

De ressalvar que qualquer representante *actual ou anterior que seja arguido individualmente* no mesmo processo *está sempre impedido de responder como testemunha*, mas neste caso *por força do seu próprio direito à não auto-inculpação*, conforme decorre do artigo 133.º, n.º 1, al. *a*), do CPP. E, mesmo se já condenado, só poderia depor como testemunha se nisso consentisse. Cabendo ainda ao actual representante o direito de recusa a depor como decorrência do próprio direito ao silêncio da pessoa colectiva.

CARLOS ADÉRITO TEIXEIRA defende que as restantes pessoas com funções na pessoa colectiva (quadros técnicos, trabalhadores, etc.), não sendo representantes designados nem arguidos a título pessoal só poderão ser ouvidos como testemunhas, a não ser que fosse criada uma nova figura processual[45]. Assim, não podem recusar o testemunho. No entanto, nada impede que sejam designados como representantes processuais (ou até membros de órgãos da pessoa colectiva) e com isso passem a ficar impedidos de testemunha, ou a ter um direito de recusa de depoimento.

43. SILVA, G.M, «Responsabilidade penal das pessoas coletivas questões processuais», conferência proferida no Centro de Estudos Judiciários, 14.01.2022 (*texto gentilmente cedido pelo autor*), 5.2. (II).

44. Neste sentido, SILVA, G.M., «Questões processuais na responsabilidade cumulativa das empresas e seus gestores», in MONTE, M.F. (et al.) (coord.), *Que futuro para o direito processual penal?: simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, Coimbra Editora, Coimbra, 2009, pág. 800.

45. TEIXEIRA, C.A., «A pessoa colectiva como sujeito processual; ou a "descontinuidade" processual da responsabilidade penal», *Revista do CEJ*, núm. 8 (especial), 2008, pág. 112. No processo civil são ouvidos como testemunhas.

MÁRIO PEDRO MEIRELES considera que para obviar à manipulação processual por parte da pessoa colectiva, que poderia nomear como membros dos órgãos representativos pessoas que pretende impedir que prestem declarações como testemunhas, deveria fixar-se quem são os representantes, por exemplo no momento de prestação do Termo de Identidade e Residência[46]. CARLOS ADÉRITO TEIXEIRA refere que a substituição de representante no processo pode ser uma forma «airosa» de a pessoa colectiva evitar que as declarações prestadas valham como meio de prova, já que entende que se um representante se remeter ao silêncio não podem ser utilizadas as declarações anteriores, independentemente da qualidade em que foram recolhidas, igualmente, se um representante usar o silencio em audiência, não poderão ser utilizadas as declarações prestadas por outro em fase anterior[47]. Estes «problemas» não encontram de todo solução legal, não nos parecendo que exista qualquer impedimento ao círculo de potenciais representantes da pessoa colectiva, se estatutariamente e legalmente permitida a sua nomeação ou desingnação. Aliás, nada impede até que possa designar um terceiro externo para representante processual, se os estatutos o permitirem, com isso passando o mesmo a incluir-se no círculo daqueles impedidos de depor como testemunhas. Creio que são temas que deverão merecer uma maior reflexão.

Em Espanha, por exemplo, o art. 786 bis.1 da Ley de Enjuciamiento Criminal impede a nomeação de representante na fase de audiência daquele que tenha de prestar declarações em julgamento na qualidade de testemunha[48]. Como explica GASCÓN INCHAUSTI, esta regra está directamente relacionada com a possibilidade de o representante exercer o direito de permanecer em silêncio, parecendo que a mesma «se destina a evitar a fraude que consistiria em a pessoa colectiva acusada pode escapar a uma declaração incriminatória da testemunha através da nomeação de representante – com direito ao silêncio – da testemunha essencial da acusação» – que terá o dever de dizer a verdade. O autor alerta, todavia,

46. MEIRELES, M.P., «A responsabilidade penal das pessoas colectivas ou entidades equiparadas na recente alteração ao Código Penal ditada pela Lei 59/2207, de 4 de Setembro: algumas notas», *JULGAR*, núm. 5, 2008, págs. 135-136.
47. TEIXEIRA, C.A., «A pessoa colectiva como sujeito processual; ou a "descontinuidade" processual da responsabilidade penal», *Revista do CEJ*, núm. 8 (especial), 2008, pág. 112.
48. Cf. GASCÓN INCHAUSTI, F., «Los desafíos del proceso penal frente a personas jurídicas en la legislación y en la praxis española: representación y derecho a no autoincriminarse», *RPCC,* núm. 29, pág. 97; BRITO, T.Q., «Processo contra pessoas colectivas: algumas propostas de adaptação (urgente) do Código de Processo Penal português», in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág. 497, nota 90.

para os problemas derivados da referida norma: (i) o direito da pessoa colectiva a não se auto-inculpar-se pode ser prejudicado, uma vez que não haverá pessoa singular que tenha real possibilidade de o exercer em nome da pessoa colectiva; (ii) se aplicada extensivamente como incluindo qualquer pessoa que possa vir a ser testemunha, pode «privar a pessoa colectiva da possibilidade de ter um representante em quem tenha confiança suficiente e que tenha um certo conhecimento do processo penal, ambos factores que devem ser considerados necessários para o correcto exercício do direito de defesa». O autor propõe uma limitação implícita à norma a partir do tipo de factos sobre os quais a pessoa possa depor e a relação desta com a estrutura da pessoa colectiva. Neste ordenamento, a propósito das alterações do representante, o autor refere que as alterações pertencem à estratégia de defesa, poderão ser forçadas (morte do representante) ou convenientes (falta de confiança, desempenho no processo, etc.), não podendo ser recusadas, a não ser que se constate o seu carácter «abusivo ou fraudulento». Poderia esta limitação em casos de abuso de direito aplicar-se no regime português?

A solução há-de passar, como diz GASCÓN INCHAUSTI[49], por «encontrar um equilíbrio entre a violação do direito ao silêncio – que ocorreria se, em alguns casos, apenas ao representante fosse dado o poder de permanecer em silêncio – e a evasão à acção penal – que ocorreria no caso de uma extensão excessiva deste poder».

Na doutrina portuguesa, podemos salientar ainda as posições de TERESA QUINTELA DE BRITO e de MARIA JOÃO ANTUNES. A posição das autoras sobre o âmbito pessoal do direito ao silêncio da pessoa colectiva parte da distinção entre o *objecto* do depoimento, e não apenas da qualidade de representante da pessoa colectiva. TERESA QUINTELA DE BRITO defende que estão abrangidos por um impedimento de testemunhar todas as pessoas físicas intervenientes no facto colectivo, quanto aos factos de conexão por estas protagonizados e que condicionam a imputação de responsabilidade à pessoa colectiva, e ainda quanto aos factos internos da pessoa colectiva (*v.g.* actuação em nome e no interesse da pessoa colectiva, pessoa que ocupe posição de liderança, pessoa que age sob autoridade das pessoas que nela exerçam posição de liderança)[50]. Já

49. GASCÓN INCHAUSTI, F., «Los desafíos del proceso penal frente a personas jurídicas en la legislación y en la praxis española: representación y derecho a no autoincriminarse», *RPCC,* núm. 29, pág.114.

50. BRITO, T.Q., «Processo contra pessoas colectivas: algumas propostas de adaptação (urgente) do Código de Processo Penal português», in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, págs. 504-505.

MARIA JOÃO ANTUNES[51] sugeria a aplicação de um direito de recusa de testemunho para os dirigentes que não fossem arguidos individuais nem representantes da pessoa colectiva no processo, solução que veio a ser adoptada no artigo 134.º, n.º 1, al. *c)*, do CPP. Creio que a solução actualmente vigente é útil, no sentido de representar um primeiro passo para a aplicação e discussão jurisprudencial do tema do âmbito subjectivo do direito ao silêncio da pessoa colectiva. Mas parece-me que, tal como aponta TERESA QUINTELA DE BRITO, a solução adoptada não é inteiramente coincidente com aquilo que deve ser a tutela do direito à não auto-inculpação da pessoa colectiva, pelo que o tema deve continuar a ser objecto de discussão crítica.

Para além do âmbito pessoal da aplicação do direito à não auto-inculpação, existem questões relacionadas com o seu *âmbito material de aplicação*, nomeadamente saber se este abrange o direito a recusar entrega de documentos (aplicável às pessoas singulares), ou não. E se, inexistindo tal direito de recusa no âmbito de processo contra-ordenacional, mas existindo no processo penal, tais documentos, se obtidos no processo contra-ordenacional, poderão ser utilizados neste. Penso que o direito das pessoas colectivas será idêntico ao das pessoas singulares, não obstante já termos defendido uma limitação deste quanto aos documentos a cuja existência a lei obriga. MARIA JOÃO ANTUNES defende que a entrega ou a recusa de entrega de documentos referentes aos factos de conexão se factos internos da pessoa colectiva cabe apenas e só ao representante da pessoa colectiva no processo. No entanto, este direito de recusa de entrega não abrangerá documentos relevantes para a inculpação de um arguido pessoa singular[52]. TERESA QUINTELA DE BRITO defende que apenas assim será quando for possível autonomizar completamente estes factos daqueles da pessoa colectiva e que, em qualquer caso, a sua valoração deverá ficar sujeita a um regime «paralelo ao das declarações do co-arguido (artigos 343.º, n.º 4, e 345.º, n.º 4» do CPP[53].

O que nos parece maior problema será o que resulta *do cruzamento do problema do âmbito pessoal e material do direito à não auto-inculpação no seio de uma pessoa colectiva.* Por exemplo, a reforma não tocou no artigo 14.º, n.º 5, da Lei 109/2009, de 15 de Setembro. Assim, o mesmo preconiza que a

51. ANTUNES, M.J., *Processo Penal e pessoa colectiva arguida,* Almedina, Coimbra, 2020, pp. 65-72.

52. ANTUNES, M.J., *Processo Penal e pessoa colectiva arguida,* Almedina, Coimbra, 2020, pp. 66-67.

53. BRITO, T.Q., «Processo contra pessoas colectivas: algumas propostas de adaptação (urgente) do Código de Processo Penal português», in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, págs. 505.

injunção para apresentação ou concessão do acesso a «dados informáticos específicos e determinados, armazenados num determinado sistema informático», «não pode ser dirigida a suspeito ou arguido nesse processo». Pergunta-se: como opera esta proibição no seio de uma pessoa colectiva? Pode a injunção ser dirigida à mesma, posto que o seja a um funcionário (por ex., do departamento informático) que, de acordo com o que vimos *supra* não estará abrangido pelo direito ao silêncio da pessoa colectiva?

Afigurar-se-me que a resposta não será simples. E que não pode olvidar-se que, estando os dados na disposição desse funcionário, apenas o estão porque este está legitimado por força das respectivas funções. Assim, não poderá ser-lhe dirigida essa injunção, cominando a recusa com o crime de desobediência. O funcionário, se receber essa injunção, poderá encaminhar a mesma aos representantes da pessoa colectiva, podendo estes recusar-se a cumprir.

Neste sentido GASCÓN INCHAUSTI[54], face ao direito espanhol, refere que podem surgir problemas quando se solicitem os documentos ou informações a gestores que não sejam representantes, ou aos funcionários que estejam incumbidos de os guardar ou de com eles trabalhar. O autor nota que, apesar de parecer que a lei estabelece um dever geral de produzir objectos e documentos suspeitos de estarem relacionados com um processo penal (Art. 575 LECrim), deve entender-se que tal dever «só se aplica àqueles que são terceiros no sentido absoluto», pelo que «gestores e funcionários seriam, neste sentido, "possuidores em nome de outrem", de molde a afirmar-se que apenas os detêm "em nome e por conta da pessoa colectiva"». Em consonância, o autor considera razoável «entender que o direito da pessoa colectiva de recusar a entrega de documentos não pode ser contornado solicitando-os a título pessoal aos que com ela trabalham», que poderão assim recusar legitimamente a entrega. Aliás, o autor defende que se tais pessoas os entregarem voluntariamente poderá estar em causa uma aquisição de prova ilícita, pois estaríamos perante uma violação do direito à não auto-inculpação que a empresa ficaria impedida de exercer (ao contrário do que se passaria se estivessem na posse de terceiros com quem tenham contratado para o efeito).

MARIA JOÃO ANTUNES[55] defende que as pessoas com posição de liderança que não representem a pessoa colectiva no processo e aquelas

54. GASCÓN INCHAUSTI, F., «Los desafíos del proceso penal frente a personas jurídicas en la legislación y en la praxis española: representación y derecho a no autoincriminarse», *RPCC,* núm. 29, pág. 106.

55. ANTUNES, M.J., *Processo Penal e pessoa colectiva arguida,* Almedina, Coimbra, 2020, pp. 66-67.

que, não ocupando tal posição, detenham meios de prova em nome e por conta da pessoa colectiva, devem poder recusar-se a entregá-los. Só assim poderá garantir-se o direito à não auto-inculpação da pessoa colectiva. De outra forma, privar-se-ia a pessoa colectiva arguida «direito de decidir sobre a entrega no processo de determinado meio de prova». Evidentemente, tal não preclude a obtenção coerciva de tal documentação através de buscas e apreensões[56].

Menos clara já será a situação em que no âmbito de uma diligência de busca nas instalações da pessoa colectiva seja solicitada colaboração ao referido funcionário para pesquisa no sistema informático, por exemplo fornecendo uma chave criptográfica, ou uma palavra-passe. Por um lado, este estará a fornecer dados que não lhe pertencem e aos quais só acede pelas funções que exerce, sem autorização para tal. Parece-me que, por este motivo, valem as posições de MARIA JOÃO ANTUNES e de TERESA QUINTELA DE BRITO, conferindo o poder de decidir sobre a entrega de tal elemento ao representante. Por outro lado, se uma autoridade judicial ordenou a referida busca, sendo o funcionário potencialmente uma testemunha, deverá na mesma colaborar e o não fornecimento de tais dados poderá implicar a inutilidade da diligência. A solução deve ser objecto de reflexão e ponderação, pois, a aceitar-se a imposição da obrigação de fornecimento de tais chaves, creio que estaremos perante uma solução restritiva do direito à auto-inculpação da pessoa colectiva que, para passar o crivo da constitucionalidade (e conformidade com os instrumentos internacionais e de direito da UE aplicáveis), tem de ser considerada restrição proporcional e que não afecte a própria essência do direito à não auto-inculpação da pessoa colectiva arguida.

Qualquer que seja a solução, creio que não deve, todavia, colocar-se demasiado o acento tónico nas obrigações de colaboração a incidir sobre as empresas ou seus empregados. Isto porque essas obrigações dificilmente levarão à obtenção de prova fiável nos casos de verdadeiras fraudes ou intenções criminosas (onde, *maxime*, pode haver uma colaboração enganosa, fornecendo elementos não fiáveis). Nestes casos não há como obviar à necessidade de usar de buscas ou pesquisas informáticas em que as autoridades estejam preparadas para actuar sem a colaboração da pessoa colectiva e dos seus empregados e representantes ou dirigentes. Melhor

56. BRITO, T.Q., «Processo contra pessoas colectivas: algumas propostas de adaptação (urgente) do Código de Processo Penal português», in ALBUQUERQUE, P.P./ CARDOSO, R./MOURA, S. (org.), *Corrupção em Portugal. Avaliação legislativa e propostas de reforma,* Universidade Católica Editora, Lisboa, pág. 505, exprime a sua concordância com esta posição.

incentivo à obtenção de prova fiável será possivelmente a consagração de um regime premial atractivo para a empresa, tornando maioritariamente vantajosa a adopção de uma conduta de colaboração voluntária e superando assim os obstáculos na obtenção da prova, com as devidas cautelas.

CONCLUSÃO

A Lei 94/2021, de 21 de Dezembro, fez finalmente face a alguns desafios em matéria de direitos de defesa das pessoas colectivas. No entanto, não resolveu todos os problemas e permanecem várias dúvidas quanto às normas aplicáveis, que urge resolver. Sobretudo, é necessário pensar até que ponto um processo penal contra uma pessoa colectiva implica um diferente paradigma quanto ao próprio papel da defesa e às suas interacções com o processo.

Subsistem também outros problemas, a impor reflexão e regulação. Damos apenas a título de exemplo a matéria das investigações internas. Trata-se de um campo não regulado em Portugal, não podendo excluir-se que uma visão mais anacrónica e formal, contraditória com as exigências de *compliance* decorrentes de várias normas que regulam a actividade empresarial, as considere até se inclusivamente uma interferência com o inquérito ou a instrução, no sentido da aquisição e produção da prova. Parecer ser desejável do ponto de vista da comunidade que as empresas investiguem internamente uma possível infracção, até para tomarem medidas para a prevenir no futuro (e depois, se o entenderem, utilizem o produto dessa investigação para a sua defesa). Dizer o contrário parece-me algo desfasado da realidade. No entanto, por outra perspectiva, esta permissão também gera problemas de possível desigualdade quanto a arguidos individuais que estão privados de fazer a "sua" investigação e de a veicular nos autos de forma processualmente relevante, sem temerem ser alvo de censura por perturbação da aquisição probatória. Por outra perspectiva, discute-se actualemnte na Europa até que ponto as investigações internas das empresas podem se introduzidas em processo contra a vontade da própria pessoa colectiva e como deve conjugar-se essa permissão ou proibição com o regime do segredo profissional quando efectuadas por Avogados[57]. Matéria a estudar e aprofundar.

57. Cf. BERT, P., «Case of the Week: Federal Constitutional Court Allows Search of Jones Day's Offices in Volkswagen Case», *Dispute Resolution Germany*, 06.07.2018, https://www.disputeresolutiongermany.com/2018/07/case-of-the-week-federal-constitutional-court-allows-search-of-jones-days-offices-in-volkswagen-case/ (consulta em 05.10.2022).

V
Victimización y nuevas tecnologías

Capítulo 14

Víctimas de trata de seres humanos, investigación del delito y nuevas tecnologías*

Andrea Planchadell-Gargallo

Catedrática de Derecho Procesal
Universitat Jaume I, Castellón

I. INTRODUCCIÓN

En estas páginas se pretende hacer un breve repaso de la influencia de las nuevas tecnologías en la investigación de los delitos de trata, si la hay y en qué sentido. Las posibilidades y facilidades que las nuevas tecnologías suponen ha propiciado que las organizaciones criminales y los delincuentes, en general, se aprovechen de ellas para fortalecer sus actividades delictivas, lo que es evidente en figuras como el narcotráfico, la trata de personas, la explotación sexual o la pornografía infantil. Es decir, las nuevas tecnologías se integran en el *modus operandi* de esta delincuencia, por lo que también debe integrarse en las actividades preventivas[1], de

* Este capítulo se enmarca dentro del Proyecto de Investigación *Trata de seres humanos y esclavitud: Investigación, enjuiciamiento y protección procesal de las víctimas (Código: RTI2018-094686-B-C22)*, financiado por el Ministerio de Economía y competitividad – Modalidad 1: Proyectos de I+D+I del Programa estatal de investigación, desarrollo e innovación orientada los retos de la sociedad, del que soy Investigadora Principal.

1. Desde una perspectiva preventiva, por ejemplo, la OSCE (*Organization for Security and Co-operation in Europe*) y Tech Against Trafficking han analizado 305 instrumentos, financiados mínimamente por los gobiernos o por ONGs, como por ejemplo la empresa francesa Ecovadis, que ofrece a las empresas un sistema de evaluación de su responsabilidad social (RSE), para verificar, por ejemplo, que ningún niño sea explotado por los subcontratistas de una empresa multinacional. Otra herramienta identificada en el informe es la web *Slavery From Space*, desarrollada por la Universidad de Nottingham, cuyo objetivo es identificar, mediante imágenes satélites, los hornos de ladrillo de Asia del sur, sobre todo de la India, en que se realiza trabajo forzoso.

persecución y de enjuiciamiento de las autoridades si no quieren fomentar espacios de impunidad, pues las nuevas tecnologías permiten captar un mayor número de personas de una forma más rápida, por ejemplo, al eliminar la interacción "cara a cara"[2].

Sin perjuicio de la trascendencia del Protocolo de Palermo (Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional de 2003), primer instrumento internacional que atiende a la protección integral de la trata, el art. 4 del Convenio de Varsovia (Convenio núm. 197, del Consejo de Europa hecho en Varsovia el 16 de mayo de 2005, con entrada en vigor en España el 1 de agosto de 2009) define la trata como "el reclutamiento, transporte, transferencia, alojamiento o recepción de personas, recurriendo a la amenaza o uso de la fuerza u otras formas de coerción, el secuestro el fraude, engaño, abuso de superioridad o de otra situación de vulnerabilidad, o el ofrecimiento o aceptación de pagos o ventajas para obtener el consentimiento de una persona que tenga autoridad sobre otra, con vistas a su explotación. La explotación comprenderá, como mínimo, la explotación de la prostitución de otras personas u otras formas de explotación sexual, el trabajo o los servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre o la extirpación de órganos"[3]. En definitiva, se trata de captar, transportar, trasladar, acoger o recibir personas empleando determinados medios con la finalidad de explotación, sin añadirle calificativo, y aunque ésta no llegue a producirse. La Directiva 2011/36/UE del Parlamento europeo y del Consejo de 5 abril de 2011, relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas y por la que se sustituye la Decisión marco 2002/629/JAI del Consejo[4], no contiene una definición expresa de trata, si bien –de forma

2. El informe de Europol "*Criminal networks involved in the trafficking and exploitation of underage victims in the European Union*" (The Hague: Europol, 18 October 2018), p. 7, ya constataba que las organizaciones criminales implicadas en el tráfico y explotación de víctimas menores de edad en la Unión Europea estaban incrementando de forma preocupante la utilización de los anuncios online de servicios sexuales con menores haciéndose pasar por adultos.

3. Importante se considera por VILLACAMPA ESTIARTE, C., y TORRES ROSELL, N., "Trata de seres humanos para explotación criminal: Ausencia de identificación de las víctimas y sus efectos", *Revista de Estudios Penales y criminológicos* 2016, núm. 36, p. 774, la referencia que se introduce en la Directiva 2011 respecto a "explotar a la víctima en alguna actividad que produzca un beneficio económico…".

4. Junto con esta Decisión Marco, cabe citar también –sin ánimo de exhaustividad– el Plan de la UE sobre mejores prácticas, normas y procedimientos para luchar contra la trata de seres humanos y prevenirla o el Programa de Estocolmo "Una Europa abierta al ciudadano", en que se reconoce la lucha contra la trata de seres humanos como una prioridad del Consejo de Europa. A estas normas, entre otras más centradas en el

similar– en su art. 2 se definen las conductas que englobarían dicho concepto, concretamente "La captación, el transporte, el traslado, la acogida o la recepción de personas, incluido el intercambio o la transferencia de control sobre estas personas, mediante la amenaza o el uso de la fuerza u otras formas de coacción, el rapto, el fraude, el engaño, el abuso de poder o de una situación de vulnerabilidad, o mediante la entrega o recepción de pagos o beneficios para lograr el consentimiento de una persona que posea el control sobre otra persona, con el fin de explotarla". Común a las definiciones que encontramos en estos documentos es la consideración de la trata como una "moderna forma de esclavitud"[5].

II. LA NECESIDAD DEL ENFOQUE VICTIMOCÉNTRICO Y LA VULNERABILIDAD DE LA VÍCTIMA DE TRATA

El estudio de cualquier aspecto relacionado con la trata de seres humanos, en cualquiera de sus modalidades de explotación, exige hoy un enfoque en que la víctima se sitúe en el centro de interés. Esta aproximación tuitiva obliga a hacer una somera referencia a la importancia que, para la adecuada protección de la víctima de trata, supone la necesidad de este enfoque victimocéntrico[6]. Así, documentos internacionales y regionales sobre la trata, como los citados Protocolo de Palermo, Convenio de

ámbito migratorio o laboral, debe añadirse el Convenio del Consejo de Europa sobre la lucha contra la trata de seres humanos de 2005 y su creación del Grupo de Expertos en la lucha contra la trata de seres humanos (GRETA).

5. VILLACAMPA ESTIARTE, C., "El delito de trata de personas: Análisis del nuevo artículo 177 bis CP desde la óptica del cumplimiento de compromisos internacionales de incriminación", *Anuario de la Facultade de Direito da Universidad da Coruña-AFDCUDC* 2010, p. 824; PÉREZ ALONSO, E., "Marco normativo y política criminal contra la trata de seres humanos en la Unión Europea", en PÉREZ ALONSO, E. y POMARES CINTAS, E., *La trata de seres humanos en el contexto penal iberoamericano*, Tirant lo Blanch, Valencia, 2019, p. 64, se refiere a un "… viejo fenómeno que aparece disfrazado bajo nuevas formas y métodos…".

   El TEDH ya desde su Sentencia núm. 25965/04, de 7 de enero de 2010, *caso Rantsev contra Chipre y Rusia* entiende que el art. 4 del CEDH (prohibición de la esclavitud) ofrece protección frente a la trata. Pese a ello, como afirma Mestre i Mestre esta resolución "sigue siendo paradigmática porque desde su adopción han llegado pocos casos ante el TEDH…", v., MESTRE I MESTRE, R., "La jurisprudencia del TEDH en materia de trata de seres humanos y la necesidad de regresar a las categorías jurídicas de esclavitud, servidumbre y trabajo forzado", *Revista del Laboratorio Iberoamericano para el Estudio Sociohistórico de las Sexualidades* (https://doi.org/10.46661/relies.5187), pp. 1 y ss.

6. V., también, nuestros trabajos "Protección procesal de las víctimas de trata: Aproximación general"; *Revista de Derecho y Proceso Penal 2021*, núm. 61, pp. 39; "La protección procesal de las víctimas de trata: Panorama europeo", en LLORENTE ARJONA, M., (Dir.), *Estudios procesales sobre el espacio europeo de justicia penal*, Tirant lo Blanch, Valencia, 2021, pp. 117 y ss.

Varsovia, o la Directiva de 2011 afrontan el tratamiento de este fenómeno centrándose en la víctima del delito, lo que marca un punto de inflexión en su protección y tratamiento, en tanto que se considera que la trata supone una vulneración de los derechos humanos de la víctima y un atentado a la dignidad humana, por la cosificación que de la persona supone[7]. Como indica Villacampa estamos ante un "cambio de paradigma"[8] que traslada el centro de atención de la incriminación de las conductas a la protección de la víctima, suponiendo un tratamiento integral "más holístico, orientándonos a la protección y reconocimiento de los derechos de la víctima"[9].

Este enfoque se manifiesta a través llamadas "tres P" a que se refiere el Protocolo de Palermo: Prevención, protección y persecución[10]; siendo clave, además, que la protección de la víctima antes, durante y después de la celebración del proceso no dependa de que colabore o no en el mismo, sino de su propia condición de víctima, lo que obliga a la adecuada

7. De hecho, el art. 1 del Convenio de Varsovia, establece como uno de sus objetivos "proteger los derechos humanos de las víctimas…" (art. 1, b). De igual forma, el Considerando 11 de la Directiva de 2011 se refiere a la trata como "una grave violación de la dignidad humana y de la integridad física". A nivel nacional, dicho enfoque es evidente en el Protocolo Marco de Protección de Víctimas de trata de seres humanos. V.: OBAKTA, T., "Trafficking of human beings as a crime against humanity: Some implications for the international legal system", *The International and Comparative Law Quaterly*, April 2005, núm. 54, p. 448; PÉREZ ALONSO, E., "Marco normativo y política criminal contra la trata de seres humanos en la Unión Europea", en PÉREZ ALONSO, E., y POMARES CINTA, E., *La trata de seres humanos en el contexto penal iberoamericano*, *cit*., pp. 63 y 95. Así, la S TS núm. 307/2021, de 9 de abril (RJ 1514): "Como dice la STS 214/2017, de 29 de marzo, la mecánica delictiva propia de la trata de seres humanos con destino a la explotación sexual, cosifica a las mujeres víctimas y las humilla y veja con toda clase de maltratos, incluida la violencia, la agresión sexual y, si llega a plantearse, el aborto forzado".

8. VILLACAMPA ESTIARTE, C., "Víctimas de trata de seres humanos: Su tutela a la luz de las últimas reformas penales sustantivas y procesales proyectadas", *InDret* 2/2014, p. 3.

9. VILLACAMPA ESTIARTE, C., "La nueva Directiva Europea relativa a la prevención y a la lucha contra la trata de seres humanos y a la protección de la víctima ¿Cambio de rumbo de la política de la Unión en materia de trata de seres humanos?", *Revista Electrónica de Ciencia Penal y Criminológica* 2011, (13-14), 14: 2); IDEM, *El delito de trata de seres humanos. Una incriminación dictada desde el Derecho Internacional*, Aranzadi, Cizur Menor (Navarra), 2011, pp. 145 y ss., quien afirma que dicho enfoque "despliega toda su gama cromática en el conjunto de derechos y facultades previstos para la víctima de este tipo de delito", p. 188; TORRES ROSELL, N., y VILLACAMPA ESTIARTE, C., "Protección jurídica y asistencia para víctimas de trata de seres humanos", *Revista General de Derecho Penal* 2017, núm. 27, p. 2. En igual sentido, LLORIA GARCÍA, P., "El delito de trata de seres humanos y la necesidad de creación de una ley integral", *Estudios penales y criminológicos* 2019, pp. 353 y ss.

10. VILLACAMPA ESTIARTE, C., "Víctimas de trata de seres humanos: Su tutela a la luz de las últimas reformas penales sustantivas y procesales proyectadas", *InDret* 2/2014, pp. 4 y ss.

identificación de la misma como tal (art. 27 del Convenio de Varsovia y art. 9 de la Directiva de 2011)[11]. Identificación, que no siempre resulta una tarea sencilla[12].

A estas consideraciones previas, debemos añadir la vulnerabilidad consustancial a la víctima de trata[13], consecuencia de su propia condición y de las particularidades del delito que la victimiza. Estamos ante víctimas que se encuentran, generalmente, en situación ilegal, que frecuentemente

11. Puede consultarse la Sentencia del TEDH núm. n.º 71545/12, de 21 de enero de 2016, *caso L.E contra Grecia.* Al respecto puede verse también los diversos informes de GRETA, particularmente el 2.º y 4.º; AAVV.: *Guía de criterios de actuación judicial frente a la trata de seres humanos*, Consejo General del Poder Judicial, Madrid, 2018, p. 51; FERNÁNDEZ OLALLA, P., "La colaboración de la víctima en la investigación del delito de trata de seres humanos. Valoración de la colaboración de la víctima en el ámbito administrativo y penal", *Revista Aranzadi Doctrinal* 2014, núm. 9, *passim*.

    En la temprana identificación y la necesidad de protección de las victimas de trata sigue incidiendo el Plan Estratégico Nacional contra la Trata y la Explotación de Seres Humanos, del Ministerio del Interior, para los años 2021 a 2023 (se puede consultar en: http://www.interior.gob.es/documents/10180/12745481/220112_Plan_nacional_TSH_+PENTRA_FINAL_2021_2023/3f5c859a-69ef-40f8-a0b6-2a2b316f853d).

12. El art. 10 del Convenio de Varsovia establece la necesaria identificación de la víctima (art. 10) en el capítulo dedicado a las medidas para proteger y promover los derechos de las víctimas, destacando al respecto la necesaria formación y especialización de las personas involucradas en la prevención y lucha contra la trata de seres humanos. Sobre estas dificultades, puede consultarse VILLACAMPA ESTIARTE, C., y TORRES ROSELL, N., "Mujeres víctimas de trata en prisión en España", *Revista de Derecho Penal y Criminología* 2012, núm. 8, pp. 411 y ss., también publicado en inglés en el *European Journal of Criminal Policy and Research* 2014, vol. 20, núm. 1; FARALDO CABANA, P., "¿Dónde están las víctimas de trata de personas? Obstáculos a la identificación de las víctimas de trata en España", en MIRANDA RODRÍGUEZ (Coord.): *Livro de Atas. Conferencia internacional 18 de octubre. Día europeo contra o trafico de seres humanos*, U. de Coimbra, Coimbra, 2017, pp. 140 y ss. De estas dificultades se hacía ya eco el Informe Greta correspondiente al año 2019, particularmente en el caso de menores de edad; de hecho, nuestro país se encuentra entre los 45 países a los que desde esta institución se les "urge parcialmente" a mejorar la identificación de las víctimas de trata (https://rm.coe.int/9th-general-report-on-the-activities-of-greta-covering-the-period-from/16809e169e, pp. 50 a 54); preocupación general por la identificación que se reproduce en informes posteriores.

    Precisamente, las SS AP de Valencia núm. 390/2018, de 21 de junio (JUR 2018, 204231) y AP de Madrid núm. 63/2021, de 13 de enero (JUR 2021, 152066), exponen cómo a través de perfiles de Facebook una víctima pudo identificar a otras potenciales víctimas de trata, que habían estado en la misma casa de citas que ella, así como la propia identificación de investigado. El 11.º Informe Greta correspondiente al año 2021, p. 50, pone de relieve la importancia de los medios tecnológicos y la inteligencia artificial para la identificación de las víctimas, en especial de menores, por ejemplo, a través de mecanismos de reconocimiento facial.

13. PLANCHADELL GARGALLO, A., "Protección procesal de las víctimas de trata: Aproximación general", *Revista de Derecho y Proceso Penal* 2021, núm. 61, pp. 41 a 42; GÓMEZ COLOMER, J. L.: "Víctimas de trata: Declaraciones y protección en el proceso penal", *Revista de Derecho y Proceso Penal* 2021, núm. 64, pp. 2 y ss.

viven bajo unas condiciones económicas precarias, posiblemente padeciendo una cierta marginación social, muy vulnerables sentimental y emocionalmente, en no pocas ocasiones con una formación deficiente, etc.[14]. La Directiva de 2011, en su art. 2.2 indica expresamente que esta situación de vulnerabilidad concurre además "cuando la persona en cuestión no tiene otra alternativa real o aceptable excepto someterse al abuso". La necesaria adecuación a la situación de vulnerabilidad de la víctima figura como uno de los ejes centrales del reciente Plan Estratégico Nacional contra la Trata y la Explotación de Seres Humanos, del Ministerio del Interior, para los años 2021 a 2023.

Pues bien, todas estas circunstancias deben ser tomadas en consideración cuando se investiga y enjuicia el delito de trata, en cualquiera de sus manifestaciones, con o sin utilización de las nuevas tecnologías. Necesidad que se apunta claramente en el art. 1 del Convenio de Varsovia (art. 1.1, b): "proteger los derechos de la persona de las víctimas de la trata, crear un marco completo de protección y de asistencia a las víctimas y los testigos, garantizando la igualdad entre las mujeres y los hombres, así como garantizar una investigación y unas acciones judiciales eficaces").

III. BREVE REFERENCIA LAS NUEVAS TECNOLOGÍAS Y LOS ELEMENTOS DEL TIPO PENAL

Si bien no es nuestra intención llevar a cabo un estudio sustantivo de esta figura delictiva, si consideramos oportuno, partiendo de las aportaciones de la doctrina y de la jurisprudencia[15], así como de los documentos internacionales citados previamente, hacer una referencia a aquellos elementos del tipo penal en que las nuevas tecnologías pueden jugar un papel relevante.

14. S AP de Barcelona núm. 183/2020, de 22 de junio (ARP 2020, 1507).

15. MARTÍN ANCÍN, F., *La trata de seres humanos con fines de explotación sexual en el Código Penal de 2020. Aportaciones de la Ley Orgánica 1/2015*, Ed. Tirant lo Blanch y Universidad de Salamanca, Valencia, 2017; PÉREZ ALONSO, E., y POMARES CINTAS, E. (Coord.), *La trata de seres humanos en el contexto penal iberoamericano*, Ed. Tirant lo Blanch, Valencia, 2019, pp. 451 y ss. VILLACAMPA ESTIARTE, C., "El delito de trata de personas: análisis del nuevo artículo 177 bis CP desde la óptica del cumplimiento de compromisos internacionales de incriminación", *Anuario da Facultade de Dereito da Universidade da Coruña (AFDUDC)* 2010, núm. 14; IDEM., *El delito de trata de seres humanos. Una incriminación dictada desde el Derecho Internacional*, Ed. Aranzadi, Cizur Menor, 2011; VILLACAMPA ESTIARTE, C., y PLANCHADELL GARGALLO, A., *La trata de seres humanos tras un decenio de su incriminación. ¿Es necesaria una ley integral para luchar contra la trata y la explotación de seres humanos?*, Tirant lo Blanch, Valencia 2022; LLORIA GARCÍA, P., "El delito de trata de seres humanos y la necesidad de creación de una ley integral", *Estudios penales y criminológicos* 2019.

Partiendo de nuestro texto sustantivo (art. 117 bis CP), el delito de trata se puede desgranar en los siguientes elementos: Las conductas concretas que lo caracterizan, los medios utilizados para su comisión y los fines con los que se comete:

1.– Las conductas se refieren a captar, transportar, trasladar, acoger o recibir, incluyendo el intercambio o transferencia de control sobre las personas. Estas conductas se podrán realizar sobre nacionales o extranjeros;

2.– En cuanto a los medios, el Código se refiere al empleo de violencia, intimidación o engaño, o el abuso de una situación de superioridad, de necesidad o de vulnerabilidad de la víctima (nacional o extranjera)[16]; o la entrega o recepción de pagos o beneficios para lograr el consentimiento de la persona que poseyera el control sobre la víctima;

3.– Con alguna de las siguientes finalidades:

a) La imposición de trabajo o de servicios forzados, la esclavitud o prácticas similares a la esclavitud, a la servidumbre o a la mendicidad.

b) La explotación sexual, incluyendo la pornografía.

c) La explotación para realizar actividades delictivas.

d) La extracción de sus órganos corporales.

e) La celebración de matrimonios forzados.

4.– Presenta por último un componente territorial: Sea en territorio español, sea desde España, en tránsito o con destino a ella.

5.– Cuando se trate de menores de edad, se entenderá que concurre el tipo penal cuando se realice alguna de las conductas indicadas aún cuando no se recurra a ninguno de los medios comisivos expuestos.

El aspecto en que las nuevas tecnologías están presentando mayor influencia es en una de las acciones típicas indicadas, concretamente, en la captación de las víctimas y en su control[17]. La tecnología aparece, así, como

16. Existe una situación de necesidad o vulnerabilidad cuando la persona en cuestión no tiene otra alternativa, real o aceptable, que someterse al abuso.

17. LAFONT NICUESA, L., "Aspectos represivos, procesales y de protección que una futura ley integral de trata debiera abordar", en VILLACAMPA ESTIARTE, C., y PLANCHADELL GARGALLO, A., *La trata de seres humanos tras un decenio de su incriminación. ¿Es necesaria una ley integral para luchar contra la trata y la explotación de seres humanos?*, Tirant lo Blanch, Valencia 2022, p. 75. Este dato se destaca también por el 11.º Informe Greta, p. 40. Así se reconoce por la S AP Madrid núm. 471/2020, de 27 noviembre (ARP 2020, 397) o AP Guadalajara núm. 17/2020, de 13 octubre (JUR 2020, 346424).

un instrumento altamente eficaz para "captar o enganchar" a las víctimas a la servidumbre que, en sus distintas formas, supone la trata. Esta forma de captación es especialmente preocupante si pensamos en la dependencia que muchos de nuestros jóvenes tienen de las redes sociales; redes que, en estos casos, se utilizan precisamente con estos fines. Las nuevas tecnologías e internet permiten a los tratantes "cazar más activamente", con mayor precisión y con menos esfuerzo a las potenciales víctimas[18]. Además, les da la posibilidad de ofrecer nuevos productos o cambiar su acción física por actuaciones virtuales, como los actos sexuales en directo (*cybersex trafficking*), prescindir de los burdeles físicos[19], etc. También las nuevas tecnologías irrumpen de forma clara en las propias finalidades de la explotación, por ejemplo, venta por internet de la virginidad de menores de edad o de órganos a través de la *Dark Web*, que también se utiliza para conseguir la documentación falsa que permite el traslado de las víctimas.

La Organización Internacional contra la Esclavitud Moderna (*OICEM*) ha indicado, repetidamente en sus informes, que las nuevas tecnologías son uno de los instrumentos utilizados en el ámbito de la trata de persona por quienes se dedican a esta actividad. Si bien el uso de Facebook sigue siendo frecuente y relativamente rudimentario, los traficantes van mucho más allá en su uso de las tecnologías, publicando, por ejemplo, falsos anuncios de trabajo para atraer a jóvenes que desean irse al extranjero, realizan transacciones a través de criptomonedas, recurren al GPS para hacer un seguimiento en tiempo real de las personas que explotan, etc.[20].

La Resolución del Parlamento Europeo, de 10 de febrero de 2021, sobre aplicación de la Directiva 2011/36[21], haciéndose eco de la información

---

V., también, a modo de ejemplo, https://www.escudodigital.com/internacional/trata-personas-crecimiento_51016_102.html; https://elpais.com/sociedad/2022-01-16/captadas-en-redes-sociales-controladas-por-el-movil-vendidas-en-internet.html.

18. En el Informe Global sobre tráfico de personas de la ONU se pone de manifiesto cómo los llamados *loverboys* ahora utilizan los *likes* de las redes sociales para embaucar y captar a las víctimas (https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf).

19. Llaman poderosa y escalofriantemente la atención estos titulares o frases en noticias escritas: "Los nuevos burdeles ya no necesitan de neones para que todo el mundo los vea", "Pasion.com se cuela entre las 50 páginas más vistas de España, justo detrás de Netflix y por encima de las webs RTVE o Carrefour" (https://elpais.com/sociedad/2022-01-16/captadas-en-redes-sociales-controladas-por-el-movil-vendidas-en-internet.html).

20. En igual sentido, se pronuncia el informe de 22 de junio de 2020 de la Organización para la Seguridad y la Cooperación en Europa (OSCE) y por *Tech Against Trafficking* (grupo que a Amazon, Microsoft y AT&T), disponible en https://www.osce.org/files/f/documents/9/6/455206_1.pdf.

21. https://www.europarl.europa.eu/doceo/document/A-9-2021-0011_ES.html.

facilitada por Europol[22], pone de manifiesto que el uso de las tecnologías "ha ampliado la capacidad de los delincuentes para traficar con seres humanos y que se aprovecha en todas las fases, ya sea en la captación y explotación de las víctimas, hasta en el chantaje y control de sus movimientos"; a ello, añade, que ofrecen mayor anonimato. Ahora bien, en el mismo documento se indica que estas tecnologías no sólo ofrecen mayores oportunidades para los delincuentes, sino también para las víctimas y para las autoridades, policiales y judiciales.

IV. NUEVAS TECNOLOGÍAS Y LUCHA PROCESAL CONTRA LA TRATA DE PERSONAS

Si bien el delito de trata, actualmente, no se investiga ni enjuicia a través de un proceso especial al efecto, ni tampoco contempla, legalmente, especialidades concretas que le sean aplicables, lo cierto es que la investigación y enjuiciamiento del delito presenta particularidades concretas que conllevan la conveniencia y utilidad de servirse de determinados medios de investigación y de prueba. Siendo este evidente en el caso de la comisión del delito de "forma tradicional", lo es más aún cuando se utilizan para su comisión nuevas tecnologías, en el sentido indicado en el punto anterior.

1. LA INVESTIGACIÓN DEL DELITO DE TRATA

Como expresamente ha indicado el propio Tribunal Supremo en su Sentencia núm. 63/2020, de 20 de febrero (RJ 2020, 5720), en parte por la vinculación de la trata con la criminalidad organizada: "Existen formas de delincuencia, como muchas de las relacionadas con el tráfico de estupefacientes, que hacen necesarias técnicas policiales de investigación que implican restricciones de derechos fundamentales. La ausencia de testigos que se sientan 'víctimas'; el blindaje y opacidad de sus operaciones, y la capacidad organizativa a ciertos niveles en que se manejan importantes

22. Europol Operations Directorate, October 2020, *The challenges of countering human trafficking in the digital era*, disponible en https://www.europol.europa.eu/publications-documents/challenges-of-countering-human-trafficking-in-digital-era). En este informe se recoge la clarificadora afirmación de Catherine de Bolle (Directiva Ejecutiva de Europol) "Los traficantes de seres humanos utilizan cada vez más las modernas tecnologías de la comunicación para explotar a sus víctimas en múltiples ocasiones: desde la publicidad y la captación de víctimas, hasta el chantaje con fotos y vídeos para controlar sus movimientos. Para contrarrestar esta amenaza, tenemos que utilizar la gran ventaja de la inteligencia compartida y recoger más pruebas digitales".

montos económicos aboca a *esas técnicas de investigación más agresivas* si no se quiere claudicar en la lucha contra ese tipo de delincuencia"[23]. Las características de este delito, por tanto, recomiendan, en no pocos casos, la utilización de técnicas o medios de investigación especiales, en que el riesgo de afección a los derechos fundamentales en investigado es elevado. De entre ellas, junto con otros medios siempre útiles como las entradas y registros o las intervenciones telefónicas[24], creemos que, ante el uso de las nuevas tecnologías, las operaciones encubiertas informáticas están llamadas a jugar un papel esencial[25].

1.1. El agente encubierto informático

La utilidad de esta figura es evidente, pues permitirá acceder a la organización delictiva para determinar su naturaleza, su *modus operandi*, los lugares en que se encuentra y opera, la ubicación, real y física o virtual, de las víctimas, sus desplazamientos –de haberlos–, o seguir el rastro del dinero; en definitiva, investigar "los rastros electrónicos" de esas conductas.

La utilización del "agente infiltrado", informático o "físico", se ha presentado como un acto de investigación especialmente efectivo en la lucha contra diversas formas de criminalidad, principalmente en los casos en que la actividad delictiva se lleva a cabo en el marco de una organización criminal. Esta técnica, como es sabido, implica la ocultación de la verdadera identidad de un agente especialmente preparado, con la intención de que establezca –introduciéndose de una u otra forma en la organización criminal– una relación de confianza con los miembros de la misma con la intención de obtener información especial y necesaria para satisfacer el interés de persecución de dichos hechos delictivos. Se produce así un "doble engaño" pues se mantiene oculta tanto la identidad del sujeto como sus intenciones al implicarse en la actividad criminal.

De las distintas posibilidades de infiltración, la única contemplada por nuestro ordenamiento, en el art. 282 bis Lecrim, es la del agente encubierto;

23. V., también, AAVV.: *Guía de criterios de actuación judicial frente a la trata de seres humanos, cit.*, pp. 44 y ss.

24. Puede consultarse al respecto nuestro trabajo "Investigación y enjuiciamiento del delito de trata: Aspectos procesales desde la jurisprudencia", en VILLACAMPA ESTIARTE, C., y PLANCHADELL GARGALLO, A., *La trata de seres humanos tras un decenio de su incriminación…*, *cit.*, pp. 851 y ss.

25. La conveniencia de la utilización de los agentes encubiertos, así como de los confidentes, se ha destacado, por ejemplo, por el Protocolo de Cooperación Interinstitucional para fortalecer la investigación y protección a víctimas del delito de trata de personas y tráfico ilícito de inmigrantes, suscrito por la Asociación iberoamericana de Ministerios Públicos en el año 2017 (art. 8).

claro reflejo de cómo nuestra legislación ha optado por hacer frente a esta criminalidad a través de medidas de investigación "extraordinarias". La infiltración legalmente prevista se debe realizar por un miembro de las fuerzas y cuerpos de seguridad, (policía judicial) quedando limitado su ámbito de intervención a la investigación del crimen organizado. El infiltrado debe como tal analizar el *modus operandi* de la organización y sus miembros, los campos delictivos en que actúan y recoger información sobre la estructura del grupo[26].

La introducción en el número 6 y 7 del art. 282 bis de la figura expresa del agente encubierto informático[27] no es más que una manifestación de la necesidad de luchar contra ciertas formas de criminalidad que se valen de las nuevas tecnologías o frente figuras delictivas que se cometen a través de internet, haciendo uso también de las mismas en la investigación penal[28].

26. ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado. Los presupuestos jurídicos en el proceso penal español*, Tirant lo Blanch, Valencia 2010, *passim*.

27. LAFONT NICUESA, L., "El agente encubierto en el proyecto de reforma de la Ley de Enjuiciamiento Criminal", *La Ley Digital* núm. 4617/2015, pp. 1 y ss.; RIZO GÓMEZ, B., "La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica", en ASENCIO MELLADO, J.M y FERNÁNDEZ LÓPEZ, M., *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Valencia, pp. 100 y ss.; ZARAGOZA TEJADA, J. I., "El agente encubierto "online". La última frontera de la investigación penal", en *Revista Aranzadi Doctrinal* núm. 1/2017, (BIB 2017, 10526); VALIÑO CES, A., "La actuación del agente encubierto en los delitos informáticos tras la Ley Orgánica 13/2015", en FUENTES SORIANO, O., *El proceso penal. Cuestiones fundamentales*, Tirant lo Blanch, 2019, p. 381.

28. FLORES PRADA, I., *Criminalidad informática. Aspectos sustantivos y procesales*, Ed. Tirant lo Blanch, Valencia 2012, pp. 295 y ss.; FERNÁNDEZ TERUELO, J. G., "Cibercrimen. Los delitos cometidos a través de internet", *Constitutio Criminalis Carolina*, Oviedo, 2007, p. 13; ZARAGOZA TEJADA, J. I., "La modificación operada por la Ley 13/2015. El agente encubierto", Ponencias Formación Continua *La prueba obtenida a través de la infiltración y delación. El agente encubierto y el confidente*, 2 de junio de 2016, p. 2; ORTIZ PRADILLO, J. C., "Comunicaciones, tecnología y proceso penal: Viejos delitos, nuevas necesidades", en ASENCIO MELLADO, J. M y FERNÁNDEZ LÓPEZ, M., *Justicia penal y nuevas formas de delincuencia*, *cit.*, pp. 15 y ss.; IDEM, "Desafíos legales de las diligencias de investigación tecnológicas", en FUENTES SORIANO, O., *El proceso penal. Cuestiones fundamentales*, *cit.*, pp. 303 y ss.; GONZÁLEZ NAVARRO, A., "Nuevas tecnologías aplicadas a la investigación criminal: Las regulaciones española y alemana", en FUENTES SORIANO, O., *El proceso penal. Cuestiones fundamentales*, *cit.*, pp. 399 y ss.; RIZO GÓMEZ, B., "La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica", en ASENCIO MELLADO, J. M y FERNÁNDEZ LÓPEZ, M., *Justicia penal y nuevas formas de delincuencia*, *cit.*, p. 99.

Si bien el marco legal y conceptual es común al agente encubierto "presencial", en este caso la infiltración se produce en un canal cerrado de comunicación[29], entendiendo por comunicaciones mantenidas en un canal cerrado aquellas en las que, por expresa voluntad del comunicante, se excluye a terceros del canal de comunicación, es decir, se produce expresamente una restricción de quiénes participan en la misma, quien requiere de autorización expresa[30].

Señala Lafont Nicuesa que la actuación del agente encubierto informático se puede producir, en la práctica, en dos grandes ámbitos: El "ciberpatrullaje", en comunidades abiertas y en comunidades cerradas[31]. El primero de ellos implica una actuación en los canales abiertos de la red, siempre con identidad ficticia, con el objetivo de detectar conductas delictivas e identificar a sus autores; implica que no hay investigaciones concretas ni sospechosos identificados. Si bien a él se hacía referencia originalmente en la reforma del art. 282 bis, en la regulación finalmente aprobada se suprimió esta posibilidad, por lo que su actuación se circunscribe a los canales cerrados de comunicación. Ahora bien, esta supresión no debe interpretarse como una exclusión, sino que –como establece la S TS núm. 767/2007, de 3 de octubre (RJ 2007, 7297)–, esta actuación se lleva a cabo dentro de las funciones generales de prevención de la delincuencia, sin necesidad de autorización judicial o fiscal[32].

29. RIZO GÓMEZ, B., "La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica", en ASENCIO MELLADO, J. M. y FERNÁNDEZ LÓPEZ, M., *Justicia penal y nuevas formas de delincuencia*, *cit.*, pp. 101 y 103 y ss.; ZARAGOZA TEJADA, J. I., "El agente encubierto "online". La última frontera de la investigación penal", *Revista Aranzadi Doctrinal* núm. 1/2017, (BIB 2017, 10526), pp. 5 y ss., quien pone de manifiesto la dificultad que presenta, en ocasiones, marcar la línea entre canales abiertos y cerrados. Esta dificultad se señala también en las SS TS núm. 767/2007, de 3 de octubre (RJ 2007, 7297) o de 28 de junio de 2015 (RJ 2015, 8067).

30. RIZO GÓMEZ, B., "La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica", en ASENCIO MELLADO, J. M. y FERNÁNDEZ LÓPEZ, M., *Justicia penal y nuevas formas de delincuencia*, *cit.*, p. 103.

31. LAFONT NICUESA, L., "El agente encubierto en el proyecto de reforma de la Ley de Enjuiciamiento Criminal", *La Ley Digital* núm. 4617/2015, pp. 1 y ss.

32. En la misma línea se pronunció el informe del Consejo Fiscal al Anteproyecto. V., también, ZARAGOZA TEJADA, J. I., "La modificación operada por la Ley 13/2015. El agente encubierto", Ponencias Formación Continua *La prueba obtenida a través de la infiltración y delación. El agente encubierto y el confidente*, 2 de junio de 2016, pp. 7 y 8, 23 y ss.

1.2. *Notas características*

Las notas o características definitorias de esta figura se refieren a:

a) La nota esencial definitoria del agente encubierto es el engaño[33]. Al agente se le facilita una identidad supuesta que mantendrá durante toda la duración de la investigación, e incluso durante el proceso y con posterioridad al mismo. Haciendo uso de dicha identidad ficticia el sujeto, en aras a la investigación de los hechos delictivos, va a procurar ganarse la confianza de los miembros de la organización en que se infiltra ocultando, por tanto, sus verdaderas intenciones. El "engaño" se produce, por tanto, respecto de quién es, a qué se dedica y cuáles son sus intenciones para "involucrarse" con las actividades de la organización[34]. Es precisamente el engaño y el hecho de actuar con base en el mismo lo que obliga a compatibilizar esta figura con las garantías y principios constitucionales reconocidos en todo ordenamiento[35].

b) Precisamente por el engaño en que se basa toda la actuación del agente encubierto, la utilización de esta técnica de investigación aparece como excepcional o subsidiaria, debiendo acudirse a la misma cuando no existan otras vías para poder averiguar los hechos delictivos que se están investigando, pues no podemos negar que "mediante la intervención de un agente encubierto se alteran las reglas básicas del proceso penal"[36].

---

33. GASCÓN INCHAUSTI, F., *Infiltración policial y agente encubierto*, Comares, Granada, 2001, pp. 10 y 87, quien añade, como consecuencia de dicho engaño, el abuso de confianza, pues en esta figura es fundamental la "entrada y permanencia" en un determinado entorno. V., también muy detalladamente, ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado. Los presupuestos jurídicos en el proceso penal español*, pp. 67 y ss.; GUZMÁN FLUJA, V., *El agente encubierto y las garantías del proceso penal*, Portal Iberoamericano de Ciencias Penales, Instituto de Derecho Penal Europeo e Internacional, Universidad de Castilla – La Mancha, 2016, p. 17; GARCÍA SAN MARTÍN, J., "Los límites entre el agente encubierto y el agente provocador en la persecución de los delitos de tráfico ilícito de drogas", *La Ley Penal*, núm. 107, marzo-abril 2014, Cibercrimen (y II), p. 5. V., también, a modo de ejemplo, la S TS núm. 671/2018, de 19 de diciembre (RJ 2018, 1325); S TS núm. 277/2016, de 6 de abril (RJ 2016, 1325).

34. Como afirma Zafra Espinosa de los Monteros "la justificación de que los Estados de Derecho modernos acepten el engaño en una técnica de investigación penal se debe a la clandestinidad, la sofisticación y alta peligrosidad que representan las nuevas formas de criminalidad organizada", v., ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado. Los presupuestos jurídicos en el proceso penal español*, *cit*., p. 73.

35. Así se puso ya de manifiesto en el año 1992 por el TEDH en sentencia de 15 de junio de 1992 (caso Lüdi contra Suiza, TEDH 1992, 51), si bien luego fue matizado por la Sentencia del mismo Tribunal de 9 de junio de 1998 (caso Teixeira de Castro contra Portugal, TEDH 1998, 26).

36. ZAFRA ESPINOSA DE LOS MONTEROS, R., *El agente encubierto en el ordenamiento español*, Portal Iberoamericano de Ciencias Penales, Instituto de Derecho Penal Europeo e Internacional, Universidad de Castilla-La Mancha, 2016 p. 4. Así lo declara

Como toda medida de investigación excepcional la adopción de la misma por parte de las autoridades encargadas de la averiguación y persecución de los delitos se basa en un juicio de proporcionalidad o una ponderación de los intereses en juego.

A ello, debemos añadir que, en su actuación, el agente encubierto puede acabar cometiendo un hecho delictivo, del que no responderá penalmente

---

expresamente el propio Tribunal Supremo, por ejemplo, en su sentencia de 29 de diciembre de 2011 (RJ 2011, 135): "Con carácter previo debemos recordar que la protección de los derechos fundamentales invocados por los recurrentes no es absoluta y puede ser restringida en función de la necesidad de atender a intereses que, en el caso, sean considerados prevalentes en una sociedad democrática. En la actual situación en la que la delincuencia terrorista se organiza de forma tal que puede dificultar seriamente la acción de la justicia e incluso puede llegar a cuestionar la propia supervivencia del sistema, se impone la búsqueda de equilibrios entre la salvaguardia de esos derechos y la necesidad de obtener estándares aceptables de seguridad, entendida ésta como orientada fundamentalmente a garantizar el ejercicio pacífico y normalizado de los derechos. Por otra parte, es razonable que los poderes públicos cumplan sus finalidades mediante el empleo de los medios de investigación a su alcance, dentro de las posibilidades que les otorga la Ley.

Sin embargo, –como dice en la STS 1313/2009 de 16.12– lo que se consideran niveles deseables de seguridad con la finalidad de defender la estabilidad del sistema y asegurar el pacífico ejercicio de los derechos, en lo que aquí interesa mediante la persecución de conductas delictivas graves, –como son las relacionadas con el terrorismo– no puede obtenerse precisamente a costa de la vigencia de los derechos individuales cuya eficacia real lo caracterizan como sistema de libertades, y cuya integridad, precisamente, se trata de proteger. La calidad del sistema de convivencia en libertad desciende seriamente, hasta correr el riesgo de desaparecer, si la vigencia de los derechos fundamentales se supedita indiscriminadamente a la seguridad. Ello no suprime la posibilidad de restricciones. La naturaleza relativa de algunos derechos supone la posibilidad de que puedan ceder, en todo o en parte, ante otros intereses relevantes en una sociedad democrática. Pero solo en el caso, en la medida y en la forma en que tal interés estrictamente lo requiera, y nunca en tales condiciones que el derecho restringido venga a transformarse de manera general en una mera enunciación teórica.

Por ello, como en supuestos de delincuencia organizada –singularmente terrorismo– la investigación criminal puede encontrarse con serias dificultades pues el avance de la información queda seriamente dificultado por la opacidad de tales asociaciones criminales, se han arbitrado, –junto con las tradicionales fuentes confidenciales de información o datos suministrados por colaboradores o confidentes policiales, cuya legalidad ha sido admitida por la jurisprudencia del TEDH (sentencia Kostovski, de 20 de Noviembre de 1989, Sentencia Windisch, de 27 de Septiembre de 1990) siempre que se utilice como medio de investigación y no tenga acceso al proceso como prueba de cargo no sometida a contradicción de las partes, por cuanto ha de recordarse que la confidencia puede ocultar un ánimo de venganza, autoexculpación, beneficio personal, así como el antiguo brocardo de "quien ocultan rostro para acusar, también es capaz de ocultar la verdad en lo que acusa"–, otras técnicas de investigación nuevas tales como el agente encubierto –introducción de un miembro de la policía en la asociación criminal–, potenciando los arrepentidos, esto es, el desmarque de los miembros facilitando información sensible con la posibilidad de un beneficio penal, vía art. 579 CP, agente provocador o mediante colaboradores particulares, más o menos estables, con las fuerzas de seguridad que realizan labores de infiltración".

siempre que actúe bajo el paraguas de la autorización de infiltración y respete el principio de proporcionalidad. Si a ello añadimos que en la investigación que lleve a cabo puede verse obligado a afectar otros derechos fundamentales, como la inviolabilidad del domicilio o el secreto de las comunicaciones –siempre previa autorización judicial– el carácter excepcional de dicha medida y el cuidado que debe tenerse en su desarrollo son evidentes.

1.3. Ámbito objetivo

Desde el punto de vista de los delitos que pueden ser objeto de su actuación, debemos referirnos tanto a los establecidos en el apartado 4 del art. 282 bis (es decir, relacionados con la delincuencia organizada), como a los delitos a que se refiere el art. 588 ter, a), regulador de las intervenciones telefónicas[37] (que a su vez remite a los a los delitos del art. 579.1 Lecrim). De esta forma, el ámbito de actuación del agente encubierto alcanza también a los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología o servicio de la información o comunicación, delitos dolosos castigados con penas con límite máximo de al menos 3 años de prisión o delitos cometidos por organizaciones criminales o delitos de terrorismo[38].

37. CONDE-PUMPIDO, P., "El agente encubierto en la legislación española", Ponencias Formación Continua *La prueba obtenida a través de la infiltración y delación. El agente encubierto y el confidente*, 2 de junio de 2016, p. 7; LAFONT NICUESA, L., "El agente encubierto en el proyecto de reforma de la Ley de Enjuiciamiento Criminal", *La Ley Digital* núm. 4617/2015, p. 5, quien acertadamente pone de manifiesto que se conjuga dos criterios para habilitar la técnica investigadora del Agente encubierto informático: "Las dificultades de profundizar en la investigación que se entienden inherentes a la presencia de cualquier estructura criminal, simple o compleja, que se encuentre detrás de la comisión del delitos; y la gravedad del delito que se vincula a cualquier delito castigado en su límite máximo con al menos tres años y específicamente al delito de terrorismo"; RIZO GÓMEZ, B., "La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica", en ASENCIO MELLADO, J. M y FERNÁNDEZ LÓPEZ, M., *Justicia penal y nuevas formas de delincuencia*, *cit.*, p. 112.

    De esta forma, como indica ZARAGOZA TEJADA, J. I., "El agente encubierto "online". La última frontera de la investigación penal", en *Revista Aranzadi Doctrinal* núm. 1/2017, (BIB 2017, 10526), pp. 3 y ss., se suple las deficiencias que el propio ámbito de actuación del agente encubierto presencial suponía para la infiltración "virtual", respecto a ciertas conductas no necesariamente vinculadas a la criminalidad organizada o un grupo criminal. En el mismo sentido, VALIÑO CES, A., "La actuación del agente encubierto en los delitos informáticos tras la Ley Orgánica 13/2015", en FUENTES SORIANO, O., *El proceso penal. Cuestiones fundamentales*, *cit.*, p. 382.

38. SÁNCHEZ GÓMEZ, R., "El agente encubierto informático", en *La Ley Penal* núm. 11, enero-febrero 2016, p. 5.

La autorización debe ser, obviamente, motivada. Pese a la parquedad de la norma habilitante y dada la referida trascendencia, consideramos, que dicha autorización debe tener el siguiente contenido mínimo[39]: **1)** Los indicios de que se está cometiendo alguno de los delitos en que dicha medida de investigación está justificada, los delitos concretos que se sospecha están siendo cometidos y que son objeto de investigación, no siendo posible una autorización abierta para cualquier actividad delictiva, es decir, en abstracto o en general para cualquier actividad delictiva que se lleve a cabo por la organización; **2)** Cuando sea posible deberá identificarse a las personas pertenecientes a la organización, es decir, los posibles imputados; **3)** El plazo de duración de la misma, con los matices indicados seguidamente; **4)** Las actividades para las que se autoriza al agente, lo que permite exonerarle de responsabilidad en dichas actuaciones[40]; **5)** La verdadera identidad del agente y la supuesta, bajo la que actuará; **6)** La forma en que se debe comunicar con la autoridad para facilitarle la información que obtenga. Se trata así de justificar la existencia de indicios racionales de comisión de delitos en forma organizada, poniendo de manifiesto que esta técnica de investigación, pese a los riegos que pueda comportar, es necesaria e idónea para investigar dichos hechos; en definitiva, que cumple con las exigencias del principio de proporcionalidad. Esta autorización será reservada y se mantendrá fuera de las actuaciones (art. 282 bis, 1 Lecrim)[41].

Dicha autorización es la que legitima la actuación engañosa del agente, así como la actuación concreta que pueda realizar, siempre que se desarrolle dentro de los límites establecidos.

1.4. Desarrollo de la medida

Si bien somos conscientes de la dificultad que supone enumerar qué actuaciones concretas puede llegar a cabo el agente encubierto, consideramos importante hacer una breve mención a la posibilidad, prevista en el apartado 7 del art. 282 bis Lecrim, de autorizar judicialmente al agente encubierto a obtener imágenes y grabar las conversaciones, directas u

39. RIFA SOLER, J. M., "El testigo protegido y el agente encubierto", en ABEL LLUCH, X. y RICHARD GONZALEZ, M., *Estudios sobre la prueba penal, vol. II*, La Ley, Madrid, 2011, p. 349; GASCÓN INCHAUSTI, F., *Infiltración policial y agente encubierto*, *cit.*, p. 208; ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado. Los presupuestos jurídicos en el proceso penal español*, *cit.*, pp. 339 y ss.; EXPÓSITO LÓPEZ, L., "El agente encubierto", *Revista de Derecho UNED*, 2015, núm. 17, pp. 273 y 274.

40. Sobre la trascendencia de la determinación de las tareas, puede consultarse la S TS núm. 277/2016, de 6 de abril (RJ 2016, 1325).

41. S TS núm. 250/2017, de 5 de abril (RJ 2017, 1968).

online, que pueda mantener en los encuentros previstos entre el agente y el investigado, capturas de pantallas, etc.; encuentros que deberán identificarse expresamente en la autorización[42], no pudiendo entenderse como un cheque en blanco a favor del agente. Igualmente, el agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos (piénsese en archivos de contenido pornográfico)[43].

Como hemos indicado, si en el desarrollo de sus funciones como "infiltrado" pudiera verse afectado algún derecho fundamental la habilitación general no será suficiente, sino que deberá solicitar al órgano judicial las autorizaciones que al respecto se prevean en la Constitución y en la Ley rituaria o leyes especiales, cumpliendo además en su ejecución concreta con todas las previsiones legales aplicables, so pena de ilicitud (por ejemplo para una intervención telefónica; es decir, la autorización genérica de infiltración no le exime de ello). La ilicitud de lo actuado no dependerá únicamente de la afección de derechos fundamentales sin la correspondiente autorización, sino también de la posible actuación del agente al margen de la autorización original, del posible incumplimiento de los requisitos legales de los diversos actos de investigación que sí está autorizado a llevar a cabo o de la propia provocación del delito[44].

Un elemento clave en esta actuación debería ser, por su carácter excepcional, su duración temporal: Las normas que estamos analizando realmente no prevén expresamente el tiempo de duración de la medida, sino el periodo de tiempo para el que se otorga la identidad ficticia. Así, el art. 282 bis Lecrim prevé que la identidad ficticia se otorgará por un plazo de seis meses, prorrogables por periodos de igual duración. Ello nos permite inferir que dicha duración es aplicable a la infiltración[45]. Dada la falta de previsión de un número máximo de prórrogas, la duración de la medida y sus sucesivas prórrogas deberá modularse en atención al principio de proporcionalidad.

42. CONDE-PUMPIDO, P., "El agente encubierto en la legislación española", Ponencias Formación Continua *La prueba obtenida a través de la infiltración y delación. El agente encubierto y el confidente*, 2 de junio de 2016, p. 18.
43. SÁNCHEZ GÓMEZ, R., "El agente encubierto informático", *La Ley Penal* núm. 11, enero-febrero 2016, p. 6; ZARAGOZA TEJADA, J. I., "El agente encubierto "online". La última frontera de la investigación penal", *Revista Aranzadi Doctrinal* núm. 1/2017, (BIB 2017, 10526), pp. 8 y 9.
44. GASCÓN INCHAUSTI, F., *Infiltración policial y agente encubierto*, *cit.*, pp. 249 y ss. V., también, la S TS de 16 de febrero de 2006 (RJ 2006, 1068).
45. Advierte precisamente GÓMEZ DE LIAÑO FONSECA-HERRERO, "Límites y garantías de la investigación con agentes encubiertos", *Diario La Ley núm. 6142 de 7 de diciembre de 2004*, p. 8.

Al respecto, es importante matizar que la identidad supuesta puede mantenerse durante la celebración del juicio oral, y, en caso de recurso, hasta que la sentencia adquiera firmeza. Este mantenimiento se producirá cuando exista un motivo razonable para pensar que la revelación de la identidad una vez concluida la investigación podría poner en peligro la vida, la integridad o la liberta del agente encubierto o por entender que podrá seguir utilizando dicha identidad en otras actuaciones[46].

El adecuado desarrollo de la medida exige del control de la misma por parte de la autoridad que la autorizó. Este control no sólo debe producirse al inicio de la actividad de infiltración, autorizándola o permitiendo su prórroga, sino que debe extenderse al desarrollo de la medida hasta su conclusión, debiendo el agente informar del curso de su investigación y sus progresos, así como para autorizar actuaciones complementarias que requieran autorización. Dicho control será fundamental para legitimar los hallazgos casuales (art. 579 bis Lecrim) con que se pueda encontrar el agente encubierto, quedando cubierta su actuación siempre que dichos delitos formen parte de los delitos para los que legalmente dicha medida está prevista[47].

El agente encubierto no responde criminalmente por los hechos delictivos que son consecuencia necesaria del desarrollo de la investigación, pero siempre que no impliquen una provocación al delito, sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la investigación (art. 282 bis.5 Lecrim)[48]. En este sentido, el límite más importante a la actuación del agente infiltrado es que provoque él mismo la comisión del delito, adaptándose así a la jurisprudencia existente sobre el delito provocado[49]; que no cabe ni en ésta ni en otras formas de investigación.

2. OTROS MEDIOS DE INVESTIGACIÓN: LA ENTREGA VIGILADA

Como es sabido, la reforma operada en la Lecrim por la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para

46. Así, la S TS núm. 671/2018, de 19 de diciembre (RJ 2018, 1325).
47. GASCÓN INCHAUSTI, F., *Infiltración policial y agente encubierto, cit*., p. 221.
48. V., respecto a estas cuestiones, GASCÓN INCHAUSTI, F., *Infiltración policial y agente encubierto*, *cit*., pp. 276 y ss.; ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado. Los presupuestos jurídicos en el proceso penal español*, *cit*., pp. 396 y ss. Sobre los requisitos que dicha exoneración exige, v., LOPEZ BARJA DE QUIROGA, J., "El agente encubierto", *La Ley* 1992-2, pp. 1 y ss.; RIFÁ SOLER, J. M., "Agente encubierto o infiltrado en la nueva regulación de la Lecrim", *Revista del Poder Judicial*, 1999, (55), pp. 166, 171 y ss.
49. V., por ejemplo, las SS TS núm. 104/2019 de 27 febrero (RJ 2019, 1008); núm. 277/2016, de 6 de abril (RJ 2016, 1325); núm. 575/2013 de 28 junio (RJ 2013, 8067).

el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, regula los llamados medios de investigación tecnológicos, estableciendo previamente unas disposiciones, de carácter general, de aplicación común a todos ellos; normas generales que parten de la necesaria afección de los mismos sobre los derechos fundamentales de la persona investigada. Estas normas generales se refieren a los principios de idoneidad, especialidad, necesidad y proporcionalidad.

Sin perjuicio de la importancia que para la investigación del delito de trata puede presentar la interceptación de las comunicaciones telefónicas y telemáticas, el acceso a los datos electrónicos de tráfico, la identificación mediante IP o el registro remoto sobre equipos informáticos, dedicamos unas breves líneas a la entrega vigilada de remesas de dinero virtual, documentos u otros elementos.

Regulada en el artículo 263 bis Lecrim, estamos –junto con la utilización del agente encubierto– en un acto de investigación "especial" muy eficaz si se emplea correctamente para luchar contra ciertas modalidades de criminalidad organizada, por ejemplo, el narcotráfico[50]. Si bien, no hay mención expresa a las remesas de dinero virtual o a los documentos, creemos que –por el contexto delictual en que se producen– sería positivo la posibilidad de acudir a esta especial técnica de investigación para estos objetos.

La finalidad de esta medida es permitir que los documentos o el dinero virtuales, en este caso, circulen "libremente", sin ser intervenidos, desde el punto de "colecta", origen o elaboración hasta el punto de destino, de manera que dicho seguimiento permita "desmantelar" la organización y, en su caso, detener a todos los que se integran en la cadena delictiva, desde el miembro más modesto hasta los grandes jefes.

50. V., BELTRÁN MONTOLIU, A., "La autorización judicial de circulación y entrega vigilada de drogas, sustancias, materiales u otros bienes ilícitos como método para luchar contra la criminalidad organizada", en GÓMEZ COLOMER, J. L., *La instrucción del crimen: algunos problemas procesales*, Sepin, Madrid, 2020, pp. 99 y ss.; ALONSO PÉREZ, F., "Circulación y entrega vigilada de drogas y otras sustancias prohibidas", *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, N.º 7, 2000, pp. 2010 y ss.; NÚÑEZ PAZ, M. A., y GUILLÉN LÓPEZ, G., "Entrega vigilada, agente encubierto y agente provocador: análisis de medios de investigación en materia de tráfico de drogas", *Anuario de derecho penal y ciencias penales*, Tomo 61, Fasc/Mes 1, 2008, pp. 89 y ss.; DELGADO MARTÍN, J., "La entrega vigilada de droga u otro elemento ilícito", *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, N.º 5, 2000, pp. 1853 y ss.; MOLINA MANSILLA, M.ª C., "La circulación y entrega vigilada de objetos de delito", *La ley penal: revista de derecho penal, procesal y penitenciario*, N.º 61, 2009, p. 5; VELASCO NÚÑEZ, E., "Entregas vigiladas, infiltración y agente encubierto en Internet", *Justicia: revista de derecho procesal*, núm. 1-2, 2010, pp. 251 y ss.

El ámbito objetivo en que puede practicarse, de acuerdo con el art. 263bis. 1 Lecrim, abarca, además del narcotráfico, delitos como la adquisición, conversión o transmisión de bienes de origen delictivo; la falsificación, introducción o expedición de moneda falsa o la alteración, reproducción o falsificación de tarjetas de crédito o cheques de viaje

También esta medida exige resolución fundada en la que se determine explícitamente, en cuanto sea posible, el objeto de autorización o entrega vigilada, así como el tipo objeto de que se trate; jugando un papel fundamental el principio de necesidad y proporcionalidad.

Capítulo 15

La ciberviolencia de género: nuevas formas de victimización[1]

Mercedes Llorente Sánchez-Arjona

Profesora Titular de Derecho Procesal
Universidad de Sevilla

I. LAS VÍCTIMAS ANTE LA CIBER VIOLENCIA

En la sociedad actual resulta difícil concebir las relaciones fuera de un marco tecnológico, máxime si nos referimos a la población más joven. Las nuevas tecnologías forman parte de nuestro día a día, siendo cada vez más común tener una vida en el espacio virtual a través de formas de comunicación como WhatsApp, correos electrónicos o redes sociales como Facebook, Instagram o Tuenti, que habilitan una transmisión de datos e información constantes que han revolucionado la manera de entender las relaciones interpersonales o conceptos como la privacidad o la intimidad. Las redes sociales han posibilitado un escaparate abierto al mundo en el que se transmiten experiencias e ideas y se comparte la intimidad dejando rastro de donde estamos, que hacemos o como nos sentimos en cada momento. Y es que este nuevo entorno virtual en el que se desarrolla nuestra propia existencia puede entrar en colisión con Derechos Fundamentales fuertemente arraigados en nuestra sociedad como el derecho a la intimidad, a la privacidad, a la protección de datos o al secreto de las comunicaciones, entre otros. A pesar de sus múltiples beneficios, esta puerta abierta al mundo tiene facetas oscuras que vienen de la mano de la reproducción de conductas violentas frente a diversos actores entre los que están, con gran asiduidad, las mujeres.

1. Este trabajo se enmarca en el Proyecto I+D+i de generación del conocimiento titulado "El acceso a la justicia de las personas vulnerables" PID2021-123493OB-100, IPs Mercedes Llorente Sánchez-Arjona y Vicente Guzmán Fluja.

Resulta paradójico que, a pesar de los avances experimentados por la sociedad actual, se sigan reproduciendo en estos espacios virtuales comportamientos sexistas o claramente atentatorios contra la igualdad de género en un escenario marcadamente tecnológico y vanguardista pero que continúa manteniendo la esencia de la cultura patriarcal imperante durante siglos. De este modo, el espacio virtual mantiene las discriminaciones por razón de género con el peligro añadido que la violencia desarrollada a través de estos procedimientos tiene más posibilidades de diluirse como parte de un ambiente de normalidad[2]. Violencia y machismo se han adaptado a estos entornos virtuales, dando lugar a nuevas formas de acoso que posibilitan una insistencia desconocida hasta el momento actual, ya que el que agrede puede destinar el tiempo que desee a denigrar, humillar y acosar a la víctima, haciéndolo desde múltiples dispositivos de forma simultánea sin importar el lugar en que se halle. A la angustia que este comportamiento genera en las víctimas, ha de añadirse que lo que se cuelga en red permanece, ya que aún cuando se pueda borrar, lo cierto es que cualquier usuario puede habérselo descargado de Internet antes de que se haya procedido a su retirada[3].

Ciertamente, la agresión y el acoso en el mundo virtual tiene unas características propias que se identifican, en primer lugar, por su facilidad de acceso al bastar con un dispositivo conectado a Internet, y, en segundo lugar, por el anonimato que proporcionan, lo cual dificulta el rastreo de la persona que agrede proporcionándole sensación de impunidad[4]. En este contexto conviven conductas que tradicionalmente se configuran como delitos de amenazas, coacciones o maltrato psicológico con los delitos contra la intimidad cuando se cometen a través de redes sociales[5]. Así, en estos espacios virtuales se siguen reproduciendo y transmitiendo estereotipos y desigualdades de género que provienen de esquemas tradicionales de discriminación, sobre los que se asienta la violencia de género, que debe analizarse también a la luz de estas formas actuales de relación, las cuales nos permiten hablar de la aparición de nuevos métodos para ejercer este tipo de violencia estrechamente vinculadas al desarrollo de las

2. LORENTE ACOSTA, M., "Virtualidad ficticia y violencia de género" en *Violencias de género en entornos virtuales,* DONOSO VÁZQUEZ, T., REBOLLO CATALÁN, A., Ed. Octaedro, Barcelona, 2018, p. 8.
3. LLORENTE SÁNCHEZ-ARJONA, M., *Justicia con perspectiva de género. El nuevo paradigma en la lucha contra la violencia de género*, Ed. Aranzadi, Pamplona, 2021, p. 207.
4. DONOSO-VÁZQUEZ, T., "Las ciber violencias de género, nuevas manifestaciones de la violencia machista" en *Violencias de género en entornos virtuales,* Ed. Octaedro, Barcelona, 2018, p. 19.
5. VARGAS GALLEGO, A., "Nuevas formas de violencia contra las mujeres. Redes sociales. Delitos de descubrimiento y revelación de secretos", https://lefebvre.es.

nuevas tecnologías. De hecho, todas las conductas de violencia de género que se ejercen a través de estas nuevas tecnologías, de las redes sociales o de Internet se conocen ya como violencia de género digital. Por tanto, la ciberdelincuencia de género será aquel tipo de violencia que se desarrolla por un hombre mediante el uso de las Tecnologías de la Información y la Comunicación, contra una mujer con la intención de someterla, rebajarla o controlarla, en base a los estereotipos de género.

Es bien sabido que el maltrato por violencia de género reviste unas connotaciones verdaderamente complejas que le hacen radicalmente diferente a cualquier tipo de violencia interpersonal al que se haya podido enfrentar el Estado. La motivación que induce al agresor a ejercer este tipo de conducta va más allá de una actitud violenta puntual, trascendiendo a una actitud de intimidación y control con la que se pretende conseguir una reacción por parte de la víctima de temor y subordinación, en base a una relación estructural basada en la desigualdad que, antes, se limitaba al mundo *off line* pero que, actualmente, se manifiesta, igualmente, en el universo *on line.* A día de hoy, la proximidad física ha dejado de ser un elemento imprescindible para la comunicación provocándose cambios en las formas de interactuar fruto de una sociedad cada vez más global, basada en un tipo de comunicación interactiva apoyada precisamente por el auge de la tecnología[6].

En este contexto, el concepto de intimidad se diluye, siendo común que temas de conversación o prácticas íntimas o privadas, que se relacionan con el cuerpo, la sexualidad o los sentimientos, se compartan sin que se perciba riesgo alguno. No obstante, y aun cuando es cierto que quien lleva a cabo estas conductas pone en riesgo su propia intimidad al remitir su grabación, o permitir que le graben, no es menos cierto que esta ampliación de la exposición del riesgo, o la existencia de la propia imprudencia de la víctima, no debe conllevar que estos hechos queden impunes, al no existir autorización expresa o tácita de que esas imágenes se difundieran a terceros[7]. Tal como se pone de manifiesto en la Sentencia del Tribunal

6. MUÑIZ RIVAS, M., CUESTA ROLDAN, J. Violencia de género en entornos virtuales, *Revista del Cisen Tramas/Maepova*, vol. 3, núm. 2, octubre 2015, p. 107.

7. MAGRO SERVET, V., "Los delitos de sexting y stalking en la reforma del Código Penal", www.observatorioviolencia.org., pp. 4 y 7 apunta que "Algunas personas añaden que ese riesgo debería ser asumido por la persona que permite estas grabaciones por el peligro que ello supone, sobre todo al tratarse de imágenes que pueden dañar su intimidad, pero en realidad también es cierto que las afectadas también tienen derecho a que lo que graban ellas o les dejan que se grabe se quede en el ámbito estrictamente personal y que no trasvase esa esfera personal, por lo que la difusión no autorizada debe tener la repulsa no solo social, sino del derecho, y para ello debe existir una tipificación que permita actuar a las Fuerzas y Cuerpos de Seguridad del

Supremo 70/2010, de 24 de febrero, "quien remite a una persona en la que confía una foto expresiva de su propia intimidad no está renunciando anticipadamente a esta. Tampoco está sacrificando de forma irremediable su privacidad. Su gesto de confiada entrega y selectiva exposición a una persona cuya lealtad no cuestiona, no merece el castigo de la exposición al fisgoneo colectivo". Ciertamente, esta exposición resulta especialmente grave cuando los archivos audiovisuales tienen un contenido sexual, precisamente por el grado de afectación a la intimidad de la persona que puede darse por su difusión no consentida[8], siendo su difusión una manifestación más de los perjuicios, estereotipos y actitudes sexistas que provocan nuevas formas de violencia de género.

Los dispositivos móviles de comunicación e Internet se han convertido en un medio fundamental para la socialización en todo el mundo, ofreciendo inmensas ventajas tanto a nivel personal como profesional, si bien su uso inapropiado puede dar lugar a nuevos peligros, pudiendo ser utilizados para dañar o perjudicar de forma intencionada a personas o colectivos más vulnerables. Uno de estos peligros es, precisamente, la transmisión de la desigualdad de género, al reproducirse las estructuras sociales y culturales vigentes en la sociedad, contribuyendo a normalizar los roles de género a través de nuevas formas de violencia o consolidando las ya existentes en el mundo *off line*. Además, suele ser habitual, sobre todo en la población más adolescente, el presentar una baja percepción de la ciber violencia, provocando que perciban menos los riesgos que derivan de las conductas de vida *on line*[9].

El proceso de comunicación que proporcionan las nuevas tecnologías puede ser utilizado con fines intimidatorios, insultantes, injuriosos o agresivos atentando contra la dignidad de la mujer que ha sido o es su pareja. Nos encontramos con una forma de violencia psicológica ejercida sobre la mujer mediante conductas desarrolladas en el plano virtual que provocan en la víctima desvalorización o sufrimiento. No se trata de nuevos bienes jurídicos lesionados, sino de nuevas estrategias de lesión que requieren la adaptación de esta realidad social al ámbito judicial y punitivo. Este tipo

---

Estado para realizar la oportuna investigación por los equipos de investigación en delitos informáticos que son los que deben realizar la investigación oportuna para ver desde qué dispositivo técnico se han difundido esas imágenes y poder detener al autor de los hechos".

8. SORIANO RUIZ, N., "Difusión ilícita del sexting y violencia de género. Tratamiento penal y procesal en España", *Revista Electrónica de Estudios Penales y de la Seguridad*, www.ejc-reeps.com., 2019, p. 4.
9. VILLAR VARELA, M., MÉNDEZ-LOIS, M. J., BARREIRO FERNÁNDEZ, F., "Violencia de género en entornos virtuales: una aproximación a la realidad adolescente", *Electronic Journal of Research in Educational Psychology*, núm. 55, 2021, pp. 512-513.

de violencia afecta a la integridad moral y emocional de la mujer dejándola expuesta ante conocidos y desconocidos y generándole un tipo de presión psicológica que puede llegar a tener implicaciones muy graves. Son conductas que responden a un patrón de control y manifestación de poder que se exteriorizan en actuaciones susceptibles de la comisión de algún hecho delictivo. Al utilizarse la vía electrónica como medio para delinquir, hace que la violencia física quede descartada y estos ataques se conciban como una nueva modalidad de ejercer violencia psicológica sobre las víctimas.

Emergen nuevas tácticas de control de la pareja como puede ser el control por parte del novio del móvil de la menor para averiguar las llamadas que recibe o ha realizado, la presión para que elimine determinados contactos de redes sociales, impedir que suba determinadas fotos por considerarlas no adecuadas o averiguar donde se encuentra por cualquier tipo de aplicación. Estas y otras muchas se han convertido en importantes herramientas de control que funcionan con una intensidad desconocida hasta el momento actual y que requieren de la actuación de los poderes públicos a través de campañas de sensibilización que conciencien a la sociedad sobre los peligros de este tipo de conductas, así como las consecuencias devastadoras que pueden provocar sobre la vida de las víctimas. En el entorno virtual la víctima tiene que afrontar la ausencia de lugares seguros ya que puede ser atacada las 24 horas del día y los siete días de la semana. A ello ha de añadirse la indefensión que se deriva de la pérdida de control por las diversas actuaciones que se integran en la ciber violencia, como la difusión de imágenes íntimas o la culpabilización que suelen experimentar las víctimas por parte de su entorno social.

II. LA VÍCTIMA DE VIOLENCIA DE GÉNERO DIGITAL ANTE EL PROCESO

La ciber violencia como forma de violencia de género implica agresión psicológica, constante y repetida en el tiempo, contra la pareja o expareja, a través de la utilización de las nuevas tecnologías, teniendo como objetivo la dominación, el abuso de la posición de poder, así como la intromisión, sin consentimiento, en la vida privada de la víctima. En este tipo de delitos la reiteración se convierte en la estrategia de invasión de la intimidad más utilizada por los acosadores[10]. Esta violencia puede tener lugar

10. QUESADA AGUAYO, M., "La violencia de género y el ciberacoso en las redes sociales: análisis y herramientas de detección" en *Ciberacoso y violencia de género en redes sociales. Análisis y herramientas de prevención,* VERDEJO ESPINOSA, M. A., (coord.), Universidad Internacional de Andalucía, 2015.

durante la relación de pareja, con la utilización de los TIC para someter a la víctima a control, bien mediante la comisión de concretos delitos contra la libertad, contra el honor o contra la intimidad, bien a través de la realización de actos de violencia psíquica que determinan la aparición de un delito basado en la reiteración o habitualidad. De igual forma, este tipo de violencia puede aparecer una vez que la relación de pareja ha finalizado, en supuestos en los que el agresor no acepta la ruptura mediante el delito de quebrantamiento de prohibición de comunicación, pero también a través de conductas de acoso, o comportamientos delictivos como el *stalking*, *sexting* y *sextorsión*.

Nos enfrentamos a comportamientos que no se limitan tan solo al acoso sexual, sino que trascienden a formas de control que atentan gravemente contra la integridad moral y emocional de la mujer. Este tipo de actuaciones delictivas tiene un alto componente emotivo, ya que estas conductas están cargadas de sentimientos como celos, envidia, odio, venganza o incapacidad de aceptar un rechazo[11]. Las víctimas de ciberacoso pueden llegar a sufrir depresión, trastornos de ansiedad, ataques de pánico y un elevado nivel de estrés, lo que constituye claramente una forma de violencia psíquica especialmente grave[12].

Por tanto, y aún cuando la violencia de género en entornos virtuales no deja de ser otro tipo de violencia ejercida sobre la mujer-pareja que comparte el mismo objetivo común de subordinación y control que la violencia física, psíquica o sexual, lo cierto es que suscita una serie de peculiaridades en el plano procesal que traen causa de la forma de comisión del hecho delictivo. Estas peculiaridades procesales serán objeto de atención en las siguientes líneas, en particular, las referidas a los problemas probatorios de este tipo de violencia cometido por medios tecnológicos por ser el momento procesal que más dificultad plantea.

1. LA PRUEBA DE LA CIBER VIOLENCIA DE GÉNERO

Sin duda alguna, uno de los principales problemas a los que se enfrenta el enjuiciamiento de los delitos por violencia de género es la dificultad probatoria que caracteriza este tipo de procesos. Al escaso material probatorio con que, de ordinario, se va a contar en la práctica, al ser delitos que suelen cometerse en el ámbito de la intimidad familiar, así como a los

11. DE VICENTE PACHÉS, F., "Ciberacoso: un nuevo fenómeno de violencia contra la mujer" en *X Seminario Estatal Isonomia contra la violencia de género,* 13 de noviembre de 2014, Ed. Universitat Jaume I, 2016, p. 4.
12. CHACÓN MEDINA, A., "Una nueva cara de internet: el acoso", *Revista Ética-Net*, Granada, 2003, pp. 4-6.

frecuentes cambios de declaración de las víctimas, se han de unir ahora los problemas que se derivan del uso de las nuevas tecnologías como nueva forma de ejercer violencia y su tratamiento en el proceso.

En este contexto, la probanza de los hechos físicos es sustituida por la de los hechos virtuales con una clara afectación al marco de la prueba judicial. Nos encontramos con hechos electrónicos o digitales que han acontecido en el universo virtual y cuya probanza es por medios electrónicos. Resulta cada vez más frecuente que las pruebas que se presentan ante los Tribunales partan de un soporte digital a través de sistemas de mensajería instantánea o de redes sociales, siendo de todo punto imprescindible demostrar en sede judicial la veracidad de las comunicaciones que se aportan por las partes. Y es que las nuevas tecnologías no solo han alterado las comunicaciones entre las personas, sino que han afectado, de igual forma, al derecho probatorio modificando las características propias de la prueba en los procesos judiciales[13].

La violencia de género que se practica a través de las nuevas tecnologías supone un reto para los distintos operadores jurídicos que se enfrentan a delitos de reciente cuño perpetrados a través de formas de comisión delictiva poco conocidas y que, debido a las posibilidades de anonimato que proporciona Internet, pueden plantear problemas en el momento de probar la autoría del delito o de aportar información al proceso a fin de que alcance el deseado valor probatorio. La enorme variedad de mecanismos de comunicación a través de Internet (SMS, correos electrónicos, Facebook, Instagram, Twitter, Messenger, WhatsApp, TikTok…) hace que resulte extraordinariamente complejo establecer unos criterios procesales homogéneos para su tratamiento y valoración cuando se aportan como medio de prueba al proceso penal con el objetivo de acreditar el contenido de una comunicación determinada[14].

No obstante, la posible manipulación de las pruebas así obtenidas que pueden ser falseadas e, inclusive, inventadas nos conducen a una situación de inseguridad jurídica tanto por la complejidad técnica de este tipo de pruebas, como por la novedad y constante aparición de nuevas plataformas de comunicación que exigen la constante adaptación de nuestros Jueces y Tribunales al tener cada una de ellas peculiaridades propias. Y es que, aún cuando resulte increíble, resulta más fácil alterar el contenido de un documento tecnológico que el clásico documento en papel.

13. ARRABAL PLATERO, P., *La prueba tecnológica: aportación, práctica y valoración,* Ed. Tirant lo Blanch, Valencia, 2019, p. 33.

14. FUENTES SORIANO, O., "Comunicaciones telemáticas: práctica y valoración de la prueba" en *El proceso penal: Cuestiones fundamentales,* Ed. Tirant lo Blanch, Valencia, 2017, p. 254.

El peligro más importante a evitar es que en la búsqueda y obtención de la prueba del hecho electrónico se vulnere algún derecho fundamental, aspecto sobre el que existe una muy consolidada jurisprudencia que ha tenido ocasión de destacar que en la prueba de los hechos no todo resulta admisible, siendo uno de sus límites la ilicitud o ilegalidad en su obtención[15]. Además, no podemos olvidar que nos movemos en un terreno particularmente delicado en lo que hace al respeto y protección no solo de los derechos fundamentales, mediante instrumentos de prueba lícita, sino también del conjunto de las garantías procesales incorporadas en el derecho a la presunción de inocencia y el derecho al debido proceso[16].

Se dice que el derecho va siempre un paso por detrás de la realidad social, pero inexorablemente debe adaptarse a ella y, que duda cabe, que estas nuevas formas de prueba están ganando cada vez más peso en los procesos judiciales, de tal forma que puede afirmarse que muchas pruebas tradicionales presentadas en juicio están migrando desde el soporte de papel hacia un entorno virtual[17]. Pero aun cuando la comunicación electrónica está adquiriendo cada vez mayor relevancia en orden a esclarecer la verdad acerca de los hechos controvertidos dentro del proceso, para que cualquier forma de comunicación telemática pueda ser admitida como prueba en el proceso, precisa cumplir con las exigencias legales que se prevén, con carácter general, de pertinencia, utilidad y licitud probatoria, así como con los requisitos formales de aportación en tiempo y forma para una posterior valoración probatoria. Con todo, lo cierto es que los datos que se almacenen en estos dispositivos presentan peculiaridades probatorias específicas en atención a la plataforma de comunicación que se aporte. Expondremos a continuación las que consideramos se utilizan con mayor frecuencia para perpetrar agresiones en el marco de la pareja o expareja.

2. LOS CONTENIDOS DE WHATSAPP COMO MEDIO DE PRUEBA

Esta aplicación de mensajería instantánea es líder a nivel mundial en comunicación y permite además de chats de texto, enviar fotografías, audio y vídeos lo que le convierte en un instrumento especialmente

15. PICÓ I JUNOY, J., "Retos del derecho probatorio ante las nuevas tecnologías" en *Inteligencia Artificial Legal y Administración de Justicia,* CALAZA LÓPEZ, S., LLORENTE SÁNCHEZ-ARJONA, M., (Dir.), Ed. Aranzadi, Pamplona, 2022, p. 443.
16. ARMENTA DEU, T., "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre", *Revista de Internet, Derecho y Política*, núm. 27, septiembre 2018, p. 68.
17. LLORENTE SÁNCHEZ-ARJONA, M., *Justicia con perspectiva de género…, cit*., p. 230.

idóneo para perpetrar agresiones en el seno de la pareja o expareja. La frecuencia de su uso ha provocado que las conversaciones de *WhatsApp* sean un medio de comunicación que forma parte de nuestro día a día y como vehículo de comunicación es un instrumento tecnológico que se utiliza por los victimarios para ejercer violencia sobre sus víctimas. Ello ha supuesto que el contenido de estos *WhatsApp* se hayan convertido en una de las principales vías para demostrar situaciones de violencia ante los Juzgados y Tribunales, esto es, se han incorporado como medio de prueba en juicio.

Ahora bien, una característica de este tipo de comunicación es que el contenido de la información que se pretende hacer valer en juicio no es conservado por un servidor externo a los dispositivos electrónicos de los comunicantes. De esta manera, el juez no podrá solicitar a *WhatsApp Inc* la certificación del contenido de los mensajes, sino que su acreditación viene dada por los propios dispositivos electrónicos usados durante la conversación[18]. Esta peculiaridad de *WhatsApp* es propia de las plataformas de mensajería instantánea que transmiten y comparten información de forma simultánea de manera bidireccional o multidireccional, pero que no es almacenada en ningún servidor externo[19], a diferencia de la información que se vuelca en redes sociales que se almacena en bases de datos gestionadas por sus administradores y accesibles a un determinado volumen de usuarios. En este punto, lo único que podrá certificarse por la empresa *WhatsApp* será lo que se conoce como "datos de tráfico" que se concretarán en constatar las comunicaciones, el origen y destino de las mismas, los datos que se conservan sobre identidades y nombres de usuario y clave, que incluyen el número de abonado telefónico asociado o el IP de referencia[20].

Conforme a pronunciamientos de la jurisprudencia más reciente, para que los *WhatsApp* sean admitidos como medio de prueba en el proceso han de haber sido obtenidos de manera lícita debiendo comprobarse, posteriormente, la autenticidad e integridad de los mensajes. Por consiguiente, el primer requisito que deben cumplir los mensajes de *WhatsApp* para ser admitidos como prueba es que en su obtención no se hayan vulnerado ni el derecho a la intimidad ni el secreto de las comunicaciones

18. DELGADO MARTÍN, J., "La prueba de WhatsApp"*, Diario La Ley*, Sección Tribuna, 15 de septiembre de 2015, núm. 8605, p. 2.
19. RODRÍGUEZ LAÍNZ, J. L., "Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea (A propósito de la STS, Sala II, 300/2015, de 19 de mayo)", *Diario La Ley*, Sección Doctrina, 25 de junio de 2015, 8569, pp. 6-7.
20. RODRÍGUEZ LAÍNZ, J. L., "Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea"…, *cit.*, p. 7.

recogidos en el artículo 18 de la Constitución[21]. Sobre este particular, la Sentencia del Tribunal Supremo 291/2019, de 31 de mayo, apunta que las grabaciones privadas en casos de maltrato no afectan al derecho a la intimidad. Citando una ya consolidada jurisprudencia de la Sala II[22], se alude a la Sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre, que señala que "No hay 'secreto' para aquél a quien la comunicación se dirige, ni implica contravención de lo dispuesto en el artículo 18.3 de la Constitución la retención, por cualquier medio, del contenido del mensaje. Dicha retención (la grabación, en el presente caso) podrá ser, en muchos casos, el presupuesto fáctico para la comunicación a terceros, pero ni aun considerando el problema desde este punto de vista puede apreciarse la conducta del interlocutor como preparatoria del ilícito constitucional, que es el quebrantamiento del secreto de las comunicaciones. Quien graba una conversación de otros atenta, independientemente de toda otra consideración, al derecho reconocido en el artículo 18.3 de la Constitución; por el contrario, quien graba una conversación con otro no incurre, por este solo hecho, en conducta contraria al precepto constitucional citado. Si se impusiera un genérico deber de secreto a cada uno de los interlocutores o de los corresponsables ex art. 18.3, se terminaría vaciando de sentido, en buena parte de su alcance normativo, a la protección de la esfera íntima personal ex art. 18.1, garantía ésta que, 'a contrario', no universaliza el deber de secreto, permitiendo reconocerlo sólo al objeto de preservar dicha intimidad…Los resultados prácticos a que podría llevar tal imposición indiscriminada de una obligación de silencio al interlocutor son, como se comprende, del todo irrazonables y contradictorios, en definitiva, con la misma posibilidad de los procesos de libre comunicación humana… Como conclusión, pues, debe afirmarse que no constituye contravención alguna del secreto de las comunicaciones la conducta del interlocutor en la conversación que graba ésta (que graba también, por lo tanto, sus propias manifestaciones personales)". De este modo, el Tribunal Supremo defiende que sobre la validez de las grabaciones privadas entre dos personas hay que recordar que no resulta preciso el consentimiento del afectado por ellas; que se exige la presencia de los interlocutores en la conversación, pero si se impugna su validez formal, debe insistirse en que

21. La reciente Sentencia 276/2017, de la Audiencia Provincial de Valencia, de 25 de abril de 2017, así lo recoge cuando señala que "cualquier medio de prueba que se proponga, deberá ser obtenido de forma lícita, de forma que, directa o indirectamente, no se violenten los derechos o libertades fundamentales. En otras palabras, el primer presupuesto de la aceptación de un mensaje de WhatsApp como prueba en un procedimiento, es que en su obtención no se hayan vulnerado ni el derecho a la intimidad ni el secreto de las comunicaciones".

22. Sentencia del Tribunal Supremo 517/2016 de 14 Junio 2016, 298/2013, de 13 de Marzo, o 45/2014, de 7 de Febrero, 298/entre otras muchas.

se determine en qué medida o párrafos están entrecortados, qué frases no se corresponden con la unidad de frase, o en qué expresiones existe una provocación de parte de quien graba para obtener una determinada conversación. Y que, finalmente, estas grabaciones privadas no atentan al derecho a no declarar contra sí mismo[23].

En relación al origen de la obtención de la información que se aporta al proceso caben dos posibilidades. La primera, consiste en aportar los datos contenidos en el dispositivo propio, del que es titular la propia parte procesal. La segunda, que se aporte por un sujeto ajeno a la conversación, posibilidad solo contemplada si se trata de la policía judicial previa autorización por parte de la autoridad judicial competente. Si la aportación tiene lugar por parte de uno de los miembros de la comunicación, esta se realizará *ex post facto*, al presentarse una vez realizada, y sin intervención judicial[24], ya que al ser parte de la conversación no hay vulneración del artículo 18.3 de la Constitución[25]. Es común en los delitos por violencia de género que la víctima aporte la comunicación de *WhatsApp* donde se contengan los insultos, amenazas, humillaciones o situaciones de acoso continuado que caracterizan estas tipologías delictivas. Respecto a la forma de acceso como prueba al proceso podrá tener lugar bien como prueba documental privada, bien como documental pública. En el supuesto que se aporte como documento privado, podrá ser a través de impresión o la simple imagen de un pantallazo. Si se aporta como prueba documental pública, habrá de acudirse a un fedatario público para que visualice el *WhatsApp* al objeto de dejar fiel reflejo de su contenido para su aportación al proceso[26].

No obstante, al no almacenar *WhatsApp* los mensajes en sus servidores y quedar únicamente registradas en los terminales móviles se corre el riesgo de manipular la fuente de prueba como cuando el usuario remitente o receptor eliminan la conversación y no dejan rasgo en su móvil. De igual forma, es posible colocar mensajes que realmente no han sido enviados como remitidos o suplantar la identidad utilizando un sistema informático que envía mensajes haciéndose pasar por el móvil suplantado, o

23. Fundamento jurídico de la Sentencia 291/2019, de 31 de mayo.
24. AGUSTINA SANLLEHI, J. R., "Algunas consideraciones sobre el denominado hacking judicial", *Iuris*, núm. 199, Sección Tribuna, 1 al 14 de octubre de 2013, p. 3.
25. Sobre este particular, vid. Sentencia del Tribunal Constitucional 11/1984, de 29 de noviembre "Quien graba una conversación de otros atenta, independientemente de otra consideración, al derecho reconocido en el artículo 18.3 CE; por el contrario, quien graba una conversación con otro no incurre, por este solo hecho, en conducta contraria al precepto constitucional citado".
26. PICÓ I JUNOY, J., "Retos del derecho probatorio ante las nuevas tecnologías" en *Inteligencia Artificial Legal y Administración de Justicia,* CALAZA LÓPEZ, S., LLORENTE SÁNCHEZ-ARJONA, M., (Dir.), *cit.*, p. 444.

bien sustrayendo el propio terminal móvil[27]. El Tribunal Supremo en su Sentencia 300/2015, de 19 de mayo[28], ha abordado el riesgo de manipulación de este tipo de pruebas que, si bien viene referida a una conversación mantenida en la red social Tuenti, fija los criterios para aceptar la fuerza probatoria de las capturas de pantalla o "pantallazos", en los que se refleja el contenido de mensajes transmitidos en las redes sociales. Conforme a la referida sentencia "la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido".

Esta cautela a que hace referencia el Tribunal Supremo encuentra todo su sentido si se tiene en cuenta la existencia de aplicaciones como *WhatsFake* capaces de generar chats de *WhatsApp* falsos. Esta App permite sustituir o suplantar una conversación real de *WhatsApp*, e incluyendo las fotos adecuadas en los remitentes, el resultado es imposible de diferenciar de un pantallazo real; así, se da la posibilidad de modificar la hora de envío, el estado de la recepción de un mensaje, el emisor o enviar audios, videos y fotos que se pueden configurar como mensajes[29]. Todo ello demuestra que

27. DELGADO MARTÍN, J., "La prueba de WhatsApp", *Diario La Ley*, Sección Tribuna, *cit.*, p. 8.

28. Crítico con esta sentencia se muestra BUENO DE MATA, F., "La validez de los pantallazos como prueba electrónica: comentarios y reflexiones sobre la STS 300/2015 y las últimas reformas procesales en materia tecnológica", *Diario La Ley*, núm. 8728, Sección Tribuna, 23 de marzo de 2016, cuando afirma que "aún así, pensamos que el TS ha dejado pasar con esta sentencia una oportunidad importante para dar recomendaciones más amplias a la hora de aportar pruebas electrónicas, que fueran más acordes con las cautelas que establecen al principio de la misma resolución. Nos encontramos ante un texto lleno de buenas intenciones y con cautelas muy válidas, pero que se pierde entre recomendaciones que no son aplicables al caso concreto que se resuelve y que no da un criterio claro para aportar fuentes de prueba electrónicas ni para que las mismas sean admitidas".

29. Al igual que en *WhatsApp*, para empezar un chat se tiene que marcar el icono de la esquina superior derecha. Una vez ahí, nos permite elegir el nombre del remitente, su foto, e incluso su estado actual. Cuando lo tenemos, se da a guardar y ya está

nos encontramos ante una prueba muy sensible que puede ser alterada al no existir respaldo de los servidores de las *App*. Por esta razón, en este tipo de pruebas se ha de ser extremadamente riguroso con la cadena de custodia. Sobre este particular, la Sentencia de la Sala II del Tribunal Supremo 375/2018, de 19 de julio, apunta, en referencia a la sentencia arriba mencionada que "no es posible entender, como se deduce del recurso, que estas resoluciones establezcan una presunción *iuris tantum* de falsedad de estas modalidades de mensajería, que debe ser destruida mediante prueba pericial que ratifique su autenticidad y que se debe practicar en todo caso; sino que, en el caso de una impugnación (no meramente retórica y en términos generales) de su autenticidad –por la existencia de sospechas o indicios de manipulación– se debe realizar tal pericia acerca del verdadero emisor de los mensajes y su contenido. Ahora bien, tal pericia no será precisa cuando no exista duda al respecto mediante la valoración de otros elementos de la causa o la práctica de otros medios de prueba".

Por tanto, resultará necesaria la prueba pericial informática cuando la información proporcionada por *WhatsApp* sea impugnada por la otra parte, en cuyo caso la persona que quiera valerse de dicha prueba deberá practicar una prueba pericial que identifique el origen de la conversación, de sus interlocutores y de su contenido. Sin embargo, no será necesaria prueba pericial informática cuando dichas comunicaciones corroboren hechos que se hayan expuesto mediante medios de prueba indubitada; en estos supuestos, su autenticidad podrá inferirse a partir de otros medios de prueba.

Ciertamente, condicionar todo el valor probatorio de la comunicación electrónica a que se aporte en el proceso un informe pericial que ratifique su veracidad no resulta una solución muy operativa, sobre todo, si tenemos en consideración que nos enfrentamos a una prueba altamente compleja y costosa. Además, para los supuestos de comunicación instantánea bidireccional la realización de la pericial requiere de los dos terminales de comunicación con absoluta garantía de la cadena de custodia desde el primer momento, con objeto de evitar cualquier posible manipulación o alteración de los mismos[30]. Es ajustada a la

el chat abierto. Da la posibilidad de escribir lo que se quiera y se publicará como si esa persona lo hubiese escrito. Se tiene la posibilidad de elegir si el mensaje está siendo enviado o recibido, y también decidir si queremos que el mensaje aparezca como no recibido, recibido o leído, dependiendo del símbolo de check que se elija. También se puede editar los mismos mensajes una vez escritos o incluso eliminarlos si se quiere cambiar el discurso que se va a recrear. Una vez finalizado, se hace una captura de pantalla normal y se le da a compartir.

30. Cfr. FUENTES SORIANO, O., Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías, *Revista General*

realidad la opinión sostenida por el Tribunal Supremo cuando afirma que la comunicación aportada mediante "pantallazos" puede llegar a alcanzar valor probatorio, sin necesidad de un informe pericial, si no es impugnada por las otras partes o resulta ratificada por otros medios de prueba. Es cuando se impugna la autenticidad que se hace necesario recurrir a la prueba pericial; no obstante, no hay que perder de vista que la valoración de la prueba la llevará a cabo el juez conforme a las reglas de la sana crítica y que el convencimiento sobre su credibilidad podrá venir apoyado por otros medios de prueba, de forma tal que cuando se proceda a la valoración conjunta de la prueba la pretendida falta de autenticidad puede quedar contradicha por otros medios, como la ratificación del contenido por parte de los interlocutores, que se facilite el acceso a la fuente original o que existan contradicciones en lo declarado por el acusado[31]. Es en el supuesto de impugnación cuando resulta discutible su validez como prueba precisando del correspondiente peritaje informático, si bien, la última palabra la tendrá el juez que seguirá la regla general en materia de prueba electrónica sometiendo su eficacia probatoria a las reglas de la sana crítica[32].

3. LAS REDES SOCIALES COMO INSTRUMENTO DE VIOLENCIA

La facilidad de conexión, la inmediatez y la generalización de las redes sociales para estar en contacto, están generando una particular manera de comunicarse. La sociedad actual se halla fuertemente influenciada por el notable impacto que ha supuesto la intromisión de las redes sociales[33] en la vida diaria de las personas en donde se dan a conocer sentimientos, relaciones amorosas o sociales, compromisos profesionales, eventos sociales, viajes…, pasando a ser un escaparate de nuestra vida y exponiendo nuestra intimidad de una forma tal que resulta desconocida

de Derecho Procesal, núm. 44, Enero 2018, p. 23, que apunta muy acertadamente su discrepancia con "las rotundas afirmaciones vertidas mayoritariamente por ingenieros y peritos informáticos que tienden a presentar la prueba pericial informática como único mecanismo posible de adveración de la comunicación electrónica".

31. ARMENTA DEU, T., "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales)", *cit.*, p. 73.
32. ARRABAL PLATERO, P., "El WhatsApp como fuente de prueba" en *El proceso penal: cuestiones fundamentales, cit.*, p. 335.
33. Una red social es una estructura social formada por personas o entidades, que se mantienen conectadas y unidas entre sí por algún tipo de relación o interés común. Según ORIHUELA, J.L., *Mundo Twitter,* Ed. Alienta, Barcelona, 2011, "las redes sociales operan como un sistema sináptico que facilita la organización de sus participantes y la hiperconectividad, que permite construir conglomerados de relaciones y descubrir patrones comunes de pensamiento".

hasta el momento actual. Nuestro día a día se desnuda ante un público conocido y desconocido, sumergiéndose en un universo virtual del que perdemos el control una vez que decidimos volcar un determinado contenido, video o foto en red. Y es, precisamente, en este mundo virtual donde actitudes como el insulto, la amenaza o el chantaje se diluyen en un marco de normalidad, ampliando el control diario sobre las actividades de la pareja o expareja.

Internet se ha convertido en una revolución tecnológica que ofrece posibilidades ilimitadas y que nos aporta múltiples ventajas como forma de comunicación global; es un escaparate abierto al mundo que una vez se activa resulta imposible de detener. Es por ello que cuando una mujer es víctima de un delito cometido a través de redes sociales se enfrenta no solo al acto ilícito en sí, sino también, en ocasiones, al escarnio público; aquí, el grado de lesividad es más intenso al ir dirigido a un mayor número de destinatarios. Las redes sociales han introducido un nuevo escenario para la comisión de hechos delictivos, un escenario propicio amparado por su uso masivo y por el anonimato que proporciona que hace que las investigaciones se tornen especialmente complejas y de difícil resolución. Ahora bien, los delitos que se cometen en las redes sociales se mueven en un escenario distinto a los supuestos perpetrados a través de plataformas de comunicación instantánea, analizados con anterioridad, ya que en estos casos la información si queda temporalmente almacenada en un servidor haciendo que las labores de rastreo resulten más sencillas[34].

En este contexto, el agresor busca dañar la reputación de su pareja o expareja generándole un tipo de presión psicológica y moral que puede tener graves implicaciones, colgando fotos o comentarios que afectan la integridad moral y emocional de la mujer dejándola expuesta ante conocidos y desconocidos. De igual forma, se puede ejercer este tipo de violencia controlando las amistades que tiene en red, exigiendo que elimine fotos de su perfil, u obligando a dar de baja en sus redes a contactos que no son de su agrado[35]. Son múltiples las sentencias de las Audiencias Provinciales que condenan por la difusión a través de redes sociales de material íntimo, como la SAP de Barcelona 742/2017, de 7 de septiembre[36], que

34. FUENTES SORIANO, O., *Los procesos por violencia de género. Problemas probatorios…, cit.*, p. 26.
35. VARGAS GALLEGO, A. I., "Nuevas formas de violencia contra las mujeres. Redes sociales. Delitos de descubrimiento y revelación de secretos", https://lefebvre.es/, febrero 2013, p. 2.
36. Sentencia n.º 742/2017 de la Audiencia Provincial de Barcelona, Sección 20.ª, Septiembre 07, 2017. Vlex Global.

confirma la condena del Juzgado de lo Penal[37] por delito de malos tratos en el ámbito familiar y un delito de descubrimiento y revelación de secretos al haber difundido el condenado a través de Facebook cinco grabaciones de video de un encuentro sexual mantenido con su expareja, con una "preclara voluntad de atentar a su intimidad y dignidad personal, atendiendo al contenido de las mismas"; la SAP de Málaga 107/2016, de 23 de marzo[38], que condena por un delito de revelación de secretos del artículo 197.2 CP por la creación de un perfil falso en Facebook y Badoo a nombre de su expareja insertando una foto de ella, además de mensajes provocativos con la finalidad de hacerla objeto de requerimientos sexuales por parte de terceros; o la SAP de Burgos 136/2017, de 2 de mayo[39], por la que se condena a un sujeto que publicó en su Facebook documentos que poseía legítimamente como parte de un proceso en los que figuraban datos personales de su expareja, así como insultos contra ella. Todas estas actuaciones se realizan sabiendo que cualquier persona que acceda a las redes sociales puede tomar conocimiento de los datos que se vuelquen, en perjuicio de la intimidad de las víctimas, con la intención de causarle un perjuicio personal y social.

Aún cuando no existe un precepto que regule la aportación de fuentes de prueba de estas características, tanto la acusación particular como el Ministerio Fiscal pueden proporcionar la información que se contiene en las redes sociales en cualquiera de las formas legalmente permitidas, bien como prueba documental a través de pantallazos o aportando el PC en el que consta la comunicación, alcanzando valor probatorio mediante la ratificación de los extremos cuestionados a partir de la toma en consideración de otros medios de prueba practicados en la causa[40], como el interrogatorio de partes o de testigos cuyas declaraciones pueden arrojar luz respecto de los contenidos publicados en una determinada red social. En este sentido, no hay que olvidar que en nuestro derecho procesal penal rige el sistema de libre valoración de la prueba, consagrado en el artículo 741 de la Ley de Enjuiciamiento Criminal, que autoriza al Juez o Tribunal a formar su íntima convicción sin otro límite que los hechos probados en el juicio oral, así como con el empleo de las normas de la lógica y la experiencia.

37. Sentencia dictada por el Juzgado de lo Penal n.º 28 de Barcelona en el Procedimiento Abreviado n.º 128/17.
38. Sentencia n.º 107/2016 de la Audiencia Provincial de Málaga, Sección 8.ª, Marzo 23, 2016. Vlex Global.
39. Sentencia n.º 136/2017 de la Audiencia Provincial de Burgos, Sección 1.ª, Mayo 02, 2017. Vlex Global.
40. FUENTES SORIANO, O., *Los procesos por violencia de género. Problemas probatorios…*, *cit.*, p. 32; ARMENTA DEU, T., "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales"…, *cit.*, p. 74.

III. QUEBRANTAMIENTO DE LA PROHIBICIÓN DE COMUNICACIÓN A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS

El lugar de ejecución del delito ya no es tan solo un espacio físico, perfectamente perceptible por los sentidos; las nuevas formas de ciberdelincuencia se desarrollan en un universo virtual en el que la pena de privación de acudir a determinados lugares tiene cabida en estos espacios virtuales en los que el delito se haya cometido. En este sentido se ha pronunciado el Tribunal Supremo al sostener que si pueden tener la consideración de "lugar de comisión del delito" los espacios virtuales de encuentro y comunicación que se crean en Internet, máxime si nos enfrentamos a delitos que pueden entenderse cometidos por Internet[41]. Es, por ello, que debe evolucionarse hacia una visión no estrictamente gramatical del término "lugar del delito" y extenderla a los "espacios de difusión", porque las redes sociales no son tan solo el instrumento para la comisión de determinados delitos sino también el escenario en el que se cometen algunos delitos. Es por esta razón que la Sala de lo Penal del Tribunal Supremo declara que la imposición de la pena de prohibición de acudir al lugar del delito se puede referir a la prohibición de acceso a una determinada red social.

Pues bien, el artículo 468.2 del Código Penal hace referencia al delito de quebrantamiento de condena, sancionando con pena de prisión de seis meses a un año a todos aquellos condenados que quebranten una pena referida al derecho de residir o acudir a determinados lugares, medida cautelar o medida de seguridad impuesta en el marco de un proceso por violencia de género. Esta prohibición de comunicación está prevista en el artículo 39.h) del Código Penal como una pena privativa de derechos, y desarrollada posteriormente en el artículo 48.3 del mismo cuerpo legal. Además, se puede imponer también como medida cautelar en el marco

41. Sentencia del Tribunal Supremo, Sala de lo Penal, 547/2022, de 2 de junio. En este mismo sentido, la Sentencia del Tribunal Supremo 4/2017, de 18 de enero, apunta que "la extensión actual de las nuevas tecnologías al servicio de la comunicación intensifica de forma exponencial el daño de afirmaciones o mensajes que, en otro momento, podían haber limitado sus perniciosos efectos a un reducido y seleccionado grupo de destinatarios. Quien hoy incita a la violencia en una red social sabe que su mensaje se incorpora a las redes telemáticas con vocación de perpetuidad. Además, carece de control sobre su zigzagueante difusión, pues desde que ese mensaje llega a manos de su destinatario éste puede multiplicar su impacto mediante sucesivos y renovados actos de transmisión. Los modelos comunicativos clásicos implicaban una limitación en los efectos nocivos de todo delito que hoy, sin embargo, está ausente. Este dato, ligado al inevitable recorrido transnacional de esos mensajes, ha de ser tenido en cuenta en el momento de ponderar el impacto de los enunciados y mensajes que han de ser sometidos a valoración jurídico-penal".

de una orden de protección para las víctimas de violencia doméstica en los términos que se prevén por el artículo 544 ter de la LECr, o como una medida de seguridad, conforme al artículo 106.1 f) del Código Penal. A los efectos de integrar este delito es indiferente que la prohibición de comunicación se haya impuesto como pena, medida cautelar o medida de seguridad. La prohibición de comunicarse con la víctima o con aquellos familiares o personas que determine el Juez o Tribunal, impide al penado establecer contacto con ellas, por cualquier medio de comunicación, bien sea informático o telemático, escrito, verbal o visual.

Aún cuando este delito de quebrantamiento de condena está ubicado entre los "Delitos contra la Administración de Justicia", del Título X del Libro II del Código Penal, tanto la Jurisprudencia[42] como la Doctrina le reconocen un doble bien jurídico protegido cuando las penas o medidas cautelares se adoptan en un proceso por violencia de género, ya que, junto con el correcto funcionamiento de la Administración de Justicia, estas conductas suponen un ataque a la seguridad y tranquilidad de la persona a la que se pretende proteger. Por tanto, la finalidad principal "es la de proteger a las víctimas directas del delito de la victimización secundaria derivada del posible encuentro con el autor del delito y, fundamentalmente, excluir el riesgo de que se puedan llegar a verificar nuevas lesiones en los bienes jurídicos protegidos de éstas o de terceros. Siendo ésta la finalidad atribuida por el legislador a la privación del derecho a acudir a determinados lugares, la consideración de que tales lugares dan cabida a los espacios virtuales en que el delito haya sido cometido en modo alguno implica separarse de la finalidad prevista: tal privación impide la reiteración de la conducta lesiva para el bien jurídico en cada caso protegido, ya sean bienes jurídicos personalísimos –como puede suceder en los delitos contra el honor, la intimidad o la integridad moral cometidos en redes, foros o páginas de Internet– o bienes jurídicos colectivos como puede suceder en los delitos de terrorismo en relación al adoctrinamiento o captación,

42. En concreto, la Sala II del TS en su sentencia 846/2017, de 21 de diciembre, apunta que "la situación jurídica creada por la prohibición de acercamiento y comunicación dispuesta prohíbe al condenado el acercamiento a la víctima, pena aflictiva, y protege a la víctima evitando situaciones de peligro. Esta doble dimensión de la medida permite individualizar cada acto de aproximación a la víctima como acto típico del delito de quebrantamiento pues en cada acto se reproduce el ataque a la seguridad dispuesta por la prohibición de acercamiento". De igual forma, la Sentencia de la Sala II del TS 664/2018, de 17 de diciembre, establece "una especial configuración de la modalidad que analizamos, la del artículo 468.2 CP, que además de compartir con los quebrantamientos incluidos en el número 1 del artículo 468 CP como bien jurídico objeto de protección la efectividad de determinadas resoluciones de la Autoridad Judicial en materia de ejecución de penas, medidas de seguridad y medidas cautelares acordadas durante el proceso, persigue como finalidad última la de prevenir situaciones de peligro para las víctimas".

enaltecimiento o justificación de los delitos de terrorismo o delitos relacionados con la distribución de pornografía infantil"[43].

Si las órdenes de alejamiento en el espacio físico se suelen quebrantar de diversas formas, cuando nos movemos en el espacio virtual las redes sociales se convierten en el lugar perfecto para romper con las medidas de alejamiento y prohibición de comunicaciones. De hecho, a día de hoy, los quebrantamientos de condena están relacionados con los sistemas de mensajería o con redes sociales en más de un 80% de los casos. Lógicamente, si la comunicación es directa a través de mensaje privado con la víctima no existen dudas en cuanto a la comisión del hecho delictivo, el problema puede llegar a plantearse en otros tipos de interacciones que ofrecen las redes sociales y que pueden plantear problemas a la hora de determinar si se ha producido un quebranto de la prohibición de comunicación[44].

Comenzando por *WhatsApp*, el posible delito de quebrantamiento a través de esta aplicación puede provenir de los "estados" de *WhatsApp* o de la participación en grupos comunes. Las fotografías o textos escritos que se pueden subir a la aplicación con una duración temporal de 24 horas y que se conocen como "estados" pueden ser visualizados por los contactos de la persona que los comparte. En el supuesto que el investigado o condenado ponga un estado de *WhatsApp* refiriéndose a la perjudicada, pero sin remitírselo expresamente a la misma, los pronunciamientos emitidos hasta el momento actual por la jurisprudencia de las Audiencias Provinciales no se muestran uniformes, ya que mientras en la mayor parte de las resoluciones, se ha considerado que no se quebranta la prohibición de comunicación, sin perjuicio que pueda constituir un delito de injurias según el contenido de lo que se publique, otras estiman que este quebrantamiento si tiene lugar. En este último sentido, la SAP Valladolid de 14 de abril de 2015[45] establece que "la información que se coloca en el 'estado de WhatsApp' por parte de un usuario de la citada aplicación, es una información que se pone para que pueda ser visualizada y conocida por todos los que tengan ese número de teléfono móvil incorporado a su teléfono, pero en este caso el acusado aprovechaba el subterfugio del 'estado de *WhatsApp*' para quebrantar la prohibición de comunicación que se le había impuesto, pues en vez de ofrecer algún dato que pudiera servir para su identificación, lo que hacía era mandar unas comunicaciones dirigidas de manera específica hacia la persona con la que se le había dicho que no se podía comunicar, comunicaciones que además tenían un claro

43. Sentencia del Tribunal Supremo, Sala de lo Penal, 547/2022, de 2 de junio.
44. GUTIÉRREZ MAYO, E., "Quebrantamiento de la prohibición de comunicación a través de las redes sociales", de 4 de mayo de 2018, www.elderecho.com.
45. Número de recurso 263/2015.

contenido injurioso, y en las que además, por el método utilizado, provocaba que sus expresiones cuando menos injuriosas gozaran de cierta publicidad, precisamente entre todos sus contactos de '*WhatsApp*', por lo que se comparte que el acusado sí ha quebrantado la orden de prohibición de comunicación que tenía y que también ha cometido las faltas de injurias por las que ha sido condenado". Por el contrario, el sentir mayoritario de la jurisprudencia se refleja en la SAP de Ciudad Real de 21 de enero de 2019[46], que viene "a sostener la atipicidad de la conducta al no tratarse de actos de comunicación y requerirse la colaboración activa de la persona afectada que debe necesariamente entrar o indagar en esos denominados estados, pero sin que se produzca un acto real de comunicación. No hay, en sentido formal, un emisor del mensaje, sino la mera configuración de eso que se denomina estado del usuario de la cuenta. Si es factible que de lo relacionado en ese concreto estado pudiera derivarse posibles delitos de amenazas o coacciones o injurias o acoso…mas no puede hablarse de establecimiento de comunicación con quebranto de la orden fijada judicialmente"[47].

46. Número de recurso 72/2018.

47. Sentencia de la Sección 27.ª de la Audiencia Provincial de Madrid de 26 de junio de 2018, que confirma la sentencia absolutoria de instancia, por cuanto no puede obviarse que "…su acceso no deriva de una conducta del acusado, sino de la de la propia recurrente, que ha de acceder a la cuenta de WhatsApp de él, y entrar, de forma expresa en su contenido, para conocer las frases, pensamientos, ideas, consignas, etc., que el titular de la cuenta haya podido hacer constar en su estado" Y con mayor claridad la Sentencia de la Sección 7.ª de la misma Audiencia Provincial de Madrid de 19 de marzo de 2018, que revoca la de instancia, absolviendo del delito de quebrantamiento por cuanto "…no es el ahora condenado quien se dirigió a la víctima sino que fueron otros, terceros ajenos a este procedimiento, los que comunicaron las incidencias que se iban produciendo en el estado del perfil del WhatsApp del ahora recurrente y desde luego no podemos entender que esa conducta tenga encaje en el delito de quebrantamiento de condena puesto que el condenado no se dirigió a Antonia, ni se comunicó con ella por ninguno de los medios que se indican en la sentencia, ni tampoco encargó a otro que le dijera algo en su nombre sino que esas terceras personas visitaron el perfil del WhatsApp de Humberto y se lo comunicaron a Antonia, entendiendo que la condena sobrepasa en exceso los términos del art. 468.2 del C. Penal por el que ha sido condenado y por lo tanto deberá ser absuelto de ese delito, pudiendo tener encaje esa conducta en el tipo de acoso que al no ser homogéneo con el de quebrantamiento de condena no vamos a examinar". Sentencia de la Sección 6.ª de la Audiencia Provincial de Vizcaya de 8 de mayo de 2017, que igualmente absuelve del delito de quebrantamiento por el que había sido condenado el recurrente, pues aunque "…reconoció a lo largo de todo el procedimiento, que escribió en su estado de WhatsApp el texto que aparece recogido en el relato de hechos probados de la sentencia apelada, pero que en ningún momento iba dirigido a la denunciante; que la tenía 'bloqueada', y que ella no podía ver ni el estado, ni enviar o recibir mensajes desde su terminal, extremo no controvertido, ya que reconoció aquélla que es cierto que fue su hija Catalina quien leyó el estado de WhatsApp de Justiniano y se lo contó a su madre. Claudia manifestó igualmente a lo largo de todo el procedimiento

De igual forma, se produce un quebrantamiento de condena en aquellos supuestos en que la víctima sube una foto o un texto como "estado" y se visualiza por el victimario. Parece lógico sostener que, en estos casos, se puede también entender que se quebranta la prohibición de comunicación ya que la perjudicada va a constatar en su móvil que el investigado ha visualizado su estado. Puede argumentarse en contra que la víctima puede bloquear de sus contactos al victimario, pero lo cierto es que no puede hacerse recaer sobre ella semejante obligación. Cuando el investigado o condenado mira el estado de *WhatsApp* de la víctima es consciente que ella recibirá en su teléfono la información de que ha visto su estado, lo que equivale a un mensaje indirecto de "he visto tu estado", que en vez de ser escrito se constata de este modo por la aplicación. Esto mismo puede aplicarse en las "*Stories*" de Instagram o Facebook. Lógicamente, esta afirmación tiene sentido si estas visualizaciones se producen de forma reiterada pudiendo provocar en la víctima un quebranto en su sensación de seguridad que es uno de los bienes jurídicos protegido en este delito de quebrantamiento[48]. En el supuesto que ambos pertenecieran a un mismo grupo de *WhatsApp*, dado que no se puede obligar a la persona perjudicada a que abandone el citado grupo, debe ser el condenado o investigado quien lo haga o, en su caso, abstenerse de participar ya que siempre que escriba un mensaje se está produciendo un proceso de transmisión de información entre el emisor-condenado y el resto del grupo, incluida la víctima, que quebranta la prohibición de comunicación.

---

que tenía 'bloqueado' al denunciado". Cita esta última Sentencia la de la Sección 3.ª de la Audiencia Provincial de Cantabria de 13 de octubre de 2014 que aún referido a delito de amenazas sostuvo que no se podía cometer tal delito mediante el denominado estado de WhatsApp. Sentencia de la Sección 26.ª de la Audiencia Provincial de Madrid de 28 de enero de 2016 "…las expresiones ya consignadas fueron proferidas por el acusado incorporándolas y manteniéndolas durante un cierto tiempo en su estado de WhatsApp. Es decir, no nos encontramos aquí ante mensajes remitidos por el acusado a una concreta destinataria (ni, por tanto, a la ahora recurrente)… Es notorio que para conocer las expresiones o mensajes que pueden contenerse en un determinado estado de WhatsApp, en la medida en que éstas no sean enviadas junto a cualquier otro mensaje a un tercero, es preciso que éste sea quien, entre los 'contactos' que figuren en su propia agenda de dicha aplicación, seleccione el de la persona de su interés para conocer el 'estado' que, sin un destinatario en particular, ha decidido consignar…En el supuesto analizado, y respecto a si la publicación del texto en su estado de WhatsApp supuso la vulneración de la prohibición de comunicación con la denunciante, existen, al menos a juicio de esta Sala, dudas razonables acerca de que el acusado tuviera el propósito de que su frase llegara siquiera al conocimiento de Claudia, faltando el principal elemento de comunicación establecido en la prohibición descrita en la medida impuesta; consideraciones que determinan la necesidad de revocar el fallo condenatorio de la sentencia apelada, y absolver al Sr. Justiniano también del delito de quebrantamiento de medida cautelar".

48. GUTIÉRREZ MAYO, E., *Quebrantamiento de la prohibición de comunicación a través de las redes sociales, cit*.

Si atendemos a la red social Facebook hay que diferenciar diversas situaciones en función de las posibilidades de interacción que proporciona esta red social. Así, si se escribe un comentario en alguna foto que suba la víctima o se publica algo en su muro, no cabe duda de que nos encontramos con un acto de comunicación; lo mismo que si se nombra o etiqueta en cualquier publicación o fotografía del que tiene la prohibición de comunicación al salir publicada en el propio muro de la víctima. Otra manera de quebrantar la prohibición de comunicación es dando al "me gusta" en una publicación de la víctima. En este sentido, la sentencia de la Audiencia Provincial de Madrid 291/2017, de 20 de noviembre de 2017, señala que "es sabido que constituiría un hecho delictivo de quebrantamiento del artículo 468 CP el hecho de que un condenado de pena de prohibición de comunicación enviara por cualquier medio de comunicación un simplemente ¿Cómo estás?… De ahí que expresiones tales como un 'me gusta' a una foto o comentario del titular de un perfil subida a Facebook por el denunciante, supondría un acto de comunicación al serlo entre afectado/condenado por la orden de prohibición de comunicación 'por cualquier medio' y el perjudicado, ya que ello es lo que pretende que no ocurra con la pena, esto es, que el condenado no se comunique "de ninguna manera" con la víctima". Además, no se puede hacer descansar sobre la víctima la obligación de bloquear o eliminar, ya que es el acusado el que tiene dicha obligación legal de no comunicarse con ella[49]. Se considera acertadamente por los Tribunales que un "me gusta" en Facebook se debe considerar una comunicación, por lo que dicha acción llevaría a la consumación del delito de quebrantamiento de condena. Esta actuación aplicable a Facebook se puede trasladar a otras redes sociales.

Recientemente, el Pleno de la Sala de lo Penal del Tribunal Supremo en su sentencia 553/2022, de 2 de junio, confirma la condena por quebrantamiento de medida cautelar consistente en una prohibición de comunicación con su ex pareja por cualquier medio, incluido Internet, al escribir unos textos en *Google+* a sabiendas de que llegarían a la víctima. En su sentencia considera que "las redes sociales –Google+ o cualquiera otra más activa y extendida– no pueden servir de escudo para incorporar

49. Sentencia de la Audiencia Provincial de Barcelona, Sección 20, de fecha 2 de mayo de 2016 establece "Pues bien, dado el funcionamiento de la red social Facebook resulta evidente que el acusado, al acceder al perfil de la denunciante y darle al 'me gusta', lo hizo con la intención y pleno conocimiento de que llegaría y sería visto por la denunciante, titular del perfil, por lo que se trata de un mensaje dirigido a la misma, sin que pueda hacer descansar en la denunciante la obligación de bloqueo o eliminación, pues es el acusado quién tiene la obligación legal de no comunicarse con ella y al hacerlo, aún cuando sea mediante un 'me gusta', infringió la prohibición de comunicación. Es por ello que la conducta del acusado reúne todos los requisitos del delito de quebrantamiento de condena".

mensajes que, amparados en la generalidad de una u otra reflexión, escondan un recordatorio a una persona protegida por decisión jurisdiccional". Añade que lo verdaderamente determinante no es –frente a lo que alega la defensa– que los "pensamientos o reflexiones" deban entenderse como simples enunciados que no están dirigidos a una persona concreta, sino que esas palabras, una vez contextualizadas, tengan un destinatario respecto del que existe una prohibición judicial de comunicación y que su contenido llegue a su conocimiento. Se afirma por la Sala que resulta "evidente que ese destinatario ha de dibujarse de forma inequívoca, sin necesidad de un esfuerzo interpretativo que convierta artificialmente un enunciado general en un mensaje concebido como vehículo para una comunicación proscrita por el órgano jurisdiccional. Y para que el quebranto de esa prohibición adquiera relevancia penal es suficiente con que, de una u otra forma, el mensaje incorporado a una red social alcance su objetivo y tope con su verdadero destinatario". Y es que precisa que "el carácter multitudinario del uso de las redes sociales y la multiplicación exponencial de su difusión, lejos de ser un obstáculo que debilite el tipo subjetivo –esto es, el conocimiento de que esas palabras van a llegar a la persona protegida– refuerza la concurrencia del dolo. El autor sabe o se representa que ese mensaje que quebranta la prohibición puede alcanzar, por una u otra vía, a su destinatario. De ahí que la Sala no comparta el velado reproche que se formula a la denunciante por el hecho de no '… haber bloqueado la comunicación con el acusado'. La Sala expone que la persona en cuyo favor se ha dictado una medida cautelar que incluye la prohibición de comunicarse 'no asume la obligación de desconectarse de canales telemáticos o redes sociales anteriormente activos, de suerte que la omisión de esta medida pudiera influir en el juicio de subsunción. Es, por el contrario, el investigado el verdadero y único destinatario de la prohibición y el que ha de adoptar todas las medidas indispensables para que esa comunicación bidireccional no vuelva a repetirse'". Por lo que, se concluye por el Pleno, que "Conforme a esta idea, parece indudable que las afirmaciones '…espero tu llamada por favor' '…me puedo morir de asco para saber qué tiene mi hijo. Ya está bien no? Llevo desde el jueves así sin saber nada, ¡por favor!' son algo más que reflexiones compartidas sobre la soledad en fechas navideñas. Encierran un mensaje que cobra pleno sentido si se conecta su literalidad con el conflicto familiar que une a la pareja y en cuyo seno el acusado ejecutó actos que justificaron la medida de protección".

Por consiguiente, el fundamento de la prohibición de comunicación ha de encontrarse en la necesidad de evitar la victimización secundaria, con los perjuicios psicológicos que supondría una mera comunicación en

el que la víctima sufriera ese temido contacto con su agresor. En reiteradas ocasiones, el temor de la víctima no es tan solo por la presencia física del condenado, sino, también, por un acto de comunicación virtual del investigado o condenado. Las múltiples posibilidades de interacción que ofrecen las redes sociales suponen un reto a la hora de determinar si se ha producido o no un quebrantamiento de la prohibición de comunicación, pero, en ningún caso, pueden amparar conductas que impliquen una interacción en las que el investigado o condenado sabe, positivamente, que está haciendo llegar un mensaje a la víctima que contribuya a quebrantar la indemnidad de la víctima que, junto con el correcto funcionamiento de la Administración de Justicia, constituyen los bienes jurídicos protegidos.

Capítulo 16

Víctimas de violencia de género, justicia restaurativa y utilidad de los ODR[1]

Blanca Otero Otero

Profesora Ayudante Doctora de Derecho Procesal
Universidad de Vigo

I. INTRODUCCIÓN

A lo largo de los últimos tiempos, se ha venido evidenciando que la justicia penal no ha atendido de forma conveniente las necesidades de las víctimas. La víctima del delito ha sido la gran olvidada dentro del proceso penal y, en no pocas ocasiones, el proceso penal ha causado y causa un perjuicio a la víctima; constituyendo ese paso por el sistema judicial, a menudo, una experiencia que reporta insatisfacción y dolor a muchas de las víctimas.

El propio proceso puede dar lugar a lo que se ha venido llamando victimización secundaria y, en consecuencia, no ayuda a hacer frente a la reparación del daño derivado del delito. Los sistemas de justicia penal se han focalizado en la condena de los delincuentes y no han atendido profundamente la reparación efectiva del daño derivado del hecho delictivo, constriñendo a la víctima a un mero papel secundario[2].

1. Este trabajo ha sido elaborado en el marco del proyecto de investigación "Respuesta jurídica y socioeducativa a la violencia de género ejercida por menores. Protección de la víctima e intervención con el menor agresor", subvencionado por el Ministerio de Ciencia e Innovación, Proyectos de I+D+I" dentro de los Programas Estatales de Generación de Conocimiento y Fortalecimiento Científico y Tecnológico del Sistema de I+D+I y de I+D+I orientada a los Retos de la Sociedad en la convocatoria de 2019, (Ref. PID2019-106700RB-I00).

2. MONTESDEOCA RODRÍGUEZ, D., *Justicia restaurativa y sistema penal*, Tirant lo Blanch, Valencia, 2021, p. 78.

En lo referente a las víctimas de violencia de género, esta respuesta punitiva –en la cual se priva a la víctima de cualquier control sobre la intervención penal en cuestiones que afectan directamente a su vida cotidiana– parece no haber conseguido el efecto de prevención que podría beneficiar a las futuras víctimas; e igualmente, la asistencia a las víctimas de violencia podría señalarse insuficiente y en gran parte condicionada a la intervención judicial[3]. Es así que, la denuncia penal o el inicio de las actuaciones penales, no siempre ofrecen alguna solución a la víctima de violencia de género.

En este sentido, aun cuando se adopten medidas de protección a la víctima –orden de protección y prohibición de comunicación–, no existe un acompañamiento real de la misma ni se examinan sus necesidades e intereses, generando en la mujer víctima de violencia de género una sensación de abandono, insatisfacción e incomprensión tanto por las instituciones como por parte de la sociedad en general. Igualmente, el investigado y condenado, recibe una respuesta punitiva, acompañado de una prohibición de aproximación que a menudo impide o dificulta una relación normalizada con los hijos comunes, aumentándose así tanto la frustración como la insatisfacción y generándose posibles conflictos futuros que pueden contribuir a nuevos episodios de violencia[4].

Por tanto, puede señalarse que estamos en presencia de determinadas situaciones conflictivas que, por su especial naturaleza, o por las circunstancias concurrentes en las mismas, precisan de otro tipo de intervenciones de carácter multidisciplinar que vengan a ofrecer una solución más adecuada, o respuestas más globales e integrales y así, satisfacer las necesidades e intereses de estas víctimas[5].

3. Señala GUARDIOLA LAGO ("La víctima de violencia de género en el sistema de justicia y la prohibición de la mediación penal", *Revista General de Derecho Penal*, 12, 2009, p. 14) "Las víctimas de delitos están más interesadas en una asistencia y una reparación por el delito cometido, cosa que incluye una validación externa, un reconocimiento del daño causado y un esfuerzo por repararlo".

4. GEMME, "Aportes del grupo de trabajo de Justicia Restaurativa", pp. 17-18. (https://mediacionesjusticia.com/aportes-alep, última consulta: 13/09/2022).

5. Como refiere OUBIÑA BARBOLLA ("La distancia que les separa, la distancia que nos separa: mediación en casos de violencia doméstica en España y en otros sistemas", GARCIANDÍA GONZÁLEZ, P. M. y SOLETO MUÑOZ, H. (Dirs.) *Sobre la Mediación Penal (Posibilidades y Límites en un Entorno de Reforma del Proceso Penal Español),* Thomson Reuters Aranzadi, Navarra, 2012, pp. 184-185) "la violencia de género encierra un conflicto jurídico y humano complejo en la medida en que se produce un hecho delictivo que lesiona un bien jurídico que todos hemos entendido digno de protección y que por eso se tipifica en el Código Penal. Sin embargo, la violencia de género también incluye un conflicto personal entre dos personas que mantienen o han mantenido una relación afectiva de mayor o menor duración; es más en muchas ocasiones esa relación continúa a pesar de la violencia".

En este contexto, no resulta difícil constatar que, en los últimos años se han producido importantes cambios que han ido centrando y realzando las necesidades de la víctima. La orientación de la justicia penal hacia la víctima se ha producido como consecuencia de una progresiva concienciación de la necesidad de conferirle la consideración que, ineludiblemente, debe ostentar en el proceso. Se hace necesario que a la víctima se le permita intervenir, con la finalidad de alcanzar una reparación por el daño sufrido además de recuperar un sentimiento de seguridad vital[6].

De esta manera, se han abierto paso determinadas corrientes tendentes a la reivindicación de la transcendencia e importancia de la víctima; en este sentido, ha irrumpido la Victimología, que ha contribuido en buena medida a paliar esta situación de olvido de la víctima[7]. Igualmente, diferentes movimientos tales como las teorías abolicionistas o los movimientos feministas, entre otros, han suscitado un cambio dogmático del Derecho Penal a través de la inclusión de políticas favorecedoras de la justicia restaurativa y de la víctima[8]. Como señala BARONA VILAR, se inicia un movimiento de "redescubrimiento" de la víctima, dado que durante siglos fue la gran olvidada, hasta el extremo que la doctrina venía afirmando que la víctima vivía en un vacío legal que implicaba una situación de inferioridad en el ámbito procesal respecto de los sujetos intervinientes en el proceso[9].

De este modo, desde lo que se viene conociendo como el feminismo de tercera ola, se han ido destacando los efectos positivos de la aplicación de mecanismos de justicia restaurativa como forma de satisfacer las necesidades de las víctimas, favorecer en mayor medida la admisión de responsabilidad de los hechos cometidos por parte del infractor e incrementar las posibilidades de condena de la violencia[10].

---

6. OTERO OTERO, B., "Víctima y justicia restaurativa en la justicia de menores", en PILLADO GONZÁLEZ, E. (Dir.), *La víctima en el proceso penal de menores: Tratamiento procesal e intervención socioeducativa*, Dykinson, 2021, p. 144.
7. *Vid*. MONTESDEOCA RODRÍGUEZ, D., *Justicia restaurativa y sistema penal*…, p. 74-78.
8. BARONA VILAR, S., "Mirada restaurativa de la justicia penal en España, una bocanada de aire en la sociedad global líquida del miedo y de la securitización", en SOLETO MUÑOZ, H. (Dir.) y CARRASCOSA MIGUEL, A. (Dir.) *Justicia restaurativa: una justicia para las víctimas*, Tirant lo Blanch, Valencia, 2019, p. 59.
9. BARONA VILAR, S., *Mediación penal. Fundamento, fines y régimen jurídico*, Tirant lo Blanch, Valencia, 2011, pp. 95-96.
10. VILLACAMPA ESTIARTE, C., "Justicia restaurativa en supuestos de violencia de género en España: situación actual y propuesta político-criminal", *Política Criminal: Revista Electrónica Semestral de Políticas Públicas en Materias Penales,* Vol. 15, N.º 29, Julio 2020, p. 56.

La justicia restaurativa tiene como objetivo romper la dicotomía víctima-agresor, intentado variar los papeles predeterminados que se asignan a los mismos en el curso del proceso judicial. En este sentido, permite al infractor restaurar en la medida de lo posible las consecuencias de sus actos y a las víctimas la posibilidad de participar en dicha reparación; situando a su vez a la comunidad, en una posición protagonista[11].

De forma más concreta, en relación con los supuestos de violencia de género, debe reseñarse el potencial que la justicia restaurativa puede llegar a tener para hacer frente a las necesidades psicológicas de los involucrados en este tipo de episodios de violencia. Es así que, puede ayudar a disminuir la intensidad de la ansiedad y sentimientos negativos que las partes suelen experimentar al enfrentarse al proceso judicial; en el sentido de que estas prácticas restaurativas, permiten a las partes expresar una serie de emociones o de sentimientos que podrían no ser relevantes a efectos legales, pero que a lo mejor sí son importantes a fin de dar una solución al conflicto. Además, resultan de ayuda para proporcionar a la víctima una sensación de control sobre su propio daño, facilitando la reparación y ofreciéndole un lugar preferente, especial e individualizado.

La justicia restaurativa constituye un cambio de paradigma, supone, por un lado, la aceptación en el sistema penal de la función restaurativa o reparadora y, por otra parte, la aceptación de que, además del proceso, pueden incorporarse al sistema nuevos mecanismos de gestión y/o solución de conflictos que vengan a complementar la tutela procesal.

No obstante, pese a las ventajas señaladas, existen una serie de aspectos controvertidos en torno a la aplicación de estos procedimientos de justicia restaurativa en los supuestos de violencia de género. Y, asimismo, resulta cuestionada la utilidad de los ODR para este tipo de asuntos; es decir, si los ODR se pueden presentar como una posible vía para introducir los procedimientos de justicia restaurativa en esta materia de violencia de género. Pues bien, a lo largo de las páginas que siguen, una vez

11. *Vid*. LOORENTE SÁNCHEZ– ARJONA, M., *Justicia con perspectiva de género: El nuevo paradigma en la lucha contra la violencia de género*, Aranzadi, Cizur Menor (Navarra), 2021; SUBIJANA ZUNZUNEGUI, I.J. y PORRES GARCÍA, I. "La viabilidad de la justicia terapéutica, restaurativa y procedimental en nuestro ordenamiento jurídico", *Cuadernos Penales José María Lidón*, 9, Deusto Digital, Bilbao 2013 (http://www.deusto-publicaciones.es/deusto/pdfs/lidon/lidon09.pdf, última consulta: 13/09/2022); TAMARIT SUMAYA, J., "La justicia restaurativa: concepto, principios, investigación y marco teórico", en TAMARIT SUMAYA, J. (coord..), *La justicia restaurativa: desarrollo y aplicación práctica*, Compares, Granada, 2012; WALGRAVE, L.: "La justice restauratrice et les victimes", *Le Journal International de Victimologie* 1(4), 2002; ZEHR, H., *El pequeño libro de la Justicia Restaurativa*, Good Books, Intercourse, USA, 2010.

analizada la justicia restaurativa en los supuestos de violencia de género y su marco normativo, se profundizará en la utilidad de los ODR en este tipo de supuestos, como una forma de ampliar las opciones de reparación a las víctimas de violencia de género.

II. MARCO NORMATIVO

Si analizamos el marco normativo en materia de justicia restaurativa en supuestos de violencia de género, podemos destacar que todo el movimiento analizado en el apartado anterior ha ido obteniendo cierto reflejo legal a nivel internacional, europeo y con más retraso en nuestra legislación española.

1. REGULACIÓN EUROPEA EN MATERIA DE JUSTICIA RESTAURATIVA

Desde diferentes estancias se han ido elaborando numerosas propuestas y recomendaciones que han ido introduciendo la aplicación de programas de justicia restaurativa en materia penal y más en concreto, en materia de violencia de género.

En el ámbito de las Naciones Unidas, debe reseñarse la Resolución 1999/26, de 28 de julio, del Consejo Económico y Social de las Naciones Unidas, sobre elaboración y aplicación de medidas de mediación y justicia restitutiva en materia de justicia penal; la Resolución 2000/14, de 27 de julio, del Consejo Económico y Social, sobre principios básicos para la aplicación de programas de justicia restaurativa en materia penal; el Informe del Secretario General del Consejo Económico y Social de las Naciones Unidas de 7 de enero de 2002, sobre reforma del sistema de justicia penal: logro de eficacia y equidad: justicia restaurativa y la Resolución 2002/12, de 24 de julio, del Consejo Económico y Social de las Naciones Unidas, sobre principios básicos para la aplicación de programas de justicia restaurativa en materia penal.

Si tomamos como referencia el Consejo de Europa, cabe referirse a la Recomendación núm. R (85) 11, de 28 de junio de 1985, del Comité de Ministros del Consejo de Europa a los Estados miembros, relativa a la posición de la víctima en el marco del proceso penal y el derecho penal; la Recomendación núm. R (87) 21, de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa a los Estados miembros, sobre la asistencia a las víctimas y la prevención de la victimización; la Recomendación núm. R (99) 19, de 15 de septiembre de 1999, del Comité de Ministros

del Consejo de Europa a los Estados miembros, relativa a la mediación en materia penal y la última Recomendación CM/Rec (2018) 8 del Comité de Ministros a los Estados miembros relativa a la Justicia Restaurativa en materia penal, que viene a sustituir a la del mismo Consejo de Europa de 1999[12].

Por su parte, en el ámbito de la UE, debe destacarse la Decisión Marco 2001/220/JAI del Consejo, de 15 de marzo de 2001, relativa al estatuto de la víctima en el proceso penal[13], y la Directiva 2012/29/UE del Parlamento Europeo y del Consejo por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, y que sustituye a la Decisión Marco 2001/220/JAI[14].

La Decisión Marco 2001/220/JAI establece en su art. 10.1 que los Estados miembros deben promover la mediación en las causas penales para las infracciones que sean adecuadas a este tipo de medida. De esta manera, la mediación penal, debidamente incorporada al proceso penal, atiende prioritariamente a la protección de la víctima y al restablecimiento de la paz social mediante el diálogo comunitario y el encuentro personal entre los directamente enfrentados[15].

Ahora bien, debe señalarse que la Directiva 2012/29/UE continúa con la estrategia global de protección a las víctimas, pero entre sus objetivos no se sitúa específicamente el impulso de la mediación penal. Tal y como viene recogido en su art. 12.2 "Los Estados miembros facilitarán la derivación de casos, si procede, a los servicios de justicia reparadora, incluso mediante el establecimiento de procedimientos u orientaciones sobre las condiciones de tal derivación"[16]; es decir, su finalidad es garantizar que las víctimas reciban la información, el apoyo y la protección adecuada y

12. TAMARIT SUMALLA, J. M., "La justicia restaurativa en España ¿Qué impacto puede tener la Recomendación? *Revista de Victimología*, (8), 2018, pp. 181-184.
13. DOCE L 82 de 22 de marzo de 2001.
14. DOUE L 315 de 14 de noviembre de 2012. Sobre esta Directiva, *vid.* DE HOYOS SANCHO, M., "Reflexiones sobre la Directiva 2012/29/UE, por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, y su transposición al ordenamiento español", *Revista General de Derecho Procesal*, núm. 34, septiembre, 2014.
15. Esta Decisión Marco 2001/220/JAI configuraba la mediación como un mecanismo de ayuda a las víctimas. En su considerando (7) se afirmaba que "Las medidas de ayuda a las víctimas de delitos, y en particular las disposiciones en materia de indemnización y de mediación, no afectan a las soluciones que son propias del proceso civil".
16. Art.12 Directiva 2012/29/UE, bajo la rúbrica "Derecho a garantías en el contexto de los servicios de justicia reparadora", recoge en su apartado 1: "Los Estados miembros adoptarán medidas para proteger a la víctima contra la victimización secundaria o reiterada, la intimidación o las represalias, medidas que se aplicarán cuando se faciliten servicios de justicia reparadora".

que puedan participar en procesos penales, estableciendo para ello un conjunto de derechos, entre los que se cuenta el acceso a los sistemas de justicia reparadora bajo ciertas condiciones.

La citada Directiva viene a imponer a los Estados miembros, el impulso de la derivación de casos, si procede, a los servicios de justicia reparadora, entre los que se encuentra la mediación penal, junto con la conciliación, las conferencias de grupo familiar y los círculos de sentencia. Por tanto, la Directiva no impone directamente la obligación de los Estados miembros de integrar la mediación penal pero sí quedan obligados a satisfacer ese derecho de las víctimas a tener acceso a sistemas de justicia restaurativa.

En lo referente a los delitos de violencia de género, las pautas de las Naciones Unidas y del Consejo de Europa no son coincidentes. Podría decirse que los documentos de las Naciones Unidas además de contemplar la mediación con ciertas reservas abogan por una respuesta en base a la justicia retributiva, subrayando la necesidad de tomar medidas de corte punitivo. En este sentido, no aluden a procedimientos de justicia restaurativa e incluso el *Manual de legislación sobre violencia contra la mujer* de 2010 acaba recomendando la prohibición de la mediación[17].

Por su parte, en el marco del Consejo de Europa, no se contempla esta tendencia de prohibición de la mediación en los delitos de violencia de género; así, la Recomendación del Comité de Ministros del Consejo de Europa, Protección de las mujeres contra la violencia Rec (2002) 5, propone una serie de medidas tanto de orden penal como procesal penal, pero no recoge ninguna referencia en relación con la mediación o con otros procedimientos de justicia restaurativa. Y es el Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica de 11 de mayo de 2011 el que deja abierta la posibilidad de los procedimientos de justicia restaurativa incluida la mediación salvo que sea obligatoria; así, en su art. 48.1 recoge "los modos alternativos obligatorios de resolución de conflictos, incluidas la mediación y la conciliación, en lo que respecta a todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio".

Por tanto, a nivel europeo, no se prohíbe el empleo de mecanismos de justicia restaurativa en supuestos de violencia de género, además la Directiva 2012/29/UE no se refiere a los supuestos de mediación en casos de violencia de género ni doméstica, únicamente obliga a los Estados miembros a tomar medidas que aseguren que las víctimas que elijan participar en procedimientos de justicia restaurativa tengan acceso a servicios que la

17. *Vid*. https://www.mapa.gob.es/es/ministerio/planes-estrategias/igualdad-de-oportunidades/onumanuallegislation_tcm30-428123.pdf (última consulta: 22/09/2022).

provean seguros y competentes; asimismo, como refiere el Convenio de Estambul de 2011, la intervención de las partes en estas formas de resolución de conflictos debe ser siempre voluntaria.

En este sentido, ante la ausencia de una prohibición en la normativa europea, diversos Estados han ido incorporando procedimientos de justicia restaurativa, incluida la mediación, en supuestos de violencia de género[18].

2. REGULACIÓN NACIONAL EN MATERIA DE JUSTICIA RESTAURATIVA: PROHIBICIÓN DEL PROCEDIMIENTO DE MEDIACIÓN EN VIOLENCIA DE GÉNERO

En el ámbito del ordenamiento jurídico español, debe reseñarse que la regulación legal de la mediación penal se puso de manifiesto únicamente en la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de menores y el Real Decreto 1774/2004, de 30 de julio, por el que se aprueba su Reglamento de desarrollo; en el cual se regula y se contempla la mediación con una finalidad educativa y resocializadora.

En lo referente al ámbito de la justicia penal de adultos, en la última reforma del Código Penal operada con la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código penal se introduce, por primera vez previsiones relativas a la mediación, aunque de una forma limitada. Así, entre otras modificaciones, en su Disposición Final 2.ª, apartado 10, introduce el principio de oportunidad reglada, modificando algunos aspectos de la LECrim; igualmente, atribuye efectos a la reparación sobre la suspensión de la pena; así, el juez podrá acordar la suspensión de la pena bajo ciertas condiciones, valorando las circunstancias del caso, y en particular, el esfuerzo del penado en reparar el daño (art. 80.2 CP); el art. 84 CP regula que el juez o tribunal también podrá condicionar la suspensión de la ejecución de la pena al cumplimiento de alguna o algunas de las siguientes prestaciones o medidas entre las que se encuentra el cumplimiento del acuerdo alcanzado por las partes en virtud de mediación y, entre otros aspectos, recoge respecto a la concesión de los beneficios de la libertad condicional, entre otros requisitos, la participación efectiva y favorable en programas de reparación a las víctimas (art. 90 CP).

18. *Vid*. VICENTE CASILLAS, C., "La mediación en España. Algunos ejemplos europeos. Mediación y violencia contra la mujer. Una propuesta de regulación", *Cuadernos Penales José María Lidón*, 9, Deusto Digital, Bilbao 2013, pp. 205-235, (http://www.deusto-publicaciones.es/deusto/pdfs/lidon/lidon09.pdf, última consulta: 07/05/2021) que realiza un análisis de la mediación desarrollada en Austria y en Finlandia.

Asimismo, debe destacarse la Ley 4/2015, de 27 de abril, del Estatuto de la víctima (en adelante, EV) que como contiene en su Preámbulo, "con este Estatuto, España aglutinará en un solo texto legislativo el catálogo de derechos de la víctima, de un lado transponiendo las Directivas de la Unión Europea en la materia y, de otro, recogiendo la particular demanda de la sociedad española". Con este estatuto de la víctima, se garantiza el acceso de las víctimas a servicios de justicia restaurativa (art.15) y, por tanto, se abre la posibilidad de incorporar otras prácticas diferentes a la mediación penal en nuestro sistema legal. Sin embargo, debe reseñarse que dicho precepto, junto el art. 37 RD 1109/2015, de 11 de diciembre, por el que se desarrolla la Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito, y se regulan las Oficinas de Asistencia a las Víctimas del Delito, tan solo indican los requisitos que tienen que cumplirse para la derivación a mediación y nada señalan sobre los diversos procedimientos de justicia restaurativa diferentes a la mediación a los que se podrían acudir.

En lo que respecta a los delitos de violencia de género debe reseñarse que el art 44 LO 1/2004 adiciona el art. 87 ter.5 a la LOPJ, en el cual establece la prohibición de la mediación. Dicha prohibición supuso la paralización de los procedimientos de mediación en violencia de género que se estaban llevando a cabo en nuestro país, manteniéndose la misma tanto en el Estatuto de la Víctima del Delito de 2015 como en el Pacto de Estado contra la Violencia de Género de 2017[19]; en este sentido, es clara la voluntad de nuestro legislador de evitar la posible aplicación de la mediación a estos supuestos.

Ahora bien, si tomamos como punto de partida el tratamiento restaurativo hacia las víctimas tal como recoge la Directiva 2012/29/UE y el EV, las víctimas de cualquier delito tienen derecho a servicios de justicia restaurativa o reparadora. Además, cumple mencionar que el Anteproyecto de la Ley de Enjuiciamiento Criminal de 2011 que inserta por primera vez en España ese intento de regulación de la mediación penal, el Borrador de Código Procesal Penal de 2013 que introduce el concepto de justicia restaurativa en su Exposición de motivos –si bien regulando en su articulado únicamente la mediación penal– y el Anteproyecto de la Ley de Enjuiciamiento Criminal aprobado el 24 de noviembre de 2020 que viene a regular la garantía de acceso a las víctimas a los procedimientos de justicia restaurativa en su conjunto; mantienen esa prohibición de la mediación en los supuestos de violencia de género si bien regulan otros procedimientos de justicia restaurativa aplicables a estos casos.

19. *Vid*. GUARDIOLA LAGO, M. J., "La víctima de violencia de género en el sistema de justicia y la prohibición de la mediación penal" …, *op. cit.*; en donde se analizan las experiencias desarrolladas en nuestro país.

En definitiva, este análisis nos lleva a la conclusión de que la justicia restaurativa en violencia de género cuenta con una normativa y respaldo por parte de las instancias europeas, siendo necesario que los distintos Estados miembros tomen conciencia de la necesidad de una regulación específica de esta materia. En España, la ausencia de una regulación de los procedimientos de justicia restaurativa en los supuestos de violencia de género está privando tanto a las víctimas como a los infractores de las ventajas que ofrece la justicia restaurativa en numerosos supuestos; además, nuestro país viene a situarse en una posición un tanto singular en relación con las diferentes regulaciones de países de nuestro entorno que han ido incorporando los diferentes procedimientos de justicia restaurativa en este tipo de supuestos[20].

III. VIOLENCIA DE GÉNERO, JUSTICIA RESTAURATIVA Y MEDIACIÓN

En los apartados precedentes se han abordado los aspectos más relevantes en relación con la justicia restaurativa, habiéndose destacado los efectos positivos de la incorporación del procedimiento de justicia restaurativa al proceso; es así que el proceso judicial indudablemente podría ser mejorado o complementado con la adopción de otros métodos de gestión y/o solución de conflictos que intenten paliar en cierta medida las deficiencias en torno a la víctima señaladas. La justicia restaurativa tendría que estar integrada como un procedimiento complementario que mejorase el sistema penal y, por tanto, le aportase calidad, eficiencia y efectividad.

Ahora bien, como se ha señalado, en España no ha sido hasta la aprobación del EV, mediante el que se traspone la Directiva 2012/29/UE, cuando ha comenzado a legislarse en materia de mediación en el ámbito de la justicia penal de adultos. Antes de ese momento, el Anteproyecto de LECrim de 2011 insertó por primera vez ese intento de regulación de la mediación con la introducción en el apartado XXVI de su Exposición de motivos del principio de oportunidad y la mediación penal; así en el Capítulo III se regulaban los principios, procedimiento y consecuencias de la mediación penal. Posteriormente, con el Borrador

20. *Vid*. DROST, L.; HALLER, B.; HOFINGER, V.; VAN DER KOOIJ, T.; LÜNNEMANN, K.; WOLTHUIS, A.; "Restorative Justice in Cases of Domestic Violence. Best practice examples between increasing mutual understanding and awareness of specific protection needs. (JUST/2013/JPEN/AG/4587) WS1. Comparative Report", 2015 (https://www.verwey-jonker.nl/publicaties/2015/restorative-justice-in-cases-ofdomestic-violence, última consulta: 12/09/2022).

de Anteproyecto de Código Procesal Penal de 2013 se insertó el concepto de justicia restaurativa en su Exposición de Motivos, y su puesta en escena a través de la mediación en su Título VI sin hacer referencia a ningún otro procedimiento de justicia restaurativa; es así que la propia Exposición de Motivos configura la mediación penal como instrumento para alcanzar ciertos fines, dando prioridad a los intereses de la víctima. Su fundamento es la gestión del conflicto y la reparación del daño con la intervención de un tercero independiente con los conocimientos adecuados[21].

Teniendo en cuenta que ninguno de los citados textos se ha llegado a aprobar y que la todavía vigente LECrim ni siquiera incluye referencia alguna a términos como justicia restaurativa o mediación; debe reseñarse –por el avance que supone en la materia– el Anteproyecto de LECrim de 2020 que opta por introducir mecanismos alternativos, siguiendo la opción político-legislativa de los anteriores textos legales. El Anteproyecto de 2020 reproduce en esencia los contenidos del Anteproyecto de 2011 si bien, adecuándolo a la Directiva 2012/29/UE por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos. En este sentido, el Anteproyecto de 2020 viene a regular la garantía de acceso a las víctimas a los procedimientos de justicia restaurativa entre los que se encuentra la mediación penal junto con otros procedimientos; a saber, la conciliación, las conferencias de grupo familiar y los círculos de sentencia. Por tanto, no se contempla únicamente la mediación penal como se había optado tanto en el Anteproyecto de 2011 como en el Borrador de Código Procesal Penal de 2013, los cuales seguían las directrices de la Decisión Marco 2001/220/JAI, que establecía que los Estados miembros debían promover la mediación en las causas penales para las infracciones que sean adecuadas a este tipo de medidas[22].

El Anteproyecto de 2020 concibe la justicia restaurativa como un instrumento al servicio de la decisión expresa del Estado de renunciar a la imposición de la pena cuando esta no es necesaria a los fines públicos de prevención y pueden resultar adecuadamente satisfechos los intereses particulares; concibiéndose, por tanto, como un complemento efectivo del ejercicio de oportunidad (apdo. XXVII).

21. *Vid*. MARTÍN DIZ, F. "Mediación y justicia penal. Crítica ante un futuro contexto legal", en MORENO CATENA, V. (Dir.) *Reflexiones sobre el nuevo proceso penal*, Tirant lo Blanch, Valencia, 2015, pp. 751-772.

22. *Vid*. MOLLAR PIQUER, M. P., "La mediación penal", en GÓMEZ COLOMER, J. L. (Coord.) *El proceso penal en la encrucijada.* Homenaje al Dr. César Crisóstomo Barrientos Pellecer. Castelló de la Plana: Publicaciones de la Universitat Jaume I, 2015, pp. 847-863.

En este sentido, el Anteproyecto dedica algunos preceptos a la justicia restaurativa, regulando sus principios, procedimiento y consecuencias; sin entrar de lleno, en la modalidad, por excelencia, de resolución alternativa, que es la mediación penal. Y ello en consonancia con el Proyecto de Ley de Eficiencia Procesal del Servicio Público de Justicia, aprobado el 12 de abril de 2022, en el que se regula la mediación junto con otros medios adecuados de resolución de conflictos.

Ahora bien, aunque parte de la doctrina ha demandado la regulación de la mediación penal a través de una ley estatal al igual que ha sucedido con la mediación civil y mercantil[23]; estas demandas no resultan incompatibles con lo dispuesto en el Anteproyecto de LECrim de 2020 y que a su vez recogen la obligación del Estado de garantizar el acceso de las víctimas a los servicios de justicia restaurativa, tal y como se desprende tanto de la Directiva 2012/29/UE como del EV. Por tanto, es acertado que la futura regulación incluya la mediación junto con otras prácticas de justicia restaurativa.

No obstante, como se ha señalado, en lo que respecta a los delitos de violencia de género, el Anteproyecto de LECRim de 2020 mantiene la prohibición de la mediación en casos de violencia de género que instituyó la LO 1/2004 y ha mantenido el EV; –prohibición contraria a la opinión cada vez más prevalente en la doctrina española del empleo de procedimientos de justicia restaurativa-incluida la mediación– a este tipo de supuestos[24]. Si bien, este Anteproyecto de 2020, abre la puerta a la aplicación de mecanismos de justicia restaurativa diferentes a la mediación de una forma más concreta y extensa a lo regulado en el EV[25].

En este sentido, el Anteproyecto de LECrim de 2020 contempla la institución de la justicia restaurativa como un complemento efectivo del ejercicio de oportunidad y por tanto, además de regular los principios

23. En este sentido, *vid*. MARTÍN DIZ, F. "Mediación y justicia penal. Crítica ante un futuro contexto legal" …, *op. cit*.

24. En este sentido, numerosos autores se han manifestado a favor de la mediación en supuestos de violencia de género; entre otros, ALONSO SALGADO, C. "Violencia de género, justicia restaurativa y mediación", en GARCÍA GOLDAR, M. (Dir.) y AMMERMAN YEBDRA, J. (Dir.), *Propostas de modernización do dereito,* 2017; GUARDIOLA LAGO, M. J., "La víctima de violencia de género en el sistema de justicia y la prohibición de la mediación penal" …, *op. cit*.; VILLACAMPA ESTIARTE, C., "Justicia restaurativa en supuestos de violencia de género en España: situación actual y propuesta político-criminal" …, *op. cit*.

25. *Vid*. MARTÍN RÍOS, P., "La justicia restaurativa en el Anteproyecto de Lecrim de 2020", en JIMÉNEZ CONDE, F. y FUENTES SORIANO, O. (Dirs.) *Reflexiones en torno al Anteproyecto de Ley de Enjuiciamiento Criminal de 2020*, Tirant Lo Blanch, Valencia, 2022, pp. 1169-1191.

del procedimiento restaurativo en el art. 181; recoge todo lo referente al procedimiento de justicia restaurativa desde el inicio del procedimiento a instancia del Ministerio Fiscal o del órgano judicial, esto es por derivación, o a instancia de las partes (art. 182 y art. 184); fases procesales en la cuales tiene cabida la remisión a un procedimiento de justicia restaurativa y consecuencias del procedimiento restaurativo[26].

En lo que respecta a los delitos de violencia de género, si realiza una precisión en relación con las consecuencias de los procedimientos de justicia restaurativa; así el art. 175.3 recoge que la facultad de archivo por razones de oportunidad "no será de aplicación a los delitos de violencia de género ni a los relacionados con la corrupción". Es así que, los efectos del procedimiento restaurativo en supuestos de violencia de género se traducirían en suspensión del procedimiento por razones de oportunidad conforme se estipula en el art. 176 o se le aplicarán las reglas del procedimiento de conformidad (arts. 164 a 174.).

No obstante, a pesar de lo proyectado, debe reseñarse que en la actualidad tanto la mediación como otros mecanismos de justicia restaurativa se encuentran vedados en nuestro ordenamiento en temas de violencia de género. Cuestión un tanto paradójica, en el sentido de regular una prohibición absoluta, independientemente de los múltiples supuestos de violencia de género a tenor de su gravedad o de las circunstancias concurrentes en cada caso, que sí podrían beneficiarse de los procedimientos de justicia restaurativa. A modo de ejemplo, podría señalarse que las prácticas restaurativas evitarían reincidencias y facilitarían una positividad en las relaciones de las partes en los supuestos de expedientes archivados por los Juzgados de Violencia; además de los beneficios que estas prácticas podrían reportar cuando existen medidas cautelares civiles y/o penales, en el sentido de dar apoyo tanto a la víctima como al ofensor para la gestión de los aspectos relacionados con los hijos.

De esta manera, a pesar de lo delicado del tema, de que claramente no todos los asuntos de violencia de género son susceptibles de cualquiera de las prácticas restaurativas, léase la mediación, los círculos o las conferencias; no se debería cerrar la puerta a todos estos métodos complementarios de justicia restaurativa. Por ello, resulta claramente necesario atender a las circunstancias concretas del caso –a fin de valorar y determinar la oportunidad, conveniencia y viabilidad de la justicia restaurativa en cada uno de los asuntos de violencia de género– a tenor de las ventajas anteriormente señaladas tanto para la víctima, el infractor, como la propia comunidad.

26. *Vid*. FARTO PIAY, T., "El procedimiento de justicia restaurativa en el Anteproyecto de la Ley de Enjuiciamiento Criminal de 2020", *La Ley Penal*, N.º 151, 2021.

IV. LA UTILIDAD DE LOS ODR EN LOS SUPUESTOS DE VIOLENCIA DE GÉNERO

Las principales reticencias sobre la aplicación y utilización de las prácticas restaurativas en los supuestos de violencia de género parten de la simple posibilidad de que víctima e infractor se encuentren en el mismo espacio físico; un cara a cara víctima e infractor podría resultar muy perjudicial para la víctima, en el sentido de que se podría poner en riesgo tanto la salud física como psicológica de la víctima, al encontrarse con su agresor. Además de esa posible desigualdad entre víctima e infractor que podría acabar por revictimizar a la víctima.

Ahora bien, delimitar lo que por igualdad debe entenderse resulta una cuestión un tanto difícil, máximo si se considera la desigualdad de inicio de la que se parte en el ámbito penal tras la comisión del hecho delictivo. Y, por otra parte, debe partirse que en los procedimientos de justicia restaurativa no se hace necesario enfrentar directamente a la víctima y al agresor para que dichos procedimientos se puedan desarrollar y llevar a término; es decir, las sesiones tanto con la víctima como con el infractor se pueden llevar a cabo de forma separada. Además, en la actualidad, contamos con multitud de herramientas que permiten a las personas en conflicto comunicarse directamente sin tener que coincidir de forma necesaria en el mismo espacio físico.

Los llamados ODR (Online Dispute Resolution), acrónimo anglosajón con el que se designan a los medios extrajudiciales de resolución de litigios *online*, vienen a proporcionar mecanismos tanto asincrónicos como sincrónicos. Los sincrónicos nos permiten coincidir en el mismo espacio al mismo tiempo mientras que los asincrónicos, se refieren a la comunicación que no es simultánea entre quién la envía y la recibe, es decir el receptor no está precisamente conectado al mismo tiempo que el emisor. De esta manera, la comunicación puede ser realizada por cualquier medio, como pueden ser los correos electrónicos, messenger, chats, plataformas digitales especializadas, llamadas telefónicas o videoconferencias en las que se pueden llevar a cabo, por ejemplo, los encuentros restaurativos o sesiones de mediación entre víctima e infractor sin la necesidad de que se reúnan en un mismo espacio físico.

Por tanto, los ODR se presentan como una posible vía para introducir los procedimientos de justicia restaurativa en los supuestos de violencia de género, abriendo la posibilidad a realizar los encuentros restaurativos a distancia[27];

27. En este mismo sentido, señala CARRETERO MORALES ("La utilidad de los ODR en los casos de violencia de género", *en Revista Electrónica de Direito Processual,* Río de Janeiro, Ano 11, Volumen 18, n.º 1, 2017, p. 223) "la utilización de medios tecnológicos

evitando, por tanto, la presencia física de las personas involucradas en el desarrollo del propio procedimiento[28].

En los últimos tiempos, la crisis sanitaria provocada por la COVID-19 ha tenido una incidencia significativa tanto en la utilización de las comunicaciones electrónicas como de los procedimientos de justicia restaurativa. Por un lado, debe reseñarse que el desplazamiento de las actuaciones procesales derivado de la suspensión acordada durante el estado de alarma, junto con la presentación de nuevas demandas tras su levantamiento llegó a complicar de forma considerable el panorama y realidad de la Administración de Justicia a la hora de gestionar, de manera eficaz, los conflictos existentes; causándose, por tanto, mayores dilaciones en la tramitación de los procesos judiciales, en una ya de por sí colapsada Administración. Y, por otra parte, los procedimientos de justicia restaurativa se presentaron como uno de los mecanismos más eficientes para resolver multitud de conflictos tanto cuando estaba vigente el estado de alarma como cuando se decretó su levantamiento.

Ahora bien, esta nueva realidad ha tenido una incidencia específica en este tipo de procedimientos, a saber; el tercero neutral se ha tenido que adaptar, así como ha tenido que adecuar las prácticas restaurativas a un nuevo escenario de no presencialidad en las sesiones o de presencialidad limitada en función de las circunstancias sanitarias, cuestiones que han incidido de lleno tanto en la propia capacitación de la persona mediadora o facilitador como en los propios procedimientos de justicia restaurativa.

En este sentido, el escenario derivado de la crisis sanitaria ha tenido una clara repercusión en la forma habitual en la que se venían desarrollando las prácticas restaurativas en nuestro país. Si observamos su práctica y desarrollo antes de la pandemia, puede afirmarse que de forma generalizada tanto las mediaciones como otros procedimientos de justicia restaurativa se desarrollaban íntegramente de forma presencial llevándose a cabo a través de medios electrónicos en situaciones "excepcionales" en las cuales las personas en conflicto, por ejemplo, se encontraban separadas geográficamente. Por lo que puede hablarse de un antes y un después de la pandemia[29].

---

se presenta como una posible vía para introducir elementos de justicia restaurativa en la gestión de los conflictos de violencia de género, toda vez que se evitaría la presencia física de las personas involucradas en el desarrollo del proceso".

28. Como refiere BARONA VILAR ("Psicoanálisis de las ADR. Retos en la sociedad global del siglo XXI", en *LA LEY, Mediación y arbitraje*, n.º 1, Wolters Kluwer, 2020, p. 22) "por un lado, las ODR pueden ser una pieza más del *puzzle* de la Justicia economicista o de la economización de la Justicia; y, por otro lado, las ODR más bien parecen responder a las expectativas de la Economía global que a la consideración de mejor vía de acceso de los ciudadanos a la Justicia, más accesible, rápida y sencilla".

29. Como refiere GONZALO QUIROGA ("COVID-19, innovación y tecnología en la E-Justicia alternativa: ¿Algo hemos aprendido?, en FARIÑA RIVERA, F., WILHELM

1. JUSTICIA RESTAURATIVA Y ODR

Los ODR, en principio, fueron concebidos para ser utilizados en procedimientos de carácter civil o mercantil, y, de hecho, en este campo es dónde se han ido desarrollando a lo largo de los últimos tiempos. En este sentido, la Directiva 2008/52/CE del Parlamento Europeo y del Consejo, de 21 de mayo de 2008, sobre ciertos aspectos de la mediación en asuntos civiles y mercantiles, en su considerando 9.º, estableció que "la presente Directiva no debe impedir en modo alguno la utilización de las nuevas tecnologías de comunicaciones en los procedimientos de mediación", cuestión que aparece recogida en el art. 24 de la Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles y de igual modo, se establece en el art. 7 del Proyecto de Ley de medidas de eficiencia procesal al servicio público de Justicia, aprobado el pasado 22 de abril de 2022 que concreta las actuaciones desarrolladas por medios telemáticos y así recoge de forma expresa que "Las partes podrán acordar que todas o alguna de las actuaciones de negociación en el marco de un medio adecuado de solución de controversias, se lleven a cabo por medios telemáticos, por videoconferencia u otro medio análogo de transmisión de la voz o la imagen, siempre que quede garantizada la identidad de los intervinientes y el respeto a las normas previstas en este título y, en su caso, a la normativa de desarrollo específicamente contemplada para la mediación". Por tanto, sirva de ejemplo en este ámbito, la Plataforma Europea de resolución extrajudicial de litigios en línea en materia de consumo[30] o la Plataforma de tramitación electrónica de resolución extrajudicial de conflictos derivados de accidentes de tráfico en relación a las reclamaciones de daños personales a las aseguradoras[31].

Por otra parte, si tomamos como referencia la normativa analizada en los apartados precedentes en relación con la justicia restaurativa, se puede observar, que ni en la Recomendación 2018 (8) sobre justicia restaurativa del Consejo de Europa, ni en la Directiva 2012/29/UE sobre derechos de las víctimas y tampoco a nivel nacional, en el EV de 2015 y en el Real Decreto 1109/2015 por el que se desarrolla el EV y se regulan las Oficinas de Asistencia a las Víctimas del Delito se contempla y desarrolla la

---

WAINSZTEIN, J. y MUNNÉ, M. (Coords.) *Reflexiones mediadoras en la post pandemia*, CUEMYC, Pontevedra, 2022, p. 200) "Existe un antes y un después de la gestión de los conflictos a través de la justicia alternativa, la innovación y los medios telemáticos y electrónicos aplicados a la misma a través de los ODRS, en general y la telemediación o mediación online, tras y durante la pandemia COVID-19".

30. *Vid*. https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=ES (última consulta: 21/09/2022).

31. *Vid*. https://sdplex-abogados.tirea.es/ (última consulta: 21/09/2022).

posibilidad de realizar los procedimientos de justicia restaurativa a distancia, valiéndose de la utilización de medios informáticos o tecnológicos. Materia que tampoco se ha regulado en las Resoluciones del Gobierno de España y de las Comunidades Autónomas sobre la prestación de servicios durante la crisis de la COVID-19 ni en el Anteproyecto de la Lecrim de 2020[32].

Ahora bien, a pesar de los cambios que las nuevas tecnologías han ido incorporando en la actividad general de los operadores jurídicos, resulta sorprendente esta falta de regulación en este ámbito, más cuando en muchas de las prácticas a nivel procesal penal se contempla la posibilidad del uso de las tecnologías de la comunicación[33]. A modo de ejemplo, debe reseñarse lo contenido en el art. 25.2 letras a) y b) EV que hacen referencia al uso de medidas que eviten el contacto visual entre la víctima y el supuesto autor de los hechos, para lo cual podrá hacerse uso de las tecnologías de la comunicación o la utilización de tecnologías de la comunicación adecuadas para garantizar que la víctima pueda ser oída sin estar presenta en la sala de vistas.

Por todo ello, debe entenderse que las características y ventajas de la utilización de los ODR en las disputas de carácter civil o mercantil pueden ser también perfectamente aplicadas en el ámbito penal y dentro de éste, por qué no, en los asuntos de violencia de género[34].

En este sentido, mencionar las distintas experiencias que se han llevado a cabo desde distintas organizaciones en plena crisis de la COVID-19 que han venido a promover y utilizar los ODR en los procedimientos restaurativos. A modo de ejemplo, en Cataluña se llegaron a realizar círculos digitales de diálogo con personal sanitario y con familiares de las personas fallecidas por la enfermedad; el servicio público de mediación penal del Gobierno de Navarra apostó por un sistema de justicia restaurativa digital o en Estados Unidos, personas del Centro Nacional de Resolución de Conflictos, facilitaron círculos comunitarios virtuales para reunir a personas diversas en situaciones conflictivas para facilitar la comunicación y la empatía[35].

32. *Vid*. VARONA MARTÍNEZ, G., "Justicia restaurativa digital, conectividad y resonancia en tiempos del COVID-19", *Revista de victimología*, n.º 10, 2020, pp. 9-42.
33. *Vid*. PEREIRA PUIGVERT, S. y PESQUEIRA ZAMORA, M.ª J., *Investigación y proceso penal en el Siglo XXI nuevas tecnologías y protección de datos*, Aranzadi, Cizur Menor (Navarra), 2021.
34. CARRETERO MORALES, E., "La utilidad de los ODR en los casos de violencia de género" …, *op. cit*., p. 224.
35. *Vid*. VARONA MARTÍNEZ, G., "Justicia restaurativa digital, conectividad y resonancia en tiempos del COVID-19" …, op. cit.

2. LOS ODR EN LOS SUPUESTOS DE VIOLENCIA DE GÉNERO

Al igual que la justicia restaurativa no es útil para todo tipo de asuntos, la utilización de los ODR en los casos de violencia de género no sirve para todo tipo de supuestos, por lo tanto, se hace necesario velar por que la aplicación de los mismos sea conveniente y adecuada a cada asunto.

Como se ha señalado con anterioridad, los ODR se presentan como una posible vía para introducir los procedimientos de justicia restaurativa en este tipo de supuestos, al abrir la posibilidad a realizar los encuentros restaurativos a distancia. Si bien, la utilización de los ODR implica una serie de cambios y variaciones respecto de las prácticas restaurativas convencionales. Es decir, la utilización de los recursos tecnológicos implica una adaptación del propio procedimiento restaurativo como del tercero neutral y de las demás personas intervinientes en el mismo. Una demostración más de lo referido por MARTIN DIZ al señalar que los medios extrajudiciales de resolución de litigios son más universales y flexibles que el proceso judicial y, por tanto, se mueven en parámetros menos marcados y aportan mayor flexibilidad en su utilización y resultados[36].

Ahora bien, llegados a este punto, debe diferenciarse la mediación indirecta, desarrollada desde hace tiempo, de la mediación *online*, entendida como un subelemento diferenciado de los ODR[37]. La mediación indirecta se produce cuando la misma se articula mediante un tercero transmisor de la información entre víctima e infractor, para evitar el encuentro directo entre ambos; modelo adecuado e indicado para aquellos casos en que se quiere evitar el contacto directo, como pueden ser los supuestos de violencia de género. Mientras que la mediación electrónica es definida por CONFORTI como "un proceso que se realiza total o parcialmente por medios electrónicos, de forma más o menos simplificada, con la intervención de un tercero que ayuda a las partes para que intenten alcanzar por sí mismas un acuerdo, en el que siempre se ha de garantizar la identidad de los intervinientes y el respeto a los principios de la mediación previstos en la Ley"[38].

De esta manera, con la utilización de los ODR se pretende dar un paso más en las prácticas restaurativas. Es decir, aunque tanto la mediación indirecta como los ODR evitan el contacto directo entre víctima e infractor; con

36. MARTÍN DIZ, F., "Justicia digital post-covid19: el desafío de las soluciones extrajudiciales electrónicas de litigios y la inteligencia artificial", *Revista de Estudios Jurídicos y Criminológicos*, n.º 2, Universidad de Cádiz, 2020, pp. 41-74.
37. *Vid*. CONFORTI, O. D., *Pequeño Manual de Mediación Electrónica*. Acuerdo Justo, Alicante, 2013.
38. CONFORTI, O. D., *Pequeño Manual de Mediación Electrónica …, op. cit*., pp. 22-24 y 62-63.

la utilización de los ODR se abre la puerta –atendiendo las circunstancias del caso concreto– a la posibilidad de realizar un encuentro virtual, llegado el momento. Asimismo, permite la realización de grabaciones en las que tanto la víctima como el infractor puedan expresar sus sentimientos, necesidades y así asegurar el intercambio y reciprocidad entre las partes[39].

Por tanto, para un buen funcionamiento de los ODR, se hace necesaria una mayor accesibilidad y adaptabilidad a las necesidades de los casos de violencia de género. Como se ha apuntado, el tercero neutral debe adecuar su intervención a esa evitación del contacto físico no deseado entre la víctima y el infractor; por ello, tanto las partes como la persona facilitadora han de contar con el acceso a los recursos electrónicos, además de no tener problemas o dificultades con el uso de estos. Asimismo, no sólo se ha de contar con la tecnología adecuada, sino que los medios electrónicos utilizados tienen que ser seguros, garantistas y confidenciales[40].

Por otra parte, debe reseñarse la dificultad añadida que conlleva el uso de los ODR en este tipo de supuestos para el tercero neutral; es así que, se hace necesario que el neutral, cuente con competencias y habilidades para saber manejar las emociones y la comunicación tanto verbal como no verbal –en ese entorno digital– para que el propio procedimiento no devenga en impersonal. De ahí la conveniencia de utilizar de forma complementaria los medios electrónicos o fomentar la presencialidad aunque sea *online*[41]; es decir, la anteriormente denominada comunicación síncrona. Cuestión que deviene más necesaria en aquellos supuestos en los cuales entre el tercero neutral y los participantes no exista esa confianza inicial tan importante en las primeras reuniones o bien que se presenten una serie de dificultades a la hora de valorar las necesidades de las partes. En este sentido, podría optarse por un modelo híbrido –en aquellos supuestos en los que fuere posible– realizando las primeras entrevistas con cada una de las partes de manera presencial.

39. Apunta VARONA MARTÍNEZ ("Justicia restaurativa digital, conectividad y resonancia en tiempos del COVID-19" …, *op. cit.*, p. 29.) "algunas personas facilitadoras no tienen tan claro que pueda salvarse la ausencia de encuentro físico, si bien se puede matizar esta postura si pensamos en el uso de la imagen en videollamadas de justicia restaurativa y no tanto en mediaciones indirectas donde sólo se utilice la voz que, en cualquier caso, tiene también sus ventajas".

40. Lo que claramente requiere de una inversión en programas que garanticen la confidencialidad de todo tipo de procedimientos. Deberíamos contar con profesionales especializados y plataformas ODR certificadas.

41. En este sentido, FREITAS y PALERMO ("Restorative justice and technology", en NOVAIS, P. y CARNERO, D. (Eds.) *Interdisciplinary perspectives on contemporary conflicto resolution,* Hershey, PA: IGI Global, 2016) se refieren al trasvase de una dimensión física a otra digital de forma completa o complementaria.

Igualmente, teniendo en cuenta las características de este tipo de conflictos, el tercero neutral tiene que ser un especialista en violencia de género a fin de saber manejar y detectar cualquier situación de desequilibrio entre las partes; además de haber complementado su formación con el fin de manejar este tipo de procedimientos de justicia restaurativa de forma virtual.

En lo referente al propio procedimiento restaurativo, debe señalarse que el tercero neutral tendrá que ir adaptando tanto las fases como las técnicas, herramientas y estrategias a las peculiaridades y particularidades de la comunicación virtual. En lo referente a los tipos de comunicación anteriormente señalados, tanto la síncrona como la asíncrona tienen sus ventajas e inconvenientes, por lo que habrá de valorarse una u otra en función de las partes intervinientes, las circunstancias del caso, así como la evolución y/o fase del procedimiento restaurativo. Ahora bien, teniendo en cuenta las características y particularidades de los asuntos de violencia de género, como señala CARRETERO MORALES podría parecer más conveniente que la comunicación sea asincrónica, "ya que va a permitir a las partes mayor tiempo de reflexión a la hora de elaborar sus mensajes y respuestas, y además al tercero neutral también le va facilitar guiar adecuadamente el proceso, ya que va poder filtrar la información y utilizar las técnicas y reformulaciones oportunas en orden a que los mensajes lleguen de forma indicada a los respectivos receptores"[42].

Si bien, para aquellos supuestos en los cuales el tercero neutral valore de forma positiva un encuentro restaurativo y las víctimas se encuentren preparadas y necesiten expresar sus necesidades, deseos y emociones verbalmente a su agresor, la utilidad de los ODR resulta indudable y nos acerca a encuentros restaurativos *online* muy similares a los que se pueden llegar a desarrollar de forma presencial.

Por otra parte, en relación a la posibilidad de realización de otras prácticas restaurativas, como pueden ser los círculos o conferencias restaurativas, debe reseñarse que la utilización de los recursos tecnológicos puede conllevar cierta dificultad a la hora de mantener los aspectos ceremoniales; a saber, la disposición de las sillas o la utilización de un objeto para el turno de palabra. Si bien, existen experiencias positivas en su modalidad a distancia que han ido incorporando otro tipo de rituales y, por tanto, si se ha ido demostrando su efectividad[43].

42. CARRETERO MORALES, E., "La utilidad de los ODR en los casos de violencia de género" …, *op. cit*., p. 225.
43. PRANIS, K., "Online Support Circles in Response to Social Distancing", 2020 (https://comingtothetable.org/wp-content/uploads/2020/05/Circles-Social-Distancing-3-31-20.pdf, última consulta: 22/09/2022).

3. ODR E INTELIGENCIA ARTIFICIAL

Una vez analizado el alcance de la utilización de los ODR en la justicia restaurativa y más en concreto en los supuestos de violencia de género, se hace preciso adentrarnos en la utilización de la inteligencia artificial para la resolución de este tipo de conflictos.

Como es sabido, el uso de sistemas de inteligencia artificial en la Administración de Justicia no es algo novedoso. De esta manera, puede reseñarse que, de un tiempo a esta parte, la evolución tecnológica nos ha llevado a la aplicación de inteligencia artificial en el derecho, lo cual se conoce como *Artificial Legal Intelligence.* La inteligencia artificial en el ámbito jurídico implica un elemento tecnológico capaz de brindar apoyo para asesorar legalmente, asistir en la toma de decisiones e incluso, asumir la responsabilidad de la decisión de un litigio en ámbitos procesales y extrajurisdiccionales[44].

En estos términos, se plantea la posibilidad de dar cabida dentro de la inteligencia artificial a los ODR. En el sentido de que podría hablarse de una primera aplicación asistencial de la inteligencia artificial de carácter estratégico, para evaluar y ponderar el ODR más idóneo para la gestión y/o resolución del conflicto. Pudiendo ser también aplicable para seleccionar y designar el tercero neutral en función de su formación, experiencia y capacitación.

Por otra parte, podría reseñarse la aplicación de la inteligencia artificial a las ODR con funciones asistenciales a lo largo del procedimiento restaurativo. A este respecto, el sistema podría contribuir de forma activa –realizando funciones de negociación asistida– en el proceso de creatividad, en el entendido coadyuvar a las partes a determinar aspectos similares y diferentes a fin de alcanzar un resultado distinto de lo anteriormente barajado[45].

Y, por último, mencionar las posibles capacidades decisorias, al vincular ODR e inteligencia artificial. Esto es, la resolución de controversias a través de plataformas predictivas donde no interviene el factor humano. Ahora bien, debe señalarse que el uso de la inteligencia artificial con los recursos tecnológicos disponibles en la actualidad no hace especialmente posible; a modo de ejemplo, la generación de confianza y empatía entre las partes, la detección de emociones, la legitimación de los participantes, así como la construcción de un vínculo a través del diálogo. Aún menos

44. MARTÍN DIZ, F., "Justicia digital post-covid19: el desafío de las soluciones extrajudiciales electrónicas de litigios y la inteligencia artificial", …, *op. cit*., p. 63.

45. ORDELIN FONT, J. L., "El uso de la inteligencia artificial en la mediación: ¿quimera o realidad?", *Revista IUS, Derecho e Inteligencia Artificial,* vol.15, n.º 48, 2021, pp. 357-382, p. 372.

viable resultaría, cuando analizamos los supuestos de violencia de género, en los cuales el factor humano es tan importante, al precisar las víctimas de un espacio de seguridad, tranquilidad y confianza donde poder expresar sus sentimientos o emociones. Por tanto, podría afirmarse que se estarían desvirtuado las prácticas restaurativas, tanto sus principios como sus principales beneficios, al no intervenir el factor humano en este tipo de plataformas. Aspectos todos ellos, que con la simple utilización de los ODR en estos procedimientos restaurativos no se pierde, al estar presente todavía el híbrido entre la parte humana[46].

V. CONCLUSIONES

La justicia restaurativa dispone un auténtico cambio en nuestro modelo actual y, por tanto, contribuye a paliar la actual relación entre la víctima y el Estado. Es así que, con la introducción en el sistema de justicia penal de la justicia restaurativa a través de los diferentes métodos restaurativos se persigue dar apoyo a las víctimas, convirtiéndola en protagonista y, asimismo, potenciar la responsabilización del infractor, recuperando la vocación de reinserción del sistema penal. En definitiva, se humaniza el derecho penal, reformulando el modelo de justicia.

Ahora bien, aun entendiendo que la justicia restaurativa y la libertad de forma que la rige hacen difícil describir y estipular su regulación, habría sido oportuno que en la norma proyectada –Anteproyecto de LECrim de 2020– se hubiese recogido qué se entiende por justicia restaurativa –integrando todas las prácticas o mecanismos de justicia restaurativa– y en relación con el proceso penal, se hubiese regulado de forma más exhaustiva el procedimiento de justicia restaurativa y su vinculación con éste.

Además, habría sido oportuno, dada las particularidades de los supuestos de violencia de género, haber recogido todas las especificidades y cautelas que se entiende deben tomarse en esta materia para neutralizar el riesgo de que se produzcan procedimientos de justicia restaurativa inapropiados, que generen revictimización, un acuerdo desfavorable o ambas cosas[47]. En este sentido, habría sido conveniente prever su

46. Como refiere BARONA VILAR ("Psicoanálisis de las ADR. Retos en la sociedad global del siglo XXI"…, *op. cit.*, p. 17) "La evolución continúa. Estamos ya asistiendo al uso instrumental de los algoritmos y la inteligencia artificial, como "Justicia-máquina perfecta", o *machine learning* en el mismo ejercicio de la función decisoria, ora en sede judicial, ora en sede arbitral o incluso como máquina inteligente mediadora o negociadora".

47. ECHANO BASALDUA, J. I., "Mediación penal entre adultos: ámbito de aplicación en atención a la clase de infracción", *Cuadernos Penales José María Lidón*, 9, Deusto

regulación en un protocolo de justicia restaurativa aplicable a supuestos específicos, en los que se desarrollasen todos los mecanismos de justicia restaurativa –incluida la mediación– aplicables a los casos de violencia de género.

De esta forma se contribuiría a construir un modelo de justicia penal en el cual quedasen contempladas todas las alternativas disponibles con el objetivo de satisfacer las necesidades de todas las víctimas. En conclusión, la incorporación de la justicia restaurativa estaría dando respuesta a muchas de esas necesidades anteriormente descritas de las víctimas de violencia de género.

Por otra parte, la utilización de los ODR aplicables a los procedimientos de justicia restaurativa pueden abrir el abanico de opciones tanto de reparación a la víctima, de responsabilización al infractor como de participación a la comunidad. De ahí que también hubiese sido oportuno que en la norma proyectada se regulase todo lo referente a la aplicación de los recursos tecnológicos en los procedimientos de justicia restaurativa.

Como se ha señalado, una de las principales ventajas que pueden ofrecer los ODR es que a través de ellos las víctimas de violencia de género que voluntariamente quisiesen beneficiarse de las prácticas restaurativas pudiesen tener acceso a las mismas, al abrirse la posibilidad a realizar los encuentros restaurativos a distancia[48]. Las víctimas necesitan entornos seguros donde poder expresarse en términos de igualdad, apoyados por un profesional capacitado y especializado que le transmita seguridad, tranquilidad y confianza. Asimismo, con la utilización de los ODR se les estaría ofreciendo la oportunidad a las personas infractoras que lo consideren, de poder expresar su arrepentimiento y sus emociones en un espacio neutral. Es así que, estas prácticas restaurativas pueden llegar a reportar mayor tranquilidad y control a todos los participantes.

En definitiva, el uso de los ODR es indudable en este tipo de procedimientos, teniendo en cuenta tanto la flexibilidad de los mismos, como el valor añadido que puede llegar a reportar en los supuestos de violencia de género. Ahora bien, apostar por una inteligencia artificial que asuma funciones decisorias en prácticas restaurativas en general y en casos de violencia de género en particular, se antoja un tanto lejano, y hasta cierto punto, quizás improbable, dado el factor humano que impregna estos encuentros restaurativos.

Digital, Bilbao, 2013, p. 185, (http://www.deusto-publicaciones.es/deusto/pdfs/lidon/lidon09.pdf, última consulta: 07/09/2022).

48. CARRETERO MORALES, E., "La utilidad de los ODR en los casos de violencia de género"…, *op. cit*., p. 232.

VI
Retos de la Justicia juvenil ante las nuevas tecnologías

Capítulo 17

Posibilidades de desjudicialización de la ciberdelincuencia juvenil[1]

Esther Pillado González

Catedrática de Derecho Procesal
Universidad de Vigo

I. CONSIDERACIONES GENERALES SOBRE CIBERDELINCUENCIA

En las últimas décadas, los avances tecnológicos han aportado grandes beneficios a la sociedad en campos tan relevantes como la sanidad, las comunicaciones o la educación pero, al mismo tiempo, han producido cambios en el comportamiento delictivo, facilitando en muchos casos su comisión; en este contexto, la cibercriminalidad, entendiendo que, con carácter general, incluye cualquier delito en el que las TIC juegan un papel determinante en su comisión, esto es, todo aquel que es cometido en el ciberespacio[2], va adquiriendo cada vez una mayor importancia.

La falsa sensación de anonimato que confiere el entorno virtual y con ello la creencia de la falta de consecuencias de las actuaciones ilícitas, acompañada por la facilidad de la acción delictiva que ya no requiere unos especiales conocimientos técnicos, ha llevado al traslado de parte de la delincuencia al ciberespacio, tal como evidencian los datos de que se dispone.

1. Este trabajo ha sido elaborado en el marco del proyecto de investigación "Respuesta jurídica y socioeducativa a la violencia de género ejercida por menores. Protección de la víctima e intervención con el menor agresor", subvencionado por el Ministerio de Ciencia e Innovación, Proyectos de I+D+I" dentro de los Programas Estatales de Generación de Conocimiento y Fortalecimiento Científico y Tecnológico del Sistema de I+D+I y de I+D+I orientada a los Retos de la Sociedad en la convocatoria de 2019, (Ref. PID2019-106700RB-I00).

2. MIRÓ LINARES, F., *El cibercrimen. Fenomenología y criminalidad de la delincuencia en el ciberespacio*, Marcial Pons, Madrid, 2012, p. 44.

No se puede pasar por algo, además, que la crisis sanitaria provocada por la COVID-19, con el consiguiente confinamiento de toda la población, ha tenido una incidencia directa sobre la criminalidad puesto que la reducción en la movilidad y una mayor vigilancia policial ha llevado a un descenso del delito en la calle, mientras que se ha producido un aumento del cibercrimen debido a que nuestras actividades cotidianas y nuestro estilo de vida cambió sustancialmente haciendo que las relaciones interpersonales, el trabajo, las compras y el ocio hayan pasado de ser realizadas en el espacio físico, al ciberespacio; en coherencia con ello, también la actividad delictiva se ha trasladado a ese espacio y ha dado lugar a nuevas oportunidades delictivas[3]/[4].

Como muestra de ello, los datos sobre cibercriminalidad que se publican por el Ministerio del Interior evidencian que va creciendo año tras año el número de los hechos conocidos por las Fuerzas y Cuerpos de Seguridad, pasando de 92.716 en 2016 a 305.477 en 2021[5]. De la tipología de delitos cometidos, los más habituales son los fraudes informáticos (estafas), que representan el 87,4% seguidos a mucha distancia por las amenazas y coacciones que suponen un 5,7% del total o la falsificación informática (3,4%), acceso e interceptación ilícita (1,7%,), o delitos sexuales (0,5%)[6].

Como complemento de la información facilitada por al Ministerio del Interior, es importante tener en cuenta los datos publicados por la Fiscalía General del Estado (en adelante, FGE) en su *Memoria de 2020* cuando

3. *Vid.* VVAA, *Impacto del covid-19 en distintas formas delictivas*, Fundación para la investigación aplicada en delincuencia y seguridad, 2020, https://www.fiadys.org/wp-content/uploads/2020/10/2020_FIADYS-Impacto-COVID-Formas-Delictivas.pdf.
4. Todo ello sin olvidar que también se han incrementado la violencia intrafamiliar y de género como consecuencia de la convivencia que trajo consigo el confinamiento.
5. *Informe sobre cibercriminalidad en España de 2021,* Dirección General de Coordinación y Estudios. Secretaría de Estado de Seguridad, Sistema Estadístico de Criminalidad, Ministerio del Interior, p. 41, http://www.interior.gob.es/.
   La correcta comprensión de la información contenida en el citado informe requiere hacer dos consideraciones de interés: de un lado, que los datos han sido obtenidos del Sistema Estadístico de Criminalidad (SEC); para su cómputo se tienen en cuenta los hechos de los que han tenido conocimiento los siguientes cuerpos policiales: Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra, Mossos d' Esquadra y las Policías Locales que facilitan datos al SEC; como consecuencia de la incorporación al presente informe de los datos de la Ertzaintza y Mossos d' Esquadra, las series históricas publicadas hasta la fecha se han visto alteradas. De otro lado, as conductas ilícitas tenidas en cuenta son las registradas en el SEC), siguiendo la clasificación adoptada por el Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 añadiéndose, a la vista de nuestra realidad criminal, los delitos contra el honor y las amenazas y coacciones.
6. *Informe sobre cibercriminalidad en España de 2021…, op. cit*. p. 41.

señala, en el conjunto del Estado, fueron incoados un total de 16.914 procedimientos judiciales para la investigación y enjuiciamiento de hechos susceptibles de tipificarse en las categorías que nos ocupan. Este resultado no solo da cuenta del incremento en un 28,69% en el volumen anual de procedimientos incoados, que en 2019 sumaron 13.143, sino que, además, confirma la tendencia ascendente que venimos constatando en relación con los ciberdelitos desde la puesta en funcionamiento de esta área de especialización en julio del año 2011[7]. Las estafas/defraudaciones de los artículos 248 y ss. CP siguen siendo el tipo de ilícitos *on line* que generan anualmente un volumen mayor de procedimientos judiciales. En esta ocasión la cifra asciende a 12.250, lo que implica un incremento del 42,25% concretado en 3.639 expedientes, respecto de la cifra obtenida por igual concepto en el año 2019 y un porcentaje anual del 72,43% del volumen total de nuevos expedientes por ciberdelitos. Es decir, casi tres cuartas partes de las causas judiciales por ciberdelitos registradas en 2020 tuvieron por objeto hechos ilícitos de estas características. Sin embargo, tal como apunta la FGE, los datos publicados no pueden llevar a la conclusión de que la delincuencia en la red es principalmente defraudatoria pues hay otro tipo de criminalidad, como los atentados contra la libertad e indemnidad sexual de los menores o los ataques a los sistemas informáticos que son difíciles de cuantificar pues su denuncia es complicada y no se reflejan en las estadísticas policiales ni judiciales. De especial importancia son también los delios contra la libertad y seguridad personal que representan el 10,10% de los ciberdelitos, en su mayor parte amenazas y coacciones, pero también conductas de hostigamiento[8]. Finalmente, generan gran preocupación los delitos contra la libertad sexual, especialmente los que se ejercen frente a personas menores de edad; en su conjunto suponen un 8,5% del total de los ciberdelitos. Este tipo de infracciones han aumentado considerablemente en el último año no sólo como consecuencia del confinamiento provocado por la pandemia, sino también por la mayor sensibilidad de progenitores y tutores ante la vulnerabilidad de los menores, que ha llevado a un aumento de las denuncias. Pero se destaca por la FGE que los datos no reflejan la situación real, pues es frecuente que en los procedimientos incoados se investigue una diversidad de acciones atribuidas a una persona, pero

7. Apartado 8.1 del Capítulo III. *Memoria FGE de 2020*, Madrid, 2021. En esta memoria únicamente se analiza y valora la información referida a procedimientos o investigaciones que se encuentran bajo el control de los órganos judiciales y/o del Ministerio Fiscal. Son numerosísimas las denuncias o hechos presuntamente delictivos que llegan a conocimiento de los cuerpos policiales y que no son comunicados a las autoridades judiciales por falta de autor conocido, por mor de lo dispuesto en el artículo 284 LECrim.

8. En muchas ocasiones, vinculadas a violencia de género utilizando la sextorsión.

reiteradas en el tiempo y ejercitadas en relación a un número más o menos elevado de menores[9].

II. CIBERDELINCUENCIA Y MENORES

La ciberdelincuencia tiene una incidencia especial en relación a los menores de edad debido a que se trata de generaciones en las que el uso de la tecnología forma parte de su entorno habitual desde su nacimiento, de manera que su uso está absolutamente integrado en su vida; así, nuestros niños, niñas y adolescentes no han tenido que realizar ningún esfuerzo para su utilización como medio para comunicarse y relacionarse, divertirse, buscar fuentes de conocimiento o información o consumir.

Como muestra de ello, de acuerdo con los datos publicados en 2021 por el Instituto Nacional de Estadística, (en adelante, INE), el uso de internet en los últimos tres meses es prácticamente universal (99.7%) en las personas entre 16 y 24 años, luego va descendiendo conforme aumenta la edad, de manera que, a partir de los 55 años se sitúa en el 91% y, en el grupo de 65 a 74 años baja hasta el 73,3%. En cuanto a la utilización de redes sociales, el 64,7% de la población de 16 a 74 años ha participado durante los tres últimos meses en redes sociales de carácter general (como *Instagram*, *Facebook*, *Twitter*, *YouTube*…), siendo los más participativos los estudiantes (96,4%) y los jóvenes de 16 a 24 años (93,2%). Se incluye además por el INE un apartado sobre el uso de las TIC por menores entre 10 y 15 años donde se indica que en un porcentaje elevado utilizan el ordenador (95,1%) y todavía más Internet (97,5%)[10].

La enorme presencia de los menores en el ciberespacio, así como sus habilidades en el manejo de las TIC les sitúa en una posición idónea tanto para ser víctimas como victimarios de ciberdelitos; además, al ser el ciberespacio su entorno habitual y cotidiano de relación, lo perciben como un contexto inofensivo, donde no sólo no existen riesgos, sino que todas las conductas son válidas pues les resulta difícil calificar una actuación como ilícita. En concreto, en relación a los infractores, la falsa sensación de anonimato y la creencia de que sus actos en el mundo virtual no tendrán consecuencias negativas para ellos, les llevan a considerar el ciberespacio como un ámbito en el que la comisión del delito es fácil y cómoda, llegando a realizar una serie de conductas que no harían en el mundo real;

9. Apartado 8.1 del Capítulo III. *Memoria FGE de 2020*.
10. Instituto Nacional de Estadística, *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares Año 2021*, https://www.ine.es/.

aunque, en muchas ocasiones, como se acaba de apuntar, no son conscientes de la actividad delictiva[11].

Si acudimos a los datos sobre cibercriminalidad publicados por el Ministerio del Interior en el 2021 relativos al perfil del responsable, la franja de edad con mayor número de personas investigadas/detenidas es la comprendida entre 26-40 años que representa un 40% del total, mientras que la franja de 14-18 años supone menos de un 5%, superando únicamente a quienes ocupan la franja de mayores de 65 años. En lo que respecta a los menores de edad, han sido detenidos o investigados por un total de 448 menores de los cuales 183 fueron por amenazas y coacciones (40,8%), 105 fraudes informáticos (23,4%), 73 accesos e interceptaciones ilícitas (16,3%), y 60 delitos sexuales (13,4%)[12].

Si tenemos en cuenta los datos publicados por la FGE, en el año 2020 se ha producido un descenso de la criminalidad juvenil en torno al 20% motivado por la pandemia de la Covid-19, el confinamiento durante más de dos meses, los estados de alarma y las restricciones a la movilidad perimetrales y de horarios; tal como se resalta en la *Memoria*, se trata de un descenso coyuntural que impide extraer consecuencias criminológicas de futuro[13]. Por tanto, a efectos de establecer tendencias sobre la evolución de la delincuencia juvenil, deben tomarse lo datos recogidos en la *Memoria FGE de 2019*, y siempre "con carácter aproximativo y con las cautelas que impone la escasa fiabilidad estadística de las aplicaciones" utilizadas; en concreto, se constató una tendencia a la baja desde el año 2011 al 2016, que se frenó en 2016, apreciándose en 2017 un repunte ligero, aunque significativo, de la delincuencia juvenil. En el año 2018 se apreció que tal incremento no se consolidaba y alguno de los parámetros retrocedían. En 2019 se puede estimar, con prudencia, que vuelve a existir otro ligero incremento que casi retrotrae a las cifras de hace dos años. En definitiva, puede concluirse que se produce un estancamiento de la delincuencia juvenil desde 2017 a esta parte, luego de los importantes descensos de la primera mitad de la década, con ligeros picos al alza y a la baja los dos últimos años[14].

En lo que se refiere a la ciberdelincuencia juvenil, debe partirse de la dificultad de obtención de cifras concretas pues queda disperso este tipo

11. *Vid.* MARTÍNEZ GALINDO, G., "Motivación criminal de los adolescentes en el ciberespacio", *en Tratado sobre delincuencia juvenil y responsabilidad penal del menor* (coords. ABADÍAS SELMA, CÁMARA ARROYO, SIMÓN CASTELLANO), La Ley, Madrid, 2021, pp. 501 y ss.
12. *Informe sobre cibercriminalidad en España de 2021…, op. cit*. p. 53.
13. Apartado 6.2.2, del Capítulo III, *Memoria de la FGE de 2020.*
14. Apartado 6.2.2 del Capítulo III *Memoria de la FGE de 2019*, Madrid, 2020, https://www.fiscal.es.

de criminalidad entre distintos tipos delictivos; por ese motivo, en las Memorias de la FGE se parte de la contabilidad manual que se realiza por numerosas secciones y de la información que consta en los informes[15]. En concreto, se destaca que, una parte importante de los delitos de acoso escolar se perpetran de forma virtual, en muchas ocasiones a través de *Whatsapp* o de la red social *Instagram*[16]; por razones obvias, derivadas de la suspensión de clases durante la pandemia, en el 2020 se produjo un descenso significativo del número de denuncias presentadas[17]; durante el año 2019 se mantuvo una línea de estabilidad iniciada en el 2018, después del descenso en el número de denuncias que contrastó con el aumento considerable de las mismas durante en el 2015 y 2016. Pocas novedades se destacan en el año 2020 en el que se sigue procediendo al archivo de un elevado número de asuntos por no haber alcanzado el presunto infractor la edad de 14 años[18]; únicamente se resalta que, aunque el foco está puesto en el acoso cibernético entre iguales, cada vez se producen con más frecuencia supuestos en las que las víctimas son docentes a los que se fotografía o graba, sin su consentimiento, en situaciones que herían su reputación, para su difusión a través de grupos de *Whatsapp*.

Tal como se destaca por la FGE en la *Memoria de 2020*, la pandemia no ha modificado la comisión de delitos contra la intimidad, especialmente el tipo del art. 197.7 CP, por difusión de material de contenido sexual a través de redes sociales o *Whatsapp*. En este aspecto inciden de manera coincidente las delegaciones de menores de Las Palmas y Asturias, en la banalización de los comportamientos sexuales a través de las redes por parte de preadolescentes o adolescentes[19]. Respecto a este tipo penal, se insistía en la *Memoria FGE de 2019* sobre la falta de consideración que tienen los menores de su propia intimidad en cuanto se hacen fotos y graban vídeos con escenas sexualmente explícitas y también la falta de empatía y

15. No se debe olvidar que los ciberdelitos no están incluidos en un título específico del CP, sino que se trata de distintos tipos delictivos que están diseminados a lo largo del citado texto legal.
16. Dentro del ciberbullying se incluyen diversas conductas típicas, entre ellas, principalmente, el ciberstalking, las amenazas y coacciones, las injurias, los delitos contra la intimidad, la usurpación de la personalidad o los delitos contra la integridad moral.
17. Apartado 6.2.2.8 del Capítulo III, *Memoria de la FGE de 2020*.
18. Aunque en la *Memoria de la FGE de 2020* no se recoge el dato concreto de los archivos por esta causa, en el 2019, se archivó el 43% de las denuncias por ese motivo. *Vid*. apartado 6.2.2.8 del Capítulo III *Memoria de la FGE de 2019*.
19. Apartado 6.2.2.9 del Capítulo III, *Memoria de la FGE de 2020*. Se añade que "La Delegada de Las Palmas, introduce un matiz interesante: si bien en adultos la difusión de imágenes de contenido sexual va asociada frecuentemente a una ruptura de pareja, entre menores se toma como 'un puro juego', pues se facilitan imágenes sin relación previa sentimental alguna".

de conciencia delictiva de quienes posteriormente las difunden sin autorización[20]. Otro tanto ocurre con la difusión de imágenes vejatorias o degradantes en muchos casos a través de la red social *Instagram* con el objeto de sentirse integrado al conseguir más seguidores y más *likes*.

Se alerta también de la detección de conductas delictivas que buscan un beneficio económico, ya sean estafas, como pueden ser compras fraudulentas[21] o de delitos de daños informáticos con graves repercusiones para infraestructuras críticas[22].

Ante la ciberdelincuencia ejercida por menores de edad, y al margen de necesidad de políticas centradas en la prevención de la comisión de este tipo de delitos, debe incidirse en la importancia de establecer medidas alternativas a la justicia penal que sean de aplicación en estos casos, tal como resalta el Comité de los Derechos del Niño[23]. Por ello, se dedican los apartados siguientes a las distintas opciones que prevé la LO 5/2000, de 12 de enero, reguladora de la responsabilidad penal de menores (en adelante, LORPM) para desjudicializar el asunto, destacando cuáles pueden ser más adecuadas para responder ante esta tipología delictiva, pero sin olvidar la atención a la víctima que, en muchas ocasiones, es también menor de edad.

III. PRINCIPIO DE OPORTUNIDAD EN EL PROCESO PENAL DE MENORES

La normativa internacional de justicia juvenil incluye diversas disposiciones que resaltan la conveniencia de introducir medidas tendentes a la desjudicialización de los asuntos en que se vean involucrados en la comisión de delitos niños, niñas y adolescentes; así, la Convención de Derechos del Niño estableció en su art. 40.3 que "Los Estados tomarán todas las medidas apropiadas para promover el establecimiento de leyes, procedimientos, autoridades e instituciones específicos para los niños de quienes se alegue que han infringido las leyes penales o a quienes se acuse o declare culpables de haber infringido esas leyes, y en particular: b) Siempre que sea apropiado y deseable, la adopción de medidas para tratar a esos niños sin recurrir a procedimientos judiciales, en el entendimiento

20. Apartado 6.2.2.9 del Capítulo III *Memoria de la FGE de 2019*.
21. Así se destaca en el apartado 6.2.2.9 *Memoria de la FGE de 2018*, Madrid, 2019, https://www.fiscal.es.
22. Apartado 6.2.2.9 del Capítulo III *Memoria de la FGE de 2020*.
23. Apartado XIII.B de la Observación general núm. 25 (2021) del Comité de los Derechos del Niño, *relativa a los derechos de los niños en relación con el entorno digita*l.

de que se respetarán plenamente los derechos humanos y las garantías legales". De forma más concreta, en la regla 11.1 de las Reglas de Beijing se señala expresamente que "se examinará la posibilidad, cuando proceda, de ocuparse de los menores delincuentes sin recurrir a las autoridades competentes, mencionadas en la regla 14.1 infra, para que los juzguen oficialmente", así, se alude a la "remisión de casos", entendiendo que es la reacción más adecuada, atendiendo a las consecuencias que la respuesta penal pudiera tener en los menores inmersos en un conflicto penal[24]. A nivel europeo, la Recomendación (87) del Comité de Ministros del Consejo de Europa sobre Reacciones sociales ante la delincuencia juvenil, en su apartado II.2, también hace un llamamiento a los Estados miembros para instaurar procedimientos de desjudicialización, considerando que el proceso penal juvenil debe ser el último recurso.

En coherencia con las citadas normas, la LORPM introduce a lo largo de su articulado distintas previsiones que suponen claras manifestaciones del principio de oportunidad, algunas con el objeto de mantener al menor alejado del sistema de justicia penal, y otras que permiten, una vez iniciado el proceso, que termine de forma anticipada con la adopción de una medida extrajudicial o, finalmente, dictada la medida en la sentencia, se permite su modificación o suspensión. En todo caso, se trata de evitar la estigmatización que para el niño, niña o adolescente supone su paso por el sistema de justicia.

Así, aunque en nuestro sistema de justicia juvenil rige de forma plena el principio de legalidad, lo que supone que, ante la presunta comisión de un delito por un niño, niña o adolescente, se iniciará el proceso que deberá tramitarse siguiendo los cauces previstos legalmente hasta el momento de la sentencia en la que se impondrá, en su caso, la medida que corresponda que será ejecutada en los términos legales, se permite un amplio margen al principio de oportunidad en distintos momentos del proceso e incluso de la fase de ejecución de las medidas impuestas. En concreto, antes del inicio de la fase de instrucción propiamente dicha, y tras la práctica de las diligencias preliminares, el Fiscal puede acordar el desistimiento de la incoación del expediente conforme a lo previsto en el art. 18 LORPM. Posteriormente, iniciada la instrucción, es posible que se decrete el sobreseimiento del expediente por diferentes razones (arts. 19 y 27.4 LORPM). Y,

24. También en esa misma línea las Directrices de Riad consideran la posibilidad de establecer un puesto de mediador o un órgano análogo independiente para los jóvenes que garantice el respeto de su condición jurídica, sus derechos y sus intereses, así como la posibilidad de remitir los casos a los servicios disponibles. En este sentido, debe existir personal capacitado para remitir a los jóvenes a sistemas alternativos a la justicia penal (directrices 57 y 58).

en la fase intermedia del proceso, o, al inicio de la fase de audiencia, cabe la terminación anticipada del proceso por conformidad del menor y de su abogado (arts. 32 y 36 LORPM). A su vez, tras la sentencia en la que se imponga al menor infractor alguna de las medidas legalmente previstas, el principio de oportunidad reglada se manifiesta tanto en la posibilidad de suspensión condicional de la ejecución del fallo (art. 40 LORPM), como en la eventual sustitución de las medidas impuestas por otras más adecuadas (arts. 51 y 14 LORPM).

Todas estas manifestaciones del principio de oportunidad tienden a hacer efectivos los principios de subsidiariedad o intervención mínima del derecho penal y el del superior interés del menor, buscando otras posibles soluciones que sean menos represivas y más educativas y que faciliten la resocialización del menor.

De todas ellas, a la vista de los delitos que con más frecuencia se cometen por los niños, niñas y adolescentes en el ciberespacio y teniendo en cuenta la necesidad de equilibrar no sólo la orientación educativa de la LORPM, sino también la atención a la víctima, teniendo en cuenta que en un porcentaje elevado de casos también es menor[25], me voy a centrar en los supuestos de desistimiento de la incoación del expediente (art. 18 LORPM) y de sobreseimiento por conciliación o reparación o realización de actividad educativa a propuesta del Equipo Técnico en su informe (art. 19 LORPM).

IV. DESISTIMIENTO DE LA INCOACIÓN DEL EXPEDIENTE DE REFORMA

Tal como señala la FGE, el desistimiento de la incoación del expediente es la manifestación "más radical" del principio de oportunidad pues, cumpliéndose los requisitos legales, depende únicamente de una decisión del Ministerio Fiscal, sin exigirse una previa propuesta del Equipo Técnico ni una conducta concreta del menor, como ocurre en el sobreseimiento acordado al amparo de los arts. 19 y 27.2 LORPM[26]. Además, acordándose a través del decreto del Ministerio Fiscal, al carecer de carácter jurisdiccional, el desistimiento no es recurrible.

25. No se debe olvidar que el interés del menor en el contexto de la justicia juvenil, no sólo se aplica al menor en conflicto con la ley, ya sean presuntos autores, acusados o condenados, sino también a quienes están en contacto con el proceso penal, ya sean víctimas o testigos. *Vid.* Apartado IV.A.2 b. Observación general núm. 14 (2013) del Comité de los Derechos del Niño, *sobre el derecho del niño a que su interés superior sea una consideración primordial (artículo 3, párrafo 1).*

26. Apartado IV.5.1 Circular 9/2011 FGE, *sobre criterios para la Unidad de actuación especializada del Ministerio Fiscal en materia de reforma de menores*.

Las circunstancias que condicionan la facultad del Fiscal de desistir de la incoación del expediente están previstas en el art. 18 LORPM en los términos siguientes; en primer lugar, debe tratarse de hechos que estén tipificados en el CP o en otras leyes penales especiales como delito menos grave (arts. 13.3 y 33.4) o leve (arts. 13.2 y 33.2)[27]. En segundo término, en el caso de los delitos graves, se requiere que no concurra violencia o intimidación en las personas, lo que no se exige en el caso de los delitos leves. Por último, que el menor no haya cometido con anterioridad otros hechos de la misma naturaleza. Esta exigencia, debido a su vaguedad, ha suscitado dudas interpretativas, porque no está claro qué se ha de entender a estos efectos por "hechos de la misma naturaleza". La FGE se ha decantado por una interpretación restrictiva de la posibilidad de acordar el desistimiento entendiendo que no se exige que el menor haya sido condenado con anterioridad por la comisión de un hecho delictivo, puesto que la LORPM se refiere a hechos, no a delitos ni a condenas[28]. Pese a ello, no se puede olvidar que es preciso que "conste" que el menor ha cometido con anterioridad esos hechos, por lo que, si bien no se requiere la existencia de una sentencia de condena previa, sí es obligado que de algún modo se haya dejado acreditada la comisión de tales hechos por el menor[29], como puede ser, por ejemplo, si ha se ha desistido de la incoación del expediente con anterioridad.

La exigencia de que el menor no haya cometido hechos de la misma naturaleza también genera dudas a la hora de su aplicación; la FGE, en su Circular1/2000, se ha decantado por una interpretación amplia de esta

27. Tal como señala la FGE en su Dictamen 1/2015 *sobre criterios de adaptación de la LORPM a la reforma del Código Penal por LO 1/2015*, pese a que la LO 1/2015, no modifica la LORPM, todas las referencias a las faltas contenidas en la misma "deben entenderse automáticamente sustituidas por la expresión "delitos leves", como categoría de infracción penal que las reemplaza" (apartado II).

28. Apartado VI.2.c Circular FGE 1/2000, de 18 de diciembre, *relativa a los criterios de aplicación de la Ley Orgánica 5/2000, de 12 de enero, por la que se regula la responsabilidad penal de los menores*.

29. Como señala GARCÍA INGELMO ("Ejercicio del principio de oportunidad en la jurisdicción de menores. Supuestos legales. Cuestiones prácticas y Directrices de la FGE", en Curso: Seminario de especialización en menores: Responsabilidad penal y protección. Novedades legislativas, Madrid, del 29 al 31 de marzo de 2017, https://www.fiscal.es, p. 13), desde la entrada en vigor de la LORPM, para verificar ese extremo, se han consultado los antecedentes que obran en las bases de datos de las Fiscalías de diligencias preliminares o expedientes que previamente se le hubiesen abierto al menor; Cuestión distinta es que tales bases y aplicaciones informáticas presenten múltiples deficiencias y no estén comunicadas entre sí, de manera que en ninguna Sección provincial es posible conocer los antecedentes de causas que se le hayan abierto a un menor en la Fiscalía de otra provincia, aunque sean provincias de la misma Comunidad Autónoma.

fórmula, prohibiendo el desistimiento cuando el menor hubiere incurrido con anterioridad en hechos constitutivos de delito grave o, si se trata de delito menos grave, que en su ejecución se haya empleado violencia o intimidación, aunque los hechos presenten una naturaleza diversa. En cambio, si los hechos anteriores eran constitutivos de delito menos grave o leve cometido sin violencia o intimidación, sólo impiden el desistimiento si tienen la misma naturaleza que el hecho actual, atendiendo a si se ha visto lesionado el mismo bien jurídico de un modo semejante[30]. Continuando con esa misma línea restrictiva, en su Circular 9/2011, la FGE señala que la norma debe ser interpretada con prudencia y a partir de la consideración de que el desistimiento es un beneficio pensado para infractores primarios; así, tendrá carácter excepcional el desistimiento cuando consten antecedentes, careciendo de sentido cuando se acumulen diligencias abiertas por diferentes tipos penales[31].

Finalmente, debe tenerse en cuenta que, aunque el art. 18 LORPM lleva como rúbrica, desistimiento de la incoación del expediente por corrección en el ámbito educativo y familiar[32], esta condición no se contempla expresamente en el texto del art. 18 LORPM; sin embargo, las circunstancias que rodean al menor serán tenidas en cuenta como un elemento más de valoración dentro del margen de discrecionalidad del fiscal a la hora de la toma de decisión.

A la vista de los requisitos anteriores, y teniendo en cuenta los propios criterios establecido en la Circular FGE 9/2011, el fiscal, ante la posibilidad de desistir de la incoación del expediente debe tener en cuenta que se trate de un hecho delictivo aislado que responda a una conducta antisocial propia de la adolescencia. También habrá de valorarse el tiempo transcurrido desde la comisión del delito puesto que, si es demasiado, la intervención carecerá de sentido; esto ocurre en los casos en que el autor ha alcanzado la mayoría de edad, pues ya no procede la adopción de medidas que están concebidas para menores.

Además, pese al silencio del art. 18 LORPM, el fiscal debería tomar declaración a la víctima, si es individualizable, no sólo para tener una idea

30. Apartado VI.2.C Circular FGE 1/2000.

31. Apartado IV.5.1. Circular FGE 9/2011.

32. Esa referencia al ámbito educativo y familiar es prácticamente lo único que queda de la redacción del Proyecto de 1998, cuyo art. 18 era mucho más restrictivo y señalaba que "El Ministerio Fiscal podrá desistir de la incoación de expediente cuando, tratándose de menores de dieciséis años, los hechos denunciados puedan encontrar su corrección en el ámbito educativo familiar o comunitario, y a ello se comprometan los padres o representantes legales del menor, o los responsables de las correspondientes instituciones sociales. En tal caso, el Ministerio Fiscal dará traslado de lo actuado a la entidad pública de protección de menores para la aplicación, si procede, de lo establecido en el art. 3-1 de la presente Ley".

clara de las circunstancias que rodean la comisión del delito, sino también para que se sienta partícipe de la resolución del conflicto que se ha generado con la acción delictiva; y aunque no se incluye en ningún momento como requisito para el desistimiento el pago de la responsabilidad civil, se trata de un elemento que, aunque no debería condicionar su decisión para evitar discriminaciones, puede ser valorado por el Fiscal a la vista de las circunstancias concurrentes.

Por supuesto, el decreto que dicte el Ministerio Fiscal, pese al silencio del art. 18 LORPM debe estar motivado, y no es susceptible de recurso al no ser una resolución judicial, tal como ya se ha apuntado[33]; todo ello con independencia de que sea necesaria su notificación a ofendidos y perjudicados, tal como prevén los arts. 4.5 y 18.1 LORPM[34]. Además, pese a no exigirse por al citado precepto, también debería comunicarse esta resolución a los representantes legales del menor, para evitar que los mismos desconozcan que el menor ha cometido una infracción penal[35].

33. Tampoco cabe aquí ninguna revisión por parte del Juez de Menores, que carecería de competencia funcional para ello.

    Se ha cuestionado mucho la imposibilidad de recurrir esta resolución, sobre todo, a la vista de las previsiones contenidas en el Estatuto de la Víctima del delito relativas al derecho de la víctima a recurrir las resoluciones de sobreseimiento, incluso cuando no está personada en el procedimiento. Al respecto, en el Dictamen 1/2016, del Fiscal de Sala coordinador de Menores, *sobre adaptación de la Ley 4/2015, del Estatuto de la víctima del delito, al ámbito de la Justicia Juvenil*, señala que el art. 12.2 Estatuto de la Víctima del Delito, reconoce el derecho de la víctima a recurrir las resoluciones de sobreseimiento, "conforme a lo dispuesto en la Ley de Enjuiciamiento Criminal, sin que sea necesario para ello que se haya personado anteriormente en el proceso", de acuerdo con su tenor literal, sólo es aplicable en el contexto de un procedimiento judicial, pero no en las diligencias preliminares, que, en cuanto diligencias de investigación, tienen un carácter preprocesal. Ahora bien, para evitar situaciones de indefensión, "según las circunstancias y gravedad del asunto, cuando la víctima hubiera manifestado en preliminares su intención de personarse, o concurra cualquier otro motivo relevante, puede valorarse por el Fiscal, aunque aprecie motivos para acordar el sobreseimiento conforme al art. 16.1 LORPM, la posibilidad de solicitarlo del Juez de Menores tras incoar expediente, habilitando así al perjudicado para que pueda recurrir y personarse en el expediente abierto".

    Se trata de una cuestión, la irrecurribilidad de la decisión del fiscal de desistir de la incoación del expediente, que habrá que replantearse en una futura reforma de la LORPM para garantizar de forma adecuada los derechos de las víctimas en el ámbito de la justicia juvenil.

34. También se prevé expresamente en el art. 18 LORPM el traslado de lo actuado a la entidad pública de protección de menores para la aplicación de las previsiones contenidas en el art. 3 LORPM relativas a la actuación ante la comisión de delitos por menores de 14 años; no obstante, sólo se procederá a este traslado cuando, a la vista de las circunstancias concurrentes, se observe una situación de riesgo o desamparo que requiera la intervención de la citada entidad. *Vid.* apartado VI.2 Circular FGE 1/2000.

35. GARCÍA INGELMO, F. M.– "Ejercicio del principio de oportunidad en la jurisdicción de menores. Supuestos legales. Cuestiones prácticas y Directrices de la FGE…", *op. cit.*, p. 17

Una buena práctica en todo caso, es la toma de declaración del menor, antes de la adopción del decreto de desistimiento pues permite un "cara a cara" con el Fiscal que va a permitir a este último constatar su arrepentimiento por el hecho y hacerse una idea más aproximada de su situación personal y familiar. Sirve, asimismo, para informar al menor de las consecuencias de su conducta y para que sus padres tengan conocimiento de la infracción[36]

A vista de lo expuesto, el ámbito para acordar el desistimiento en los ciberdelitos es escaso, pues queda limitado a los supuestos de delitos menos graves o leves, sin violencia o intimidación; así, podría ser de utilidad como medida de desjudicialización en relación a los delitos contra la intimidad, ya se trate de *sexting* o de relevación y difusión de contenidos de carácter vejatorio o denigrante para la víctima. También podría ser de interés su utilización en supuestos de *ciberbullying* siempre que no conlleven amenazas o coacciones. En estos casos, puede no ser necesaria una respuesta desde el sistema de justicia juvenil, siendo suficiente que la familia o la escuela adopten medidas en relación al menor y el delito. El fiscal deberá examinar las circunstancias concurrentes que rodean la comisión del delito y al propio menor, debiendo escuchar a la víctima y, en todo caso, dar audiencia al menor para que se enfrente a las consecuencias de sus actos delante del fiscal y constatar si es consciente del daño causado y se arrepiente de su actuación. Además, en supuestos de acoso escolar y pese a no estar expresamente previsto, el desistimiento habrá de acompañarse de una simultánea remisión de testimonio de lo actuado a la dirección del centro docente para que adopte las iniciativas que estime oportunas en relación a víctima y victimario[37].

V. SOBRESEIMIENTO DEL EXPEDIENTE POR CONCILIACIÓN, REPARACIÓN O ACTIVIDAD EDUCATIVA

En todos aquellos casos en que el fiscal, a la vista de las circunstancias concurrentes en relación a la presunta comisión del delito por parte del menor, descarta la adecuación del desistimiento, deberá dictar decreto

36. GARCÍA INGELMO, F. M.– "Ejercicio del principio de oportunidad en la jurisdicción de menores. Supuestos legales. Cuestiones prácticas y Directrices de la FGE…", *op. cit.*, p. 20.

37. Apartado 7.1.1 Instrucción FGE 10/2005, de 6 de octubre, *sobre el tratamiento del acoso escolar desde el sistema de justicia juvenil*. Insiste la FGE en el carácter subsidiario del sistema de justicia juvenil, de manera que "el primer nivel de lucha contra el acoso escolar debe estar liderado por los profesores del centro educativo, y que ellos deben ser los primeros destinatarios de la puesta en conocimiento del problema. El abordaje debe ser conjunto, y preferentemente desde los niveles básicos de intervención: padres, profesores y comunidad escolar".

de incoación del expediente de reforma. Iniciada formalmente la fase de instrucción, en atención a las diligencias de investigación practicadas y teniendo en cuenta el contenido del informe elaborado por el Equipo Técnico, podrá ponerle fin de forma anticipada solicitando al Juez de Menores el sobreseimiento y archivo de las actuaciones; para ello, atenderá a la gravedad y circunstancias de los hechos y del menor, de modo particular a la falta de violencia o intimidación graves en su conducta, y condicionando tal posibilidad a la observancia por parte del menor de alguna de las siguientes conductas: que se haya conciliado con la víctima, que haya asumido el compromiso de reparar el daño causado a la víctima o al perjudicado por el delito, o que se haya comprometido a cumplir la actividad educativa propuesta por el Equipo Técnico en su informe (art. 19.1 LORPM)[38].

Esto es, el fiscal, dentro del margen de discrecionalidad que le permite la LORPM, valorará si, de toda la información de que dispone en relación al menor presunto infractor y al delito, y siempre que entienda necesaria una respuesta dentro del sistema de justicia juvenil, es adecuada la celebración de la audiencia con la consiguiente práctica de prueba que permita fundamentar una sentencia, o es más conveniente, a la vista del interés del menor, una medida extrajudicial[39].

Pues bien, la viabilidad del sobreseimiento que regula el art. 19 LORPM, se condiciona a la concurrencia de tres presupuestos concretos; en primer término, que el hecho imputado al menor constituya delito menos grave o leve, entendiendo, como ya se expuso al analizar este mismo requisito para el desistimiento de la incoación del expediente, que la adecuada comprensión del precepto exige la remisión a los correspondientes preceptos del CP[40].

38. También procedería en este momento un sobreseimiento a propuesta del Equipo Técnico el ET ante la inconveniencia de continuar la tramitación del expediente en interés del menor en los supuestos previstos en el art. 27.4 LOPRM; de un lado, cuando se hubiera expresado suficientemente al menor el reproche que merece su conducta a través de los trámites ya practicados, en el sentido de que por el simple hecho de que el menor haya estado sometido al proceso de menores hasta este momento ya constituye un reproche suficiente. De otro, cuando resulte inadecuada cualquier intervención por el tiempo transcurrido desde la comisión de los hechos, debido a que ha pasado mucho tiempo desde que el menor cometió los hechos y ya carece de sentido llevar a cabo una actividad educativa.

39. Tal como apunta la SAP de Navarra, de 21 de diciembre de 2002 (JUR 2002, 284756), la mediación no es obligatoria en ningún caso, sin que requiere que el fiscal, de cumplirse los requisitos del art. 19 LORPM, valore las circunstancias concurrentes; el mismo sentido, el Equipo Técnico, si así lo considera, a la vista del interés el menor, puede incluir en su informe esta medida extrajudicial.

40. Por tanto, se rechaza la aplicación del art. 19 LORPM cuando se trata de la presunta comisión de un delito grave. *Vid*. AAAP de Navarra, de 9 de octubre de 2012 (JUR 2012, 404373); Barcelona, de 9 de enero de 2013 (JUR 2013, 66583).

En segundo lugar, que los hechos se hayan cometido sin violencia o intimidación graves, lo que supone que se podría decretar el sobreseimiento aunque haya existido cierta violencia o intimidación en la actuación del menor, siempre que no se puedan calificar de graves[41]. Por lo demás, se debe entender que esta violencia grave que excluye la posibilidad de sobreseimiento es la cometida sobre las personas, evidenciando una falta de respeto a los valores fundamentales de la convivencia, puesto que la violencia referida exclusivamente a las cosas puede ocasionar un perjuicio patrimonial que siempre es susceptible de reparación.

En otro orden de cosas, también cabe destacar que el art. 19 LORPM nada dice sobre la necesidad de que el menor no sea reincidente o no haya cometido con anterioridad otros hechos similares. Pero esta circunstancia se puede entender implícita en la referencia legal a las "circunstancias de los hechos y del menor" que deben ser valoradas por el fiscal antes de decidir sobre la procedencia del sobreseimiento, ya que parece lógico incluir entre tales circunstancias los antecedentes del menor[42]. En este sentido, la FGE considera que este tipo de medidas extrajudiciales son adecuadas cuando se trate de dar una respuesta puntual a infracciones igualmente puntuales cometidas por menores, debiendo descartarse cuando el hecho o circunstancias del menor demanden una respuesta global[43].

Finalmente, exige el art. 19 LORPM que el menor se haya conciliado con la víctima o haya asumido el compromiso de reparar el daño causado a la víctima o perjudicado o se comprometa a cumplir la actividad educativa que propone el Equipo Técnico en su informe. Además, tras la reforma operada por la LO 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, debe tenerse en cuenta el requisito incluido en el nuevo apartado del art. 19.2 LORM. Al respecto, cuando se trate de un menor autor de alguno de los delitos tipificados en los Capítulos I y II del Título VIII del Código Penal, o que estén relacionados con violencia de género, no tendrá efecto de conciliación, a menos que la víctima lo solicite

41. *Vid.*, CALLEJO CARRIÓN, S., "El principio de oportunidad en la LO 5/2000, de 12 de enero, reguladora de la Responsabilidad Penal de los Menores", *Diario La Ley*, Núm. 6366, 24 de noviembre de 2005, p. 7; ORNOSA FERNÁNDEZ, R., *Derecho Penal de Menores*, Bosch, Barcelona, 2007, p. 280.

    A efectos de calificar la violencia o intimidación como "graves", GARCÍA ESTEBAN y GUTIÉRREZ ALBENTOSA ("Criterios para la interpretación del término 'graves' del art. 19.1 de la Ley penal del menor en el proceso de mediación", La Ley-penal, núm. 156, 2022, pp. 7 y 8) establecen un catálogo abierto de pautas orientativas entre las que incluyen el trato degradante, las lesiones, el uso de armas o medios peligrosos o la utilización de violencia excesiva, desproporcionada e innecesaria.

42. *Vid.* CALLEJO CARRIÓN, S., "El principio de oportunidad en la LO 5/2000, de 12 de enero…", *op. cit.*, p. 7.

43. Apartado IV.5.2 Circular FGE 9/2011.

expresamente y que el menor, además, haya realizado la medida accesoria de educación sexual y de educación para la igualdad". No ha sido muy afortunado el legislador a la hora de redactar el precepto, cuya lectura genera dudas de interpretación no sólo porque no queda claro qué debe solicitar expresamente la víctima (¿la conciliación?), sino porque tampoco queda claro si la medida "accesoria" de educación sexual y de educación para la igualdad condiciona el sobreseimiento por mediación tanto en caso de conciliación como de reparación[44]. Quizás la forma más coherente de entender esta nueva disposición a la vista del propio espíritu de la LO 10/2022 y del interés superior del menor que inspira la LORPM será que, cuando se trate de alguno de los delitos que el precepto enumera, en caso de conciliación o reparación, voluntariamente aceptada por ambas partes, imprescindible para que sea posible la mediación, su efectividad venga condicionada porque el menor realice un programa educativo en materia de educación sexual y educación para la igualdad. El papel del Equipo técnico será esencial, tal como se expone seguidamente, para asegurarse de que la víctima de alguno de esos delitos acepta participar en la mediación, una vez comprobado que está en condiciones para hacerlo.

Se prevén en el art. 19 LORPM tres supuestos distintos que pueden agruparse a la vista de la posición de la víctima; en los dos primeros, se requiere intervención de la víctima que, en un procedimiento de mediación con el infractor, tratará de alcanzar un acuerdo de conciliación o reparación, mientras que, el tercero, únicamente implica la posible aceptación y cumplimiento por el menor de la actividad educativa que le propone el Equipo Técnico en su informe, sin que se requiera ningún tipo de actuación de la víctima o perjudicado[45].

Tal como señala el art. 19.4 LOPJM, "una vez producida la conciliación o cumplidos los compromisos de reparación asumidos con la víctima o perjudicado por el delito o falta cometido, o cuando una u otros no pudieran llevarse a efecto por causas ajenas a la voluntad del menor; el Ministerio Fiscal dará por concluida la instrucción y solicitará del Juez el sobreseimiento y archivo de las actuaciones, con remisión de lo actuado"; no hace referencia el precepto transcrito a la posible oposición de la acusación particular a la petición de sobreseimiento del fiscal. Pese a que no existe una posición unánime en la jurisprudencia, la mayoritaria entiende

44. Habla el legislador de "medida accesoria" en un momento en que procederá, en su caso, un sobreseimiento porque ha habido una conciliación entre infractor o víctima o el cumplimiento de un compromiso de reparación que la víctima ha aceptado, pero no la imposición de ninguna medida.

45. *Vid.*, ÁLVAREZ RAMOS, F., "Mediación penal juvenil y otras soluciones extrajudiciales", *International e-Journal of Criminal Sciences*, Artículo 3, Número 2, 2008, http://www.ivac.ehu.es, p. 8.

que, pese a que, tras la reforma del art. 25 LORPM se reconoció a la víctima el derecho a personarse como acusación particular, reforzándose su papel en el proceso por la LO 8/2006, que modifica, entre otros, el art. 19 LORPM, "sigue siendo una facultad exclusiva del Ministerio Fiscal la de pedir el desistimiento, sin que en dicho trámite se otorgue ninguna intervención a la acusación particular, por lo que debemos concluir que, en estos casos, la petición de la acusación particular solicitando la continuación del procedimiento carece de relevancia. En consecuencia, el Juzgado de Menores, tal y como establece el art. 33.c) de la Ley de Responsabilidad Penal de los Menores, deberá proceder al archivo por sobreseimiento de las actuaciones cuando el Ministerio Fiscal solicite el desistimiento"[46].

A lo expuesto por la jurisprudencia, debe añadirse otra consecuencia que podría derivarse de la posible apertura de la audiencia al menor infractor por la oposición de la acusación particular al sobreseimiento del fiscal y que apoya este posicionamiento; a saber, si el menor, después de cumplir los acuerdos de conciliación o reparación alcanzados en el procedimiento de mediación o la actividad educativa a la que se hubiera comprometido, se ve sometido a una audiencia a instancias de la acusación, sería perjudicial para su propio desarrollo personal pero además, podría suponer una vulneración del principio *non bis in idem*[47].

1. SOBRESEIMIENTO POR CONCILIACIÓN O REPARACIÓN

La mediación con menores infractores tiene en nuestro ordenamiento jurídico un estricto carácter reglado, ya que el legislador no ha permitido que la víctima y el infractor puedan acudir a este mecanismo en cualquier momento y circunstancia, sino que está claramente delimitado tanto el momento en que puede tener lugar como los presupuestos que deben concurrir. De ahí los requisitos que se recogen en el apartado 1 del art. 19.1 LORP, que además de establecer límites en relación a la gravedad de los delitos, y la ausencia de violencia e intimidación graves en su comisión, no solo la condiciona a que exista conciliación o reparación entre autor y víctima, sino que determina, en el apartado segundo del mismo precepto cuándo se deben entender cumplidos cada una de esas situaciones.

46. AAP de Barcelona, de 15 de mayo de 2008 (JUR 2008, 204991). Igualmente, Igual: AAAP de Las Palmas, de 22 marzo de 2010 (JUR 2010, 419218); de Barcelona, de 4 de noviembre de 2009 (JUR 2010, 45352); de Segovia, de 12 de septiembre de 2009 (JUR 2009, 41962).

47. GARCÍA INGELMO, F. M.– "Ejercicio del principio de oportunidad en la jurisdicción de menores. Supuestos legales. Cuestiones prácticas y Directrices de la FGE…", *op. cit.*, p. 33.

En concreto, a efectos de poder sobreseer el expediente de reforma por conciliación, el art. 19.2 LORPM, entiende producida la misma "cuando el menor reconozca el daño causado y se disculpe ante la víctima, y ésta acepte sus disculpas" (art. 19.2 LORPM). De esta disposición se deduce que la conciliación requiere necesariamente la concurrencia de dos voluntades, la del menor infractor, que debe reconocer el daño causado y disculparse ante la víctima; y la de ésta, que debe aceptar dichas disculpas[48]. Con el objeto de no dejar en manos de la víctima la continuación de la causa, cuando el principio interés del menor aconseja la terminación del proceso sin necesidad de celebrar la audiencia, el apartado 4 del mismo art. 19 LORPM, entiende procedente igualmente el sobreseimiento si la conciliación "no pudiera llevarse a efecto por causas ajenas a la voluntad del menor"[49].

Por tanto, nada impide que el Fiscal pueda dar por concluida la instrucción y solicitar al Juez de Menores el sobreseimiento cuando el menor haya reconocido el daño causado y presentado sus disculpas a la víctima y, ante la negativa de ésta a aceptarlas, se comprometa a cumplir la actividad educativa que propone el Equipo Técnico en su informe[50]. A su vez, la falta de anuencia de la víctima a la petición de disculpas del infractor puede ser valorada por el Equipo Técnico a los efectos de proponer el sobreseimiento del expediente en interés del menor por entender que ya se ha expresado suficientemente el reproche al mismo a través de los trámites ya practicados o por considerar inadecuada cualquier intervención respecto del menor, dado el tiempo ya transcurrido desde la comisión de los hechos (art. 27.4 LORPM).

La segunda actuación que puede realizar el menor a fin de que se decrete el sobreseimiento del expediente de reforma es la reparación del

48. En este sentido, el AAP de Ciudad Real de 14 noviembre de 2008 (JUR 2009, 411871) entiende que no se han cumplido los requisitos de la mediación por conciliación porque las víctimas no habían considerado suficientes las disculpas y, por tanto, no se sienten reparadas; es más, las víctimas ni siquiera han sido citadas para ser escuchadas, acordándose el archivo a sus espaldas, no arbitrándose los mecanismos de conciliación previstos en el art. 19 LORPM.

49. En este sentido, en el AAP de Barcelona, de 15 de mayo de 2008 (JUR 2008, 204991), en relación a una situación de acoso escolar, concurriendo todos los requisitos del art. 19 LORPM pero sin que fuera posible la conciliación al negarse la víctima a aceptar las disculpas de la menor, a la vista del informe obrante en la causa elaborado por el Equipo Técnico, en los que se concluye que la valoración de la actitud mostrada por la menor es positiva y que la misma ha respetado la voluntad de la víctima de no participar en el programa de mediación, reiterando su compromiso de no repetir nuevos incidentes como el presente, se considera idónea la decisión del MF de archivar el expediente. En los mismos términos, AAAP de Málaga, de 13 de noviembre de 2020 (JUR 2022, 118877); Las Palmas, de 22 de marzo de 2010 (JUR 2010, 419218).

50. Apartado IV.5.2 Circular FGE 9/2011.

daño causado a la víctima o al perjudicado por el hecho delictivo. Y, a estos efectos, el art. 19.2 LORPM define esta reparación como "el compromiso asumido por el menor con la víctima o perjudicado de realizar determinadas acciones en beneficio de aquéllos o de la comunidad, seguido de su realización efectiva". Es decir, a diferencia de la conciliación, se trata aquí de proporcionar al ofendido o perjudicado una satisfacción de carácter material, de la que pueden beneficiarse ellos directamente, o bien la comunidad.

Para que se decrete el sobreseimiento del proceso, no basta, en principio, con el simple compromiso del menor de reparar, sino que se requiere además la realización efectiva de la actividad reparadora comprometida. Por ello, el Equipo Técnico debe mantener informado al fiscal de los compromisos adquiridos por el menor y de su grado de cumplimiento (art. 19.3 LORPM); y aquél sólo podrá dar por concluida la instrucción y solicitar del Juez el sobreseimiento una vez cumplidos los compromisos de reparación o cuando se constate que éstos no se pudieron llevar a efecto por causas ajenas a la voluntad del menor (art. 19.4 LORPM).

Debe tenerse en cuenta que, al igual que ocurre con la conciliación, la reparación implica un "compromiso asumido por el menor con la víctima o perjudicado" (art. 19.2 LORPM), y si ésta es menor de edad o incapaz, tal compromiso "habrá de ser asumido por el representante legal de la misma, con la aprobación del Juez de Menores" (art. 19.6 LORPM). Por tanto, la reparación también exige la concurrencia de las voluntades de los sujetos implicados[51].

En lo que respecta al contenido de la actividad reparadora que puede llevar a cabo el menor, el legislador se limita a disponer que podrá consistir en "determinadas acciones" en beneficio de la víctima o perjudicado o de la comunidad; por tanto, habrá de entenderse que tiene cabida cualquier tipo de actuación por parte del menor que tenga un efecto reparador para la víctima o perjudicado (vgr., sacar a pasear a una persona dependiente al cuidado de la víctima) o que se realice a favor de la comunidad (vgr., colaborar en las actividades de una ONG dedicada a la atención y cuidado de personas con discapacidad), correspondiendo al Equipo Técnico proponer en cada caso aquéllas que estime más adecuadas para la reeducación del menor (art. 27.3 LORPM).

51. Tal exigencia queda patente en la regulación que hace el art. 5.1 RD 1774/2004 de la mediación que a estos efectos debe llevar a cabo el Equipo Técnico, en la que se exige que ambas partes manifiesten previamente su disponibilidad a participar en este procedimiento y que, en su caso, quede constancia de los acuerdos de reparación adoptados.

Es importante destacar que reparación *ex* art. 19 LORPM es de carácter "penal y educativa", y por tanto no coincide con la reparación que integra el contenido de la responsabilidad civil previsto en los arts. 110 y 112 CP. Por eso, el propio art. 19.2 *in fine* señala que la misma se entiende "sin perjuicio del acuerdo al que hayan llegado las partes en relación con la responsabilidad civil". Esto significa que, en principio, dicha reparación no extingue la acción civil para obtener el resarcimiento de todos los daños y perjuicios causados por el hecho delictivo; por tanto, de prosperar el sobreseimiento, se podrá ejercitar ante la jurisdicción civil a través del proceso declarativo que corresponda por razón de la cuantía, salvo que las partes en el marco de la propia mediación hubieran acordado otra cosa[52].

En coherencia con la finalidad reeducadora de la reparación, se ha de buscar que el menor sea consciente del daño causado y acepte el acto reparador como adecuado y proporcionado. Por ello, la actividad reparadora que se le imponga al menor debe guardar en cada caso una cierta relación o conexión con el bien jurídico lesionado o puesto en peligro por el hecho delictivo cometido, así como una proporcionalidad con la gravedad de tal delito y la intensidad del daño causado por el mismo[53].

Como ya se ha adelantado, desde la reforma operada por la LO 10/2022, se condiciona el sobreseimiento por conciliación o reparación cuando se trata de la comisión por el menor de alguno de los delitos tipificados en los Capítulos I y II del Título VIII del Código Penal, o estén relacionados con la violencia de género, a la realización de una "medida accesoria de educación sexual y de educación para la igualdad".

La mediación será realizada por el Equipo Técnico que deberá seguir las pautas establecidas en el art. 5 RD 1774/2004. Siendo la voluntariedad uno de los principios esenciales de la mediación, es especialmente importante que, tal como ya se ha adelantado, ambas partes acepten su participación en la misma; para ello, el Equipo Técnico recabará primeramente la aceptación del menor y a continuación de sus representantes legales, para, posteriormente hacer lo mismo con la víctima, resultando necesario, si ésta es menor, también la anuencia de sus representantes legales. Si ambas partes muestran su conformidad a participar en el procedimiento de mediación, se concertará un encuentro por el Equipo Técnico para

52. *Vid*. apartado. VIII.5 Circular FGE 1/2007, de 23 de noviembre, *sobre criterios interpretativos tras la reforma de la legislación penal de menores de 2006*.

53. *Vid.* CALLEJO CARRIÓN, S., "El principio de oportunidad en la LO 5/2000, de 12 de enero…", *op. cit.*, p. 8; CRUZ MÁRQUEZ, B., "La mediación en la Ley Orgánica 52000, reguladora de la responsabilidad penal de los menores: conciliación y reparación del daño", Revista Electrónica de Ciencia Penal y Criminología, 2005, p. 9.

concretar el acuerdo de conciliación o reparación, salvo que no se considere conveniente reunir a las partes, en cuyo caso, las sesiones de mediación se realizarán de forma separada.

A efectos de evitar cualquier duda sobre una posible limitación del principio de presunción de inocencia, debe tenerse en cuenta que, cuando el menor acepta acudir a mediación, no se está propiamente reconociendo su participación en la comisión de los hechos delictivos, sino que únicamente está mostrando su disposición para alcanzar un acuerdo de conciliación o reparación con la víctima. Es decir, no se puede equiparar la conformidad del menor de iniciar un procedimiento de mediación con una confesión de los hechos objeto de acusación[54]; porque si así fuera, se estaría vulnerando el principio de presunción de inocencia. Además, la plena vigencia de este principio, impedirá que el Juez de Menores pueda tener en cuenta en el momento de su sentencia su conocimiento sobre la existencia de una propuesta al menor de participación en un procedimiento de mediación o su efectiva participación en el mismo que terminó sin acuerdo. Aunque esta segunda situación suele ser poco habitual pues en gran parte de las ocasiones, si no se alcanza acuerdo de conciliación o reparación, el fiscal suele instar el sobreseimiento por realización de una actividad educativa a propuesta del Equipo Técnico. Normalmente, suelen ser supuestos en que la víctima no acepta el contenido del acuerdo reparador o las disculpas que se ofrecen por el menor, que han sido supervisados por el Equipo Técnico que dirige el procedimiento de mediación.

2. SOBRESEIMIENTO POR REALIZACIÓN DE ACTIVIDAD EDUCATIVA A PROPUESTA DEL EQUIPO TÉCNICO

Uno de los posibles contenidos del informe sobre la situación psicológica, educativa y familiar del menor, así como de su entorno social y de cualquier otra circunstancia que pueda ser relevante que debe realizar el Equipo Técnico a requerimiento del fiscal durante la fase de instrucción, es la propuesta de una actividad educativa que debe ser realizada por el menor.

Cumpliéndose los requisitos previstos en el art. 19.1 LORPM, será posible acordar el sobreseimiento en aquellos casos en que el menor se comprometa a realizar la actividad educativa propuesta el Equipo Técnico.

54. En este sentido, ARANDA JURADO, M., La mediación penal juvenil en España, Tirant Lo Blanch, Valencia, 2022, PP. 203 y ss.; CRUZ MÁRQUEZ, B., "La mediación en la Ley Orgánica 52000, reguladora de la responsabilidad penal de los menores: conciliación y reparación del daño",…, *op. cit.*, pp. 8 y 9, Aranda Jurado. pp. 203 y ss.

No especifica el legislador qué se entiende por "actividad educativa"; es más, ni siquiera en la rúbrica del art. 19 LORPM se alude a que el sobreseimiento no sólo procede por reparación o conciliación sino también por compromiso del menor a realizar la actividad educativa que propone el Equipo Técnico. Llama la atención que frente al detalle con el que se regula qué se entiende por conciliación o reparación, a la actividad educativa se le menciona únicamente en el apartado 5 del citado precepto para alertar de que si el menor "no cumpliera la reparación o la actividad educativa acordada, el Ministerio Fiscal continuará la tramitación del expediente".

Para determinar qué se debe entender por "actividad educativa" se debe acudir al art. 7.1.l) LORPM, donde al definir las medidas definitivas, se alude a la realización de tareas socio-educativas que supondrá someter al menor infractor "sin internamiento ni libertad vigilada, a actividades específicas de contenido educativo encaminadas a facilitarle el desarrollo de su competencia social"[55]. Más clara en relación al contenido es la Exposición de Motivos LORPM cuando señala que "La realización de tareas socio-educativas consiste en que el menor lleve a cabo actividades específicas de contenido educativo que faciliten su reinserción social. Puede ser una medida de carácter autónomo o formar parte de otra más compleja. Empleada de modo autónomo, pretende satisfacer necesidades concretas del menor percibidas como limitadoras de su desarrollo integral. Puede suponer la asistencia y participación del menor a un programa ya existente en la comunidad, o bien a uno creado 'ad hoc' por los profesionales encargados de ejecutar la medida. Como ejemplos de tareas socio-educativas, se pueden mencionar las siguientes: asistir a un taller ocupacional, a un aula de educación compensatoria o a un curso de preparación para el empleo; participar en actividades estructuradas de animación sociocultural, asistir a talleres de aprendizaje para la competencia social, etc".

No obstante, no se debe correr el riesgo de asimilar de forma automática la actividad educativa que se puede proponer por el Equipo Técnico con una de las medidas previstas en el art. 7 LORPM que, como es bien sabido, únicamente pueden imponerse en la sentencia condenatoria, una vez practicada la prueba en la audiencia. Por tanto, aunque pueda tomarse como referencia el art. 7.1.l LOPJM, el contenido y la finalidad de la actividad educativa será especificada por el Equipo Técnico en su informe y, por supuesto, estará en relación con el delito cometido por el menor y siempre teniendo presentes sus necesidades educativas a la vista de sus circunstancias personales y sociales.

55. Apartado III Exposición de Motivos LORPM.

Finalmente, no deja de ser llamativo que, ante la comisión por el menor de alguno de los delitos tipificados en los Capítulos I y II del Título VIII del Código Penal, la LO 10/2022 condicione la efectividad del sobreseimiento por conciliación o reparación a la realización por el menor de "la medida accesoria de educación sexual y de educación para la igualdad", pero no haga alusión alguna a esta misma exigencia cuando se trate de archivo por actividad educativa propuesta por Equipo técnico.

3. SOBRESEIMIENTO POR CONCILIACIÓN, REPARACIÓN O ACTIVIDAD EDUCATIVA COMO RESPUESTA ANTE LA CIBERDELINCUENCIA JUVENIL

A la vista de los requisitos expuestos en los apartados anteriores, estas medidas extrajudiciales resultan muy convenientes ante las infracciones más habituales cometidas por los menores en el ciberespacio; la propia FGE las considera como la vía natural para la resolución de problemas sociales como el acoso escolar o la utilización de internet y las nuevas tecnologías para la comisión o difusión de delitos[56].

Más en concreto, y teniendo en cuenta que en el momento de la comisión de los ciberdelitos, gran parte de los menores no son conscientes de que están realizando una actividad delictiva y que el hecho mismo de su comisión es una muestra de un déficit educativo en el manejo de internet y las redes sociales y en materia de sexualidad, el sobreseimiento por conciliación o reparación o por realización de la actividad educativa propuesta por el Equipo Técnico pueden ofrecer una respuesta adecuada ante este tipo de criminalidad, soslayando el efecto estigmatizador que para el menor supone la celebración de la audiencia y reforzando además la finalidad educativa con el objetivo final de evitar la reincidencia.

Ahora bien, de los dos supuestos de sobreseimiento previstos en el art. 19 LORPM, el que tiene como base la mediación por conciliación o reparación, aparece como el instrumento más idóneo para responder ante la ciberdelincuencia juvenil, porque al componente educativo, se une la atención a la víctima, que va a encontrar también una reparación ante al daño que le ha provocado la acción delictiva.

Así, en los supuestos de *ciberbullying*, *stalking*, *sexting* o difusión de imágenes vejatorias o degradantes o incluso las amenazas o coacciones, la mediación va a facilitar que los infractores se enfrenten al daño causado por la acción delictiva y asuman la responsabilidad de sus actos. Como

56. Apartado IV.5.2 Circular FGE 9/2011.

se expuso, en un número elevado de casos, el menor infractor no es consciente de que ha cometido un delito y, en consecuencia, desconoce las consecuencias perjudiciales para la víctima derivadas de sus acciones. Por eso, es tan conveniente la mediación pues va a suponer no sólo la toma de conciencia de la infracción cometida y sus efectos, sino que, además, implica asumir sus actos y responder por lo que se ha hecho, reparando el daño causado. El componente educativo derivado de este ejercicio de asunción de responsabilidad por el menor es evidente, en cuanto una de las premisas de todo proceso educativo es la responsabilización individual sobre sus propios actos, que se presenta como un factor esencial en el desarrollo de la propia identidad. La responsabilidad individual por la comisión del delito implica confrontar al menor con su acción, haciéndole comprender el daño ocasionado a la víctima, a la sociedad en general y a sí mismo[57].

En cuanto a las víctimas, se les ofrece un espacio en el que poder plantear los miedos e inseguridades que les ha provocado el delito, permitiéndoles que obtengan una reparación del daño causado no sólo material, sino también moral y psicológica que en el proceso penal quedaba olvidada. Este protagonismo de la víctima tiene enorme importancia en el proceso penal de menores donde, inicialmente, se consideró que su intervención en el proceso no encajaba bien con el interés superior del menor en cuando principio inspirador de todo el sistema de justicia juvenil. La inclusión de la mediación como solución extrajudicial del conflicto derivado del delito cometido por un menor de edad permite equilibrar ese interés del menor con la atención a las necesidades e intereses de la víctima. Por ese protagonismo que se reconoce a la víctima, que va a ser tenida en cuenta y escuchada, la mediación, a diferencia del desistimiento, suele tener una gran aceptación social.

No obstante, las ventajas anteriores sólo serán posibles si tanto el menor infractor como la víctima se encuentran en la situación psicológica y física que requiere todo procedimiento mediador, de ahí el papel del Equipo Técnico, que deberá garantizar la igualdad entre las partes en el procedimiento de mediación y que ambas han tenido la información suficiente para prestar su consentimiento para participar en el mismo, evitando cualquier atisbo de victimización secundaria.

Para que la mediación cumpla plenamente sus finalidades educativas, reparadoras para la víctima y de prevención de la reincidencia, el Equipo Técnico deberá poner fin al procedimiento si el menor infractor no

57. GONZÁLEZ PILLADO, E., "La mediación como manifestación del principio de oportunidad en la Ley de Responsabilidad Penal de Menores", en "Mediación con menores infractores en España y los países de su entorno" (Ed. Tirant Lo Blanch ISBN 978-84-9004-717-0), Valencia, 2012, p. 84.

exterioriza de una forma clara su intención de no volver a cometer actos del mismo tipo y si la víctima no se encuentra en condiciones de tomar parte del procedimiento mediador. Especial atención deberá prestarse a la víctima cuando es menor de edad, de tal manera que tanto en el desarrollo del procedimiento como en el momento de adoptar cualquier decisión que le afecte habrá de valorarse y considerar como primordial su interés, tal como prevé de forma general el art. 2 LO 1/1996, de 15 de enero, de protección jurídica del menor.

A la vista de las grandes ventajas que la mediación aporta a víctima y victimario, el sobreseimiento del expediente por el compromiso del menor a realizar la actividad educativa propuesta por el Equipo Técnico, deberá utilizarse solo en aquellos casos en que, siendo de interés evitar la celebración de la audiencia, la mediación no resulta conveniente, o cuando ambas partes o una de ellas no acepta participar en un procedimiento de mediación o no se encuentra en una situación personal que permita esa participación.

Pese a las grandes ventajas de la mediación por conciliación o reparación, según los datos publicados por la FGE del año 2020, el número de expedientes archivados conforme al art. 19 LORPM sigue una línea descendente, representando en 2020 un 14,72% del total de expedientes abiertos, que apenas supera el 14,22% del 2019, y resulta inferior al 16,1 2% del 2018 y al 16,56% del 2017. Tal cifra porcentual sigue por debajo de la horquilla de los siete años precedentes (15-18%)[58].

Es necesaria una apuesta clara por la mediación penal juvenil, con más equipos técnicos especializados en materia de mediación que, de forma exclusiva se dediquen a esta función, así como un aumento de la inversión para los equipos de medio abierto. Además, deberán evitarse dos situaciones que se repiten en la práctica y que llevan a desechar esta medida desjudicializadora; de un lado, la exclusión prácticamente automática de la medición cuando se trate de un menor reincidente. De otro lado, la vinculación de la posibilidad de mediación al pago de la responsabilidad civil[59], pues se trata de cuestiones distintas y, en muchas ocasiones, puede

58. Apartado 6.2.3.3.2. Capítulo III. *Memoria FGE 2020.*

59. Esto no quita para que, tal como se apunta en la Circular FGE 9/2011, en aquellos casos en que consta el abono efectivo de la responsabilidad civil o existe una voluntad clara y real de llevarla a cabo, los fiscales tendrán este elemento muy en cuenta a efectos de impulsar las soluciones extrajudiciales del art. 19 LORPM. Aunque, siempre teniendo presente que la satisfacción de las responsabilidades civiles, aun siendo un factor muy positivo que el Fiscal puede tener presente, no es el objetivo final pretendido con las soluciones extrajudiciales del art. 19. *Vid.* Dictamen FGE 1/2014, *sobre pago de indemnizaciones y consignación* de cantidades en las soluciones extrajudiciales.

dar lugar a un trato discriminatorio entre menores por su situación social y económica[60].

Además, transcurridos ya 20 años desde la entrada en vigor de la LORPM, es necesario replantearse la regulación de la mediación penal juvenil si queremos apostar por su efectividad, en cuando la misma tiene un gran hándicap derivado de su limitado ámbito de aplicación a los delitos menos graves o leves cometidos sin violencia o intimidación graves[61]; además, tampoco parece conveniente que las únicas posibilidades de acuerdo se reduzcan a la conciliación o reparación entre víctima y victimario.

Así, sería muy conveniente plantearse la modificación del art. 19 LORPM en dos aspectos concretos; de un lado, la eliminación de los límites para la utilización de la mediación penal juvenil en relación al delito cometido, permitiéndose siempre que, a la vista de las circunstancias concurrentes, el fiscal y el Equipo Técnico así lo consideren, y requiriéndose, por supuesto, que víctima y victimario acepten voluntariamente participar en el procedimiento. De otro lado, el acuerdo de mediación no puede verse reducido a la posibilidad de una conciliación o un compromiso de reparación, sino que las finalidades educativa y reparadora del procedimiento junto con la flexibilidad característica del mismo deben permitir una amplitud y variedad en el contenido del acuerdo en el sentido que mejor se considere por víctima y victimario, siempre con el apoyo del Equipo Técnico, quien, en su caso, podrá proponer de forma complementaria una actividad socio-educativa que trate de cubrir las carencias que han llevado al menor a delinquir[62].

En todo caso, se insiste, la conveniencia de la mediación debería estar directamente conectada con el interés del menor en la búsqueda de la solución al conflicto derivado del delito que sea más beneficiosa, sin condicionantes derivados del tipo de delito cometido ni de su gravedad, y buscando además un equilibrio con las necesidades e intereses de la víctima.

60. La propia FGE en su *Memoria de 2018* (apartado 6.2.3.3.2. Capítulo III) alude a la situación que se produce en Guadalajara donde, en los casos de menores tutelados expedientados, aunque éstos reconozcan los hechos y asuman los compromisos del art. 19 LORPM, no se llevan a efecto, al oponerse sistemáticamente la Junta de Castilla La Mancha al pago de las indemnizaciones.

61. Especialmente crítica con el ámbito de aplicación de la mediación se muestra CRUZ MÁRQUEZ ("La mediación en la Ley Orgánica 52000, reguladora de la responsabilidad penal de los menores: conciliación y reparación del daño…", *op. cit.*, p. 18), al vedar las posibilidades de sobreseimiento por conciliación o reparación en supuestos de delitos de mediana gravedad.

62. Por ejemplo, un curso de manejo de redes sociales o de educación sexual o de autocontrol de impulsos.

Además, habrá de valorarse la necesidad de introducir en la LORPM otros mecanismos de justicia restaurativa que puedan ser utilizados para ajustar más la respuesta a las necesidades de víctima y victimario pues la mediación no siempre es el instrumento capaz de cubrir todos los intereses en juego. Así, en la línea del Anteproyecto de LECrim de 2020, que no regula la mediación penal, sino que dedica el Capítulo III del Título IV del Libro I, a la justicia restaurativa, dejando abierta la posibilidad de utilizar aquel mecanismo restaurativo que resulte más conveniente[63].

Una regulación general de la justicia restaurativa en el ámbito de la justicia juvenil permitiría, por ejemplo, la utilización de los círculos, en cuanto procedimiento de estilo mediatorio en el que, además del infractor y la víctima principal, intervienen otras personas, y que pueden ser muy útiles en el caso del *ciberbullying*, que facilitaría la intervención, involucrándolos en la resolución del conflicto, no sólo de infractor y víctima sino de todos aquellos que de forma directa o indirecta se han visto involucrados en el acoso, como pueden ser otros compañeros del colegio o miembros del profesorado.

63. *Vid*. OTERO OTERO, B., "Víctima y justicia restaurativa en la justicia de menores", en *La víctima en el proceso penal de menores. Tratamiento procesal e intervención socioeducativa* (dir. Pillado González), Dykinson, Madrid, 2021, pp. 160 y ss.

Capítulo 18

La prueba de la violencia de género digital en el proceso penal de menores[1]

Pablo Grande Seara

Profesor Titular de Derecho Procesal
Universidad de Vigo

I. INTRODUCCIÓN

La llamada violencia de género digital o ciberviolencia de género se puede definir como la violencia psicológica ejercida sobre la mujer por quien sea o haya sido su cónyuge o pareja de hecho, aún sin convivencia, a través de cualquier medio tecnológico o digital, mediante conductas en el plano virtual consistentes en injurias, coacciones, amenazas, humillaciones o vejaciones, exigencia de obediencia o sumisión, o limitaciones de su ámbito de libertad[2].

1. Este trabajo ha sido elaborado en el marco del proyecto de investigación "Respuesta jurídica y socioeducativa a la violencia de género ejercida por menores. Protección de la víctima e intervención con el menor agresor", subvencionado por el Ministerio de Ciencia e Innovación, Proyectos de I+D+I" dentro de los Programas Estatales de Generación de Conocimiento y Fortalecimiento Científico y Tecnológico del Sistema de I+D+I y de I+D+I orientada a los Retos de la Sociedad en la convocatoria de 2019, (Ref. PID2019-106700RB-I00).

2. La DELEGACIÓN DEL GOBIERNO CONTRA LA VIOLENCIA DE GÉNERO, (https://violenciagenero.igualdad.gob.es/informacionUtil/comoDetectarla/VG_Digital/home.htm), destaca diez signos que podrían indicar que se está produciendo violencia digital: "acosar o controlar a tu pareja usando el móvil; interferir en relaciones de tu pareja en Internet con otras personas; espiar el móvil de tu pareja; censurar fotos que tu pareja publica y comparte en redes sociales; controlar lo que hace tu pareja en las redes sociales; exigir a tu pareja que demuestre dónde está con su geolocalización; obligar a tu pareja a que te envíe imágenes íntimas; comprometer a tu pareja para que te facilite sus claves personales; obligar a tu pareja a que te muestre un chat con otra persona; mostrar enfado por no tener siempre una respuesta inmediata online".

Este tipo de violencia de género es la más común en el caso de los jóvenes y adolescentes, incluso a veces sin ser conscientes de ello; e incluye, entre otras, las siguientes conductas:

- *Haching* o intrusismo informático, es decir, el espionaje dentro de la pareja. Implica acceder al teléfono móvil u otro dispositivo digital de la pareja para conocer el contenido o los destinatarios de sus conversaciones o mensajes, ejerciendo así un control sobre ella.
- *Sexting*, que consiste en la difusión de imágenes (fotos o vídeos) de carácter erótico o sexual, tomadas por el agresor o grabadas por la propia víctima, para dañar el honor o la imagen de ésta.
- *Sextorsión* o extorsión sexual, que consiste en el chantaje a la víctima para que realice una determinada acción, bajo amenaza de publicar o compartir imágenes íntimas que el extorsionador tiene de ella.
- *Ciberstalking,* que es el acoso a través de medios telemáticos o redes sociales. El acosador, de forma insistente y reiterada, e incluso intimidatoria, intenta establecer contacto telemático con la víctima contra su voluntad, limitando así su capacidad de obrar o generándole sentimiento de inseguridad.
- *Ciberbullying*, que supone una situación de hostigamiento, abuso y vejación a la víctima, de forma sostenida y repetida a lo largo del tiempo. Puede adoptar formas muy heterogéneas, como, por ejemplo, enviar mensajes amenazantes a la víctima; crear un perfil falso de la víctima a través del que demanda contactos sexuales; seguir a la víctima en lugares de internet a los que accede habitualmente; dar de alta el mail de la víctima en determinados lugares de internet para que reciba spam; difundir rumores sobre la conducta de la víctima para que otras personas le acosen; etc.

Según se hace constar por el OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD, en su informe *Violencia digital de género: una realidad invisible*, el primer problema a la hora de analizar y abordar esta violencia de género digital en España, y en la UE, es la escasez de estadísticas, por lo que, en consecuencia, se sabe muy poco sobre el porcentaje real de las víctimas y de la prevalencia de los daños causados. Y añade que esta escasez de estadísticas "deriva de la dificultad de medir y cuantificar un fenómeno tan complejo, principalmente porque en la mayoría de los países no están tipificados como delito todas las formas de ejercer violencia digital contra las mujeres, de ahí que los datos policiales o de los organismos judiciales sean muy limitados"[3].

3. *Vid.*, OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD, *Violencia digital de género: una realidad invisible*, https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2022/220429_i_InformeONTSI.pdf, p. 8.

Con todo, en este informe se reflejan algunos datos que ponen de manifiesto la dimensión del problema entre las jóvenes. Se destaca que la edad es un factor determinante que incrementa las posibilidades de experimentar acoso en internet porque las más jóvenes también son las que más utilizan los servicios digitales. Así se puede constatar en los siguientes datos: más de un 25% de las mujeres entre 16 y 25 años en España han recibido insinuaciones no apropiadas a través de redes; más del 20% de las jóvenes entre 16 y 20 años ha recibido correos electrónicos, mensajes de texto o fotografías sexualmente explícitas que les hicieron sentirse ofendidas, humilladas o intimidadas; y, en menos de una década, se han multiplicado por cinco en España los delitos de contacto mediante tecnología con menores de 16 años con fines sexuales. Además, de las niñas y jóvenes que han sufrido acoso online, el 42% mostraron estrés emocional, baja autoestima y pérdida de confianza; el 24% se sintieron inseguras físicamente; y el 19% tuvo problemas con las amistades y la familia, y el 18%, en el colegio o instituto[4].

Como se puede comprender, estas conductas delictivas que integran la violencia de género digital se pueden cometer y, en su caso, tratar de probar, utilizando distintos medios o sistemas de comunicación electrónica, es decir, distintas tecnologías de la información y la comunicación (TIC´s), siendo los más comunes el correo electrónico, los mensajes SMS o multimedia (MMS), las aplicaciones de mensajería instantánea, bidireccional o multidireccional (Whatsapp, Telegram, Line,…), o las plataformas de redes sociales (Facebook, Instagram, Twiter, Youtube, Tiktok,…).

Cada una de estas tecnologías de comunicación presenta características técnicas distintas, lo que, por supuesto, tendrá consecuencias a efectos de su utilización como fuente de prueba en un proceso penal, especialmente, en lo relativo a su valoración probatoria en el caso de que la parte contraria cuestione la autenticidad de su autoría o la integridad de su contenido. Así, por ejemplo, los mensajes de Whatsapp no se guardan en un servidor del proveedor del servicio, sino únicamente en los terminales de emisión y recepción, por lo que no permite solicitar a aquel que certifique el contenido de los mensajes enviados o recibidos para su cotejo con los aportados al proceso; lo que sí es posible en el caso de la comunicación a través de redes sociales, ya que los contenidos que se suben a la red quedan almacenados en servidores de los administradores de la red social durante un tiempo[5].

4. *Vid*., OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD, *Violencia digital de género…, op. cit*., pp. 9 a 13.
5. *Vid*., FISCALÍA GENERAL DEL ESTADO, *Dictamen 1/2016, sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportados al proceso penal como*

Pero, a fin de delimitar y centrar más el tema de este trabajo, conviene destacar también que, precisamente, por sus características técnicas particulares, el uso de estas tecnologías de la comunicación se ha ido "especializando" en función del tipo de relaciones interpersonales para las que se utilizan y del perfil de usuarios más habituales. Buena muestra de ello es que, por ejemplo, el correo electrónico está quedando cada vez más relegado a un tipo de comunicación que podemos calificar como más profesional o formal; mientras que las aplicaciones de mensajería instantánea y las plataformas de redes sociales (en parte, por ser más fácilmente accesibles a través de un *smartphone*) se utilizan para las relaciones de tipo más personal e informal[6], y, en particular, entre los usuarios más jóvenes. Por ello, son estos últimos los sistemas de comunicación más propicios y habituales para la comisión de este tipo de violencia de género digital que se puede investigar y enjuiciar en el proceso penal de menores.

Por esta razón, en este trabajo, me centraré en la problemática procesal que suscita el uso en el proceso penal de estas dos fuentes de prueba: los mensajes (de texto, voz, imagen o vídeo) emitidos y recibidos a través de aplicaciones de mensajería instantánea y los mensajes o comunicaciones transmitidos a través de plataformas de redes sociales. Y tal problemática afecta, en mayor o menor medida, a lo que podemos llamar las "tres fases de la prueba electrónica o digital", a saber, la licitud de la obtención de la fuente de prueba, el medio de prueba a través del cual se pueden aportar o incorporar al proceso estas fuentes de prueba digitales, y, finalmente, la valoración probatoria de estas fuentes de prueba, en particular, en el caso de que la contraparte la impugne por cuestionar la autoría (autenticidad) o integridad (contenido) de la misma.

II. LICITUD DE LA OBTENCIÓN DE LA FUENTE DE PRUEBA DIGITAL

Como se comprenderá, las dudas que se pueden suscitar sobre la licitud en el modo de acceso y obtención de las fuentes de prueba electrónicas o digitales, y su consiguiente validez o no como fuente de prueba en un proceso penal, se refieren, básicamente, a las fuentes de prueba que hayan sido obtenidas y aportadas al proceso por las propias partes. Por

---

medio *de prueba de comunicaciones electrónicas* http://milansabogados.com/wp-content/uploads/2018/05/Dictamen-n%C2%BA-1-2016-sobre-el-valor-probatorio-de-las-capturas-de-pantallas.-Unidad-Criminalidad-Informa%CC%81tica.pdf.

6. *Vid.*, FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías", *Revista General de Derecho Procesal,* 44 (2018), p. 17.

lo general, no se plantean tales cuestiones de licitud cuando se trata de evidencias digitales obtenidas como consecuencia de una intervención policial acordada en el marco de un proceso penal, siempre que ésta se desarrolle conforme a lo previsto legalmente (arts. 588 bis a) a 588 ter m)[7]; y arts. 588 sexies a) a 588 octies LECrim[8]). Además, teniendo en cuenta que, normalmente, el tipo de delitos a los que nos estamos refiriendo son de carácter semipúblico, la presentación de denuncia por la víctima dará lugar con cierta frecuencia a la práctica de tales diligencias policiales de investigación tecnológica, sin perjuicio de la colaboración o facilidades que pueda proporcionar ésta a tal fin, por lo que tampoco será muy habitual que la parte contraria pueda impugnar con fundamento la licitud de estas fuentes de prueba.

En cualquier caso, a la hora de analizar la licitud de la obtención por las partes de los mensajes y comunicaciones electrónicas y su validez como fuente de prueba a efectos de acreditar conductas de violencia de género digital en un proceso penal, debemos partir de cuáles son los derechos fundamentales que se pueden ver afectados y hasta qué punto admiten limitaciones. Tales derechos son el derecho al secreto de las comunicaciones privadas (art. 18.3 CE) y/o el derecho a la intimidad personal (art. 18.1 CE)[9].

El derecho al secreto de las comunicaciones privadas protege el proceso de comunicación frente a cualquier intromisión ajena, tanto por parte de autoridades públicas como de particulares, y alcanza a cualquier forma y canal de comunicación. Este derecho protege el proceso de comunicación, no sólo el contenido de la misma (es decir, los mensajes que se transmiten), y, por tanto, impide que un tercero pueda interceptar cualquier dato o elemento privado de la comunicación, como son los datos identificativos

7. En ellos se regulan las siguientes actuaciones: Disposiciones comunes a todas las diligencias de investigación tecnológicas (arts. 588 bis a) a 588 bis k) LEcrim); la interceptación de comunicaciones telefónicas y telemáticas (arts. 588 ter a) a 588 ter i) LECrim); la incorporación al proceso de datos electrónicos de tráfico (arts. 588 ter j) LECrim); y el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad (arts. 588 ter k) a 588 ter m) LECrim).

8. En ellos se regulan el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies a) a 588 sexies c) LECrim); los registros remotos sobre equipos informáticos (arts. 588 septies a) a 588 septies c) LECrim); y las medidas de aseguramiento (art. 588 octies LECrim).

9. ARMENTA DEU, T., "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, Whatsapp, redes sociales): entre la insuficiencia y la incertidumbre", *IDP, Revista de Internet, Derecho y Política*, núm. 27, septiembre, 2018, pp. 71 y 72; RICHARD GONZÁLEZ, M., "Valor como prueba de los mensajes y comunicaciones electrónicas en los procesos de familia", en (Dir., Picó i Junoy, J y Abell Lluch, X.) *Problemática actual de los procesos de familia. Especial atención a la prueba*, Bosch, Barcelona, 2018, pp. 219 a 228.

de los intervinientes en la comunicación, la ubicación de estos, el tiempo y duración de la comunicación, o el tipo y contenido de la misma.

Esto significa que, por ejemplo, se vulnere este derecho al secreto de las comunicaciones por el mero hecho de que un tercero acceda a la cuenta de correo o a la aplicación de mensajería instantánea sin el consentimiento de su titular, aunque no pueda acceder o llegar a conocer el contenido de los mensajes[10]. En cambio, no se vulnera este derecho cuando el que utiliza o aporta al proceso datos de una comunicación es uno de los intervinientes en la misma; y ello con independencia del número de interlocutores que hayan participado en ella (por ejemplo, mensajes recibidos en un grupo de Whatsapp). La utilización o difusión de esos mensajes u otros datos de la comunicación por uno de los interlocutores podrá afectar, en su caso, al derecho a la intimidad, pero no al secreto de las comunicaciones.

A su vez, el derecho a la intimidad supone la existencia de un ámbito propio y reservado de una persona frente a la acción y el conocimiento de los demás. Pero es éste un derecho flexible, ya que su contenido y alcance se puede modular en función de la voluntad o conducta de su titular y de las circunstancias concurrentes en cada caso. Es decir, corresponde a cada persona acotar el ámbito de intimidad personal y familiar que quiere reservar al conocimiento ajeno. Por ello, el consentimiento (expreso o tácito) del titular permite la inmisión lícita en dicho ámbito.

Esto tiene particular importancia en el contexto familiar o de pareja, ya que las especiales relaciones de confianza que, normalmente, existen en este ámbito, al menos mientras no hay conflicto, así como el debido ejercicio de los derechos y deberes paternofiliales, hace que los límites de este derecho a la intimidad aparezcan a veces muy difuminados. Por ejemplo, como veremos, se entiende que no se vulnera este derecho a la intimidad con el uso por un miembro de la pareja de aquellos dispositivos o aplicaciones de comunicación que comparten de mutuo acuerdo (aunque ninguno de ellos podrá hacer un uso ilícito de los contenidos o de la información de la aplicación que perjudique a los demás usuarios). De igual modo, la jurisprudencia ha admitido como lícito el acceso por parte de un progenitor a los mensajes albergados en el teléfono móvil de su hijo menor de edad cuya custodia comparte, por entender que la vigilancia del uso que hace éste de las redes sociales entra dentro de sus obligaciones inherentes a la patria potestad previstas en el art. 154 CC[11].

Por tanto, no cabe duda de que estos derechos al secreto de las comunicaciones privadas y a la intimidad personal también rigen y han de ser

10. SAP de Illes Balears 431/2017, de 5 de septiembre (JUR 2017, 276317).
11. AAP de Pontevedra 893/2017, de 25 de octubre (JUR 2017, 308428)

respetados en el ámbito familiar o de pareja. Pero el contenido y efectividad de tales derechos se puede ver atenuado o difuminado por la "auto-renuncia" de sus titulares como consecuencia de la relación de confianza que suele existir en este contexto. Por ello, a efectos de determinar la licitud del acceso y obtención de mensajes y comunicaciones electrónicas para su aportación como fuente de prueba en un proceso penal por violencia de género digital, debemos distinguir diversos supuestos, según que la parte que los aporta haya sido o no emisora o receptora de los mismos[12].

1. OBTENCIÓN Y APORTACIÓN AL PROCESO DE COMUNICACIONES ELECTRÓNICAS RECIBIDAS POR LA PARTE PROCESAL

La obtención y aportación al proceso de mensajes y comunicaciones electrónicas recibidas por la propia parte no plantea, *a priori*, problemas de licitud, ya que, como se indicó, cualquiera de los interlocutores en la comunicación puede obtener y aportar lícitamente al proceso estos mensajes sin que se pueda entender vulnerado el derecho al secreto de las comunicaciones; y ello, aunque no sea el destinatario exclusivo de los mensajes en cuestión. Por ejemplo, tratándose de un mensaje recibido en un grupo de WhatsApp o a través de un correo electrónico enviado a un colectivo, cualquiera de los receptores puede aportar lícitamente al proceso dicho mensaje.

En este sentido, es clara la SAP de Asturias 280/2018, de 29 de junio, al señalar que "quien graba una conversación de otro atenta contra el derecho al secreto de las comunicaciones; pero quien graba una conversación con otro, no incurre en esta infracción, porque no hay secreto para aquel a quien la conversación se dirige"[13]. Por ello, concluye que no existe prueba ilícita cuando una parte aporta al proceso archivos de audio de conversaciones mantenidas con terceros en calidad de interlocutor.

Es más, sería lícita incluso la obtención y aportación de los mensajes al proceso por la persona titular del dispositivo electrónico en el que se han recibido tales mensajes, aunque no fuese ella directamente la destinataria de los mismos. Por ejemplo, cuando en la comunicación se utiliza el dispositivo o aplicación de mensajería de otra persona que luego encuentra dichos mensajes, o cuando, por error, se envían al destinatario

12. *Vid.*, RICHARD GONZÁLEZ, M., "Valor como prueba de los mensajes y comunicaciones electrónicas…", *op. cit.*, pp. 228 a 232.
13. SAP de Asturias 280/2018, de 29 de junio (JUR 2018, 240840).

equivocado. En este sentido, declara la SAP de Madrid 702/2015, de 24 de noviembre, que no concurre causa de nulidad porque los mensajes "han sido aportados al proceso por la propia persona titular del dispositivo electrónico que ha recibido los mensajes"[14].

En definitiva, la aportación al proceso como fuente de prueba de los mensajes y comunicaciones electrónicas que ha recibido la propia parte que los aporta es lícita ya que no vulnera el derecho al secreto de la comunicación, en tanto que la parte es interlocutora en la comunicación o titular del dispositivo o aplicación desde el que se transmite o recibe el mensaje. Y, en principio, la utilización de estas comunicaciones como fuente de prueba en un proceso, tampoco vulnera el derecho a la intimidad, siempre que el contenido de las mismas sea útil y pertinente (necesario) para probar hechos relevantes en el proceso[15].

2. OBTENCIÓN Y APORTACIÓN AL PROCESO DE COMUNICACIONES ELECTRÓNICAS TRANSMITIDAS O RECIBIDAS POR LA PARTE CONTRARIA O POR UN TERCERO

La licitud de la obtención y aportación al proceso como fuente de prueba de comunicaciones electrónicas transmitidas o recibidas por la parte contraria o un tercero queda supeditada a que se hayan respetado el derecho al secreto de las comunicaciones y el derecho a la intimidad de los interlocutores. Pero esto no significa que, en ningún caso, una parte pueda obtener y aportar lícitamente al proceso mensajes o comunicaciones de los que no es interlocutora. A este respecto, la doctrina y la jurisprudencia ha hecho algunas matizaciones

Por supuesto, no es admisible ningún tipo de interceptación por la parte de las comunicaciones de otra persona (sea la otra parte o un tercero) para poder aportarlas al proceso como fuente de prueba[16]; y ello,

14. SAP de Madrid 702/2015, de 24 de noviembre (ARP 2015, 1313).

15. *Vid.*, RICHARD GONZÁLEZ, M., "Valor como prueba de los mensajes y comunicaciones electrónicas…", *op. cit.*, p. 231.

16. *Vid.*, SAP de Asturias 39/2017, de 15 de febrero (ARP 2017, 412). Como señala CUAIRÁN ("La aportación de WhatsApp como medio de prueba en el procedimiento penal", *Diario La Ley*, n.º 9219, Sección Tribuna, 15 de junio de 2018 (La Ley 5337/2018), p. 2), el acceso no consentido a conversaciones de terceros podría vulnerar el derecho fundamental a la intimidad y/o al secreto de las comunicaciones, lo que conllevaría que, además de ser considerada como prueba ilícita, dicha conducta fuera constitutiva de un delito de descubrimiento y revelación de secretos previsto y penado en el art. 197 CP. En el mismo sentido, DELGADO MARTÍN, J., "La prueba del Whatsapp", *Diario La Ley*, n.º 8605, Sección Tribuna, 15 de septiembre de 2015 (La Ley 5350/2015), p. 1.; MAGRO SERVET, V., "¿Cómo aportar la prueba digital en el

aunque exista vínculo personal o afectivo de especial confianza con el interviniente en la comunicación. La intervención de las comunicaciones, únicamente, está permitida cuando exista una resolución judicial que la autorice en el contexto de una investigación penal y con los límites y condiciones legalmente previstos (arts. 588 bis a) y ss. LECrim).

En cambio, no existe impedimento para obtener y aportar al proceso datos personales (por ejemplo, ubicación, fotografías) y comunicaciones de terceros (mensajes de texto, audio o video) a los que se puede acceder en abierto a través de internet. Los titulares de perfiles en la red pueden establecer los niveles de privacidad que quieren aplicar[17]. Por tanto, si establecen un nivel de libre acceso, sea absoluto o limitado, a su perfil, cualquier usuario de la aplicación que tenga autorizado el acceso al mismo podrá acceder y obtener copias de sus contenidos para aportarlos lícitamente al proceso[18].

En este sentido, las SSTS 292/2008, de 28 de mayo y 1299/2011, de 17 de noviembre, señalan que, efectivamente, las comunicaciones a través de internet se encuentran protegidas por el derecho al secreto del art. 18.3 CE; pero siempre que quede constatada la voluntad de los interlocutores de realizar dicha comunicación en el ámbito de la privacidad y en el ejercicio de su derecho a la intimidad, excluyendo toda injerencia de terceros en dicha comunicación, lo que habrá que valorar atendiendo a las circunstancias de cada caso concreto. Y no parece que tal voluntad exista cuando es el propio comunicante el que permite que sus mensajes y comunicaciones sean conocidos por terceros[19].

Un tercer supuesto, que se plantea de modo relativamente frecuente en el ámbito familiar y de pareja, es el de los dispositivos y aplicaciones de mensajería compartidos, o de titularidad personal, pero con acceso y uso autorizado a otros miembros del núcleo familiar. Por ejemplo, la pareja o los miembros de la unidad familiar comparten el uso del ordenador, la

---

proceso penal?", *Diario La Ley*, n.º 9824, Sección Doctrina, 7 de abril de 2021 (La Ley 3855/2021), p. 8.

17. Por lo general las plataformas ofrecen tres niveles de privacidad/publicidad: a) accesibilidad a amigos; b) accesibilidad a amigos de amigos; y c) accesibilidad plena a toda la red (*Vid*., FISCALÍA GENERAL DEL ESTADO, *Dictamen n.º 1/2016 sobre la valoración de las evidencias en soporte papel…*, *op. cit*., p. 11).

18. Como señala ARMENTA DEU ("Regulación legal y valoración probatoria de fuentes de prueba digital…", *op. cit*., p. 74), la información insertada voluntariamente en la red para ser compartida con otros usuarios no goza de la protección del secreto de las comunicaciones; sin embargo, en supuestos como la información transmitida entre un grupo limitado o identificado de interlocutores sí resulta aplicable el art. 18.3 CE.

19. *Vid*., SSTS 292/2008, de 28 de mayo (RJ 2008, 3241) y 1299/2011, de 17 de noviembre (RJ 2012, 1540).

Tablet, una cuenta de correo electrónico, o una aplicación bancaria; y lo mismo cabe decir de los grupos de Whatsapp. En estos casos, se considera lícito que cualquiera de los sujetos autorizados para el uso de estos dispositivos o aplicaciones pueda acceder a ellos y obtener los mensajes y comunicaciones transmitidos o recibidos a través de los mismos. No se vulnera con ello el derecho al secreto de la comunicación porque todos han aceptado, expresa o tácitamente, el acceso de los demás sujetos autorizados. Ahora bien, podría vulnerarse el derecho a la intimidad si la información personal de alguno de los sujetos autorizados así obtenida se utiliza con fines ilícitos, para causarle un perjuicio[20]; lo cual no es el caso de que se utilice como fuente de prueba en un proceso penal.

Otro supuesto que también se da con frecuencia en el ámbito familiar es el del acceso por parte de un progenitor a los mensajes albergados en los dispositivos o aplicaciones de sus hijos menores de edad. En este sentido, la jurisprudencia ha admitido como lícito el acceso del progenitor a los mensajes albergados en el teléfono móvil de su hijo menor de edad, especialmente, cuando es el propio progenitor el que asume los gastos del dispositivo y de la conexión a internet, por entender que la vigilancia por los padres de la actividad en las redes sociales de los hijos menores de edad se incluye entre las obligaciones inherentes a la patria potestad del art. 154 CC.

Así, el AAP de Pontevedra 893/2017, de 25 de octubre, ante la denuncia presentada por la madre contra el padre, porque éste se habría apoderado de las conversaciones que mantuvo su hija a través de su teléfono móvil con su progenitora y denunciante, ha considerado lícito que, en virtud de este deber del padre conforme al art. 154 CC, que comparte con la denunciante la patria potestad de su hija menor, éste haya revisado en presencia de la hija determinadas conversaciones de Whatsapp mantenidas por ésta[21].

Finalmente, también se considera lícita la aportación al proceso como fuente de prueba de los mensajes y comunicaciones electrónicas que han sido remitidos al abogado por la parte contraria o el abogado de ésta, proporcionándole cierta información relevante para el proceso, por ejemplo, a efectos de intentar algún acuerdo. Nada impide que tales comunicaciones se aporten al proceso por cualquiera de los intervinientes en las mismas, salvo que estén protegidas por un deber de confidencialidad (por ejemplo, la que se puede derivar de haberse intentado previamente una mediación). Con todo, ello no obsta para que el abogado que así

20. *Vid.*, RICHARD GONZÁLEZ, M., "Valor como prueba de los mensajes y comunicaciones electrónicas…", *op. cit.*, p. 229.

21. *Vid.*, AAP de Pontevedra 893/2017, de 25 de octubre (JUR 2017, 308428).

actúa pueda incurrir en algún tipo de responsabilidad disciplinaria por incumplir las normas deontológicas relativas a las comunicaciones entre letrados[22].

III. APORTACIÓN AL PROCESO DE LA FUENTE DE PRUEBA: MEDIO DE PRUEBA

Las fuentes de prueba electrónicas o digitales (mensajes o comunicaciones electrónicas) obtenidas lícitamente por las partes pueden introducirse o aportarse al proceso de distintas formas, aunque, *a priori*, ninguna de ellas garantiza absolutamente la autenticidad e integridad del mensaje o comunicación, porque tanto la autoría como el contenido del mismo son susceptibles de manipulación o alteración. Por tanto, como veremos, la validez y suficiencia probatoria de estas fuentes de prueba dependerá en buena medida del cauce procesal o medio de prueba a través del cual se introduzcan en el proceso y de la actitud que adopte respecto de ellas la parte contraria a la que perjudique la prueba, es decir, según admita su validez o impugne su autoría o autenticidad. Esta impugnación abrirá la posibilidad, según el criterio judicial, de que la parte que aportó las pruebas digitales impugnadas desarrolle una actividad probatoria complementaria para tratar de acreditar la validez, autenticidad e integridad de las comunicaciones electrónicas aportadas, por ejemplo, mediante una prueba pericial informática.

Pero esto es una cuestión que afecta al valor probatorio del medio de prueba, que luego veremos, no a lo que ahora interesa que son las formas admisibles de introducir en el proceso estas fuentes de prueba; o dicho de otro modo, ¿cuáles son los medios de prueba a través de los cuales se pueden introducir en el proceso estas fuentes de prueba digitales?[23].

A falta de una previsión legal sobre específicos medios de prueba para introducir en el proceso estas nuevas fuentes electrónicas o digitales, tendremos que echar mano de los medios de prueba tradicionales que mejor se adecúen a la naturaleza y características de esta fuentes[24], siendo

22. *Vid.*, RICHARD GONZÁLEZ, M., "Valor como prueba de los mensajes y comunicaciones electrónicas…", *op. cit.*, p. 231.
23. A este respecto, MAGRO SERVET ("¿Cómo aportar la prueba digital…?", *op. cit.*, pp. 3 a 8) reflexiona sobre la problemática que conlleva la falta de autonomía de la prueba digital, respecto de los medios de prueba tradicionales, es decir, la necesidad de canalizar la introducción en el proceso de estas nuevas fuentes de prueba a través de los cauces o medios de prueba tradicionales, previstos legalmente.
24. *Vid.*, MAGRO SERVET, V., "¿Cómo aportar la prueba digital…?", *op. cit.*, pp. 5-8. En el mismo sentido, ARRABAL PLATERO, P., "La prueba documental como medio para

recomendable la utilización de varios de estos medios de forma cumulativa para afianzar su valor probatorio[25]. Así, aunque se podrá utilizar otros, los más habituales serán los siguientes: la prueba de reconocimiento judicial (arts. 299.2 y 382 y 384 LEC), la prueba documental y la prueba testifical (o interrogatorio del acusado).

1. LA PRUEBA DE RECONOCIMIENTO JUDICIAL: REPRODUCCIÓN Y VISIONADO DE WEBS Y MENSAJES (TEXTO, IMAGEN, AUDIO O VIDEO) APORTADOS EN FORMATO ELECTRÓNICO

Puesto que se trata de fuentes de prueba en formato electrónico, (mensajes y comunicaciones electrónicas, contenidos de webs o redes sociales) lo normal, aunque no lo habitual, sería aportarlos al proceso en ese mismo formato, al amparo de los arts. 299.2, 382 y 384 LEC, para que puedan ser objeto de un reconocimiento judicial por el órgano enjuiciador.

Esta forma de aportación sería particularmente indicada cuando se pretende incorporar como prueba el contenido de páginas web o redes sociales. En tal caso, al proponer la prueba en el correspondiente escrito de calificación provisional, se debe indicar la web o red social que se ha de visionar en el juicio, y solicitar que ese día estén disponibles en la sala de vistas los medios técnicos necesarios para poder realizar esta reproducción y visionado (u ofrecerse la parte proponente a aportarlos).

Pero, dado el carácter volátil de estas fuentes de prueba, esta forma de aportación comporta el riesgo de que el contenido que se pretende visionar en el juicio sea retirado por la parte contraria con anterioridad al día del juicio. Por ello, es conveniente proceder al "aseguramiento de la prueba digital", y una forma de hacerlo sería aportándola también

aportar evidencias tecnológicas", *Elderecho.com*, https://elderecho.com/la-prueba-documental-como-medio-para-aportar-evidencias-tecnologicas, última consulta: 07/06/2022; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, pp. 2 y 3; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías", *Revista General de Derecho Procesal*, 44 (2018), p. 19; GÓMEZ CONESA, A., "El papel de WhatsApp y redes sociales en el proceso penal del Siglo XXI (1)", *Diario La Ley*, n.º 9858, Sección Tribuna, 26 de mayo de 2021, (La Ley 5309/2021), pp. 8 y 9.

25. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer cometidos a través de las nuevas tecnologías", *Revista Acta Judicial*, núm. 7, enero-junio 2021, p. 24; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, p. 3; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 19.

de modo documental, por ejemplo, mediante un acta notarial, en la que se deje constancia del contenido que el notario pudo visionar en dicha página web o red social[26].

Además del contenido de páginas web y redes sociales, también podrán ser objeto de este reconocimiento judicial los mensajes y comunicaciones electrónicas (por ejemplo, los mensajes de Whatsapp o de correo electrónico con archivos de imagen, audio o vídeo). A tal efecto, se puede aportar y consignar ante el letrado de la Administración de Justicia, a fin de garantizar la cadena de custodia, el propio dispositivo en el que se recibió el mensaje (teléfono móvil, tablet, …), el disco duro del ordenador, o una memoria USB o tarjeta de memoria en la que se hayan almacenado los mensajes, y pedir que sean visionados en el juicio oral o examinados por el tribunal (art. 384.1 LEC).

A estos efectos, tratándose de mensajes de Whatsapp, se vería reforzado su valor probatorio si se aportasen los dos terminales o dispositivos implicados en la comunicación (el de emisión y el de recepción), porque, dadas las características técnicas de esta aplicación de mensajería, ello permitiría el reconocimiento y cotejo de los mismos por el juez, a efectos de acreditar el contenido de los mensajes y su presencia en los terminales de emisión y recepción[27].

En cualquier caso, será conveniente que, además de aportar los mensajes o correos en formato electrónico, también se acompañe la impresión o transcripción de los mismos (con o sin el apoyo de un informe pericial informático o acta notarial) para facilitarle al tribunal el acceso al contenido de esas comunicaciones electrónicas.

---

26. A tal efecto, matiza MAGRO SERVET ("¿Cómo aportar la prueba digital…?", *op. cit.*, p 8) que será suficiente aportar como documental el acta notarial, como prueba subsidiaria a la de reconocimiento judicial del contenido de la web o red social, sin que sea necesario proponer la testifical del notario que extendió el acta, porque no se requiere que el notario ratifique el acta en el juicio para que ésta haga prueba de su contenido.

27. En este sentido, señala CUAIRÁN ("La aportación de WhatsApps como medio de prueba…", *op. cit.*, p. 4) que, si bien los mensajes de WhatsApp son perfectamente utilizables como medios de prueba en un proceso penal, debiendo estarse al principio de libre valoración de la prueba por parte del juez, la configuración técnica actual de este servicio de mensajería no permite garantizar sin lugar a duda razonable la autenticidad de las conversaciones ni la integridad de su contenido, si no es mediante el cotejo de todos los terminales intervinientes en la conversación. *Vid.*, asimismo, ARMENTA DEU, T., "Regulación legal y valoración probatoria de fuentes de prueba digital…", *op. cit.*, p. 73; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, p. 7.

2. LA PRUEBA DOCUMENTAL: APORTACIÓN MEDIANTE LA TRANSCRIPCIÓN DEL MENSAJE O IMPRESIÓN DE LA CAPTURA DE PANTALLA

El medio de prueba más común para aportar al proceso las fuentes de prueba digitales, en particular cuando se trata de mensajes de texto o, incluso, de imagen y audio, es la prueba documental. Es decir, se pueden imprimir los mensajes de texto o la captura de pantalla en la que aparece el mensaje (el llamado "pantallazo"), o transcribir los mensajes de audio, y presentarlos en el Juzgado de Instrucción como prueba documental[28].

No obstante, a efectos de reforzar la solidez y valor de esta prueba, es decir, la confianza en su autenticidad e integridad, es conveniente tener en cuenta dos aspectos. En primer lugar, será conveniente que la impresión recoja toda la cadena de mensajes que se refieren al mismo hecho relevante que se pretende acreditar, pues ello permite al tribunal conocer y comprender mejor el contexto general de la comunicación en el que se remite el mensaje. Y, en segundo, tratándose de correos electrónicos, es conveniente que el "pantallazo" incluya la "cabecera del correo", pues en ella figuran datos relevantes para acreditar la autenticidad e integridad del correo, tales como el remitente, el destinatario, el asunto, la fecha y hora en que fue redactado, la fecha y hora en que fue recibido, los servidores por los que ha pasado, etc.

Esta impresión o transcripción que se aporta al proceso la puede hacer la propia parte privadamente, pero ello ofrecería pocas garantías sobre la autenticidad e integridad del mensaje documentado. Por ello, el valor probatorio de esta prueba documental se puede ver reforzado de tres modos, que permiten incrementar la confianza en la autenticidad e integridad de la comunicación electrónica[29].

---

28. En este sentido, afirma FUENTES SORIANO ("Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 24) que, se asume, como punto de partida, que la parte interesada podrá aportar al proceso como fuente de prueba de una comunicación determinada la mera captura de pantalla con la conversación, sin tener que dar, *a priori*, muestras de la autenticidad y originalidad del documento. Esta forma de aportación ha sido admitida, entre otras, por las SSTS 300/2015, de 19 de mayo (RJ 2015, 1920) y 754/2015, de 27 de noviembre (RJ 2015, 5552); 375/2018, de 19 de julio (RJ 2018, 3771); 332/2019, de 27 de junio (RJ 2019, 2792).

29. No obstante, la STSJ Galicia 556/2016, de 28 enero (JUR 2016, 45246), se muestra más exigente y declara que no basta con la aportación del pantallazo como documento privado, sino que es necesario aportar también su trascripción y exige fe pública sobre la concordancia entre ambos: "para considerar una conversación de WhatsApp como documento –a los fines del proceso laboral–, sería preciso que se hubiese aportado no sólo la copia en papel de la impresión de pantalla o, como se denomina usualmente, "pantallazo" –que es lo único se cumple por el actor–, sino una transcripción de la conversación y la comprobación de que de que ésta se corresponde con el teléfono y

El primero consistiría en la aportación de los mensajes documentados mediante acta notarial, es decir, mediante la intervención del notario como fedatario público. Pero con tal intervención del notario tampoco se garantiza de modo indubitado la autenticidad e integridad de la comunicación, sino únicamente el hecho concreto del que da fe el notario, y que dependerá del tipo de intervención que se le pida.

Así, la intervención del notario puede consistir simplemente en protocolizar la impresión o transcripción del mensaje electrónico que le presenta la parte, de modo que solo da fe de la identidad del sujeto que solicita la protocolización, del contenido del documento entregado (la impresión o transcripción del mensaje) y la fecha en que lo recibe. Pero la intervención del notario también puede consistir en acceder directamente al mensaje almacenado en el terminal o dispositivo electrónico, y levantar un acta de su contenido. En tal caso, daría fe del contenido del mensaje y de que dicho mensaje se encuentra almacenado en ese dispositivo concreto; lo que, a su vez, permitirá acreditar que, a partir de ese momento, el mensaje no fue manipulado. Pero el notario no puede dar fe de la autenticidad e integridad del mensaje, porque pudo haber sido manipulado anteriormente[30]. Finalmente, el notario también puede actuar como depositario del terminal o dispositivo electrónico en el que se almacenan los mensajes, a efectos de su aportación posterior al proceso, lo que permitirá garantizar que, a partir de ese momento, no se produce ninguna manipulación del dispositivo ni de la autoría y contenido del mensaje.

En segundo lugar, esta función del notario también puede ser realizada por el LAJ, aunque no es frecuente que se presten a ello, si bien no existe ninguna norma que lo prohíba. Si se le presenta el terminal o dispositivo

---

con el número correspondientes. Esto podría haber conseguido a través de la aportación del propio móvil del Sr. Abel y solicitando que, dando fe pública, el LAJ levante acta de su contenido, con transcripción de los mensajes recibidos en el terminal y de que éste se corresponde con el teléfono y con el número correspondientes; o, incluso, mediante la aportación de un acta notarial sobre los mismos extremos". Y añade que: "Apurando nuestras consideraciones sobre la prueba de mensajería instantánea y con fines esclarecedores, para que aceptemos como documento una conversación o mensaje de este tipo (algo diferente a su valor probatorio) podríamos establecer cuatro supuestos: (a) cuando la parte interlocutora de la conversación no impugna la conversación; (b) cuando reconoce expresamente dicha conversación y su contenido; (c) cuando se compruebe su realidad mediante el cotejo con el otro terminal implicado (exhibición); o, finalmente, (d) cuando se practique una prueba pericial que acredite la autenticidad y envío de la conversación, para un supuesto diferente de los anteriores".

30. *Vid.*, CUAIRÁN, J., "La aportación de WhatsApp como medio de prueba…", *op. cit.*, p. 4; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 19; GÓMEZ CONESA, A., "El papel de WhatsApp y redes sociales…", *op. cit.*, p. 8.

en el que se almacenan los mensajes, junto con la impresión o transcripción de los mismos, el LAJ puede acceder al terminal, verificar la existencia y contenido de los mensajes y levantar un acta por la que da fe de que la impresión o transcripción aportada es fiel reflejo del contenido de los mensajes almacenados en el terminal, así como del modelo y número de dicho terminal. Con ello se daría fe del contenido de los mensajes y de que se recibieron en dicho dispositivo concreto.

Esta forma de aportación se ha admitido, entre otras, por la SAP de Córdoba 159/2014, de 2 de abril y por la SAP de Alicante 753/2015, 9 de diciembre[31]. En ellas, se afirma lo siguiente: "En la legislación procesal actual no existe regulación específica de la prueba electrónica pese a que, como canal de comunicación, actos jurídicos y hechos con trascendencias jurídica se producen cada vez en más ocasiones a través de WhatsApp (…). Si bien en la práctica, los juzgados y tribunales suelen admitir dichas pruebas e incorporarlas al procedimiento tras realizar un cotejo de las mismas. En el caso de los mensajes de WhatsApp, se requiere a la parte que los alega para que acuda al juzgado con el dispositivo móvil y se proceda, por parte del secretario judicial, a cotejar su contenido desde el propio dispositivo con las transcripciones aportadas en papel, levantando acta por la que se de fe de que dicha documental es fiel reflejo del contenido de la conversación guardada en el móvil, así como del modelo y número de teléfono del mismo".

Como se ha dicho, a través de estas formas de aportación que hemos visto se puede acreditar que un mensaje electrónico ha sido recibido en un determinado dispositivo o terminal, y cuál es el contenido del mismo. También se podría acreditar que, a partir de un determinado momento (por ejemplo, desde que se deposita el dispositivo ante el notario o el LAJ) tal comunicación no ha sido manipulada o alterada. Pero tales formas de aportación no permiten acreditar de modo indubitado la autenticidad (es decir, la autoría real) y la integridad (es decir, que su contenido original no fue manipulado o alterado antes de su aportación) del mensaje electrónico[32]. Tales extremos solo se pueden acreditar fehacientemente mediante un análisis pericial informático del dispositivo.

31. SAP de Córdoba 159/2014, de 2 de abril (JUR 2014, 168647) y en la SAP de Alicante 753/2015, 9 de diciembre (JUR 2016, 132447).

32. Sobre los conceptos de autenticidad e integridad, *Vid.*, arts. 8 y 10 del Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación: la autenticidad del origen de una factura garantiza la identidad del obligado a su expedición y del emisor de la factura; y la integridad del contenido garantiza que el mismo no ha sido modificado. *Vid.*, DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, p. 5.

Ahora bien, tal informe pericial informático no es necesario siempre que se trate de aportar al proceso una fuente de prueba de carácter electrónico. Solo será necesario, en su caso, si la parte adversa impugna, cuestiona la autenticidad o integridad del mensaje. Si no las cuestiona, o incluso admite expresamente dicha comunicación y su contenido, bastará la aportación como prueba documental de la impresión o transcripción del mensaje para probar su realidad y contenido.

3. LA PRUEBA TESTIFICAL: APORTACIÓN MEDIANTE LA DECLARACIÓN TESTIFICAL DE TERCEROS QUE HAYAN VISTO EL MENSAJE EN EL DISPOSITIVO

Finalmente, las fuentes de prueba electrónicas o digitales también se pueden introducir en el proceso a través de la prueba testifical (o interrogatorio del acusado). Es decir, la existencia y contenido del mensaje o comunicación electrónica en cuestión también se puede introducir en el proceso a través de la declaración testifical de personas que hayan visto dicho mensaje y su contenido en el dispositivo o terminal de envío o recepción (o mediante el interrogatorio del acusado sobre el envío de tal mensaje).

IV. IMPUGNACIÓN Y VALOR PROBATORIO

Al igual que para las demás pruebas en el proceso penal, para la valoración probatoria de estas fuentes de prueba electrónicas o digitales rige el principio de libre valoración de la prueba, es decir, el juez debe valorarlas conforme a las reglas de la sana crítica y según las máximas de experiencia (así resulta de los arts. 382.3 y 384.3 LEC, que son de aplicación subsidiaria a todas las jurisdicciones, y del art. 741 LECrim), y teniendo en cuenta las demás pruebas practicadas (valoración conjunta de la prueba)[33].

33. *Vid.*, DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, pp. 4, 6 y 7. Señala este autor que la libre valoración de la prueba electrónica, "en primer lugar, quiere decir que la Ley no obliga al Juez a tener por probados los hechos que surjan de una prueba electrónica; salvo los supuestos de documento público electrónico. En segundo lugar, significa que la Ley no determina que la prueba electrónica solamente puede tener eficacia probatoria si se cumplen ciertos presupuestos legales; sino que cualquier prueba electrónica puede, en principio, desplegar efectos para acreditar un hecho relevante para el proceso. Otra cosa es la verosimilitud o eficacia probatoria que el Juez otorgue a una concreta prueba digital de conformidad con las reglas de la sana crítica. En tercer lugar, también quiere decir que el Juez valorará la prueba electrónica conforme a las reglas de sana crítica según la naturaleza del soporte en que se hayan aportado los datos; en definitiva, una valoración conforme a las reglas

Esto significa que el valor probatorio que pueden alcanzar estas fuentes de prueba dependerá de varios factores[34]: a) la propia tecnología de comunicación utilizada y, en particular, la facilidad de manipulación de la misma; b) el medio de prueba a través del cual se ha introducido en el proceso, lo que, a su vez determina la solidez de la autenticidad e integridad de la fuente de prueba (por ejemplo, si se ha aportado la simple impresión de la captura de pantalla o se aportó acta notarial con la transcripción del mensaje); y, c) fundamentalmente, dependerá de la actitud procesal de la parte a la que perjudica esta prueba, es decir, de si impugna o no la autenticidad e integridad de la comunicación.

1. LA PARTE CONTRARIA NO IMPUGNA LA AUTENTICIDAD Y/O INTEGRIDAD DE LA FUENTE DE PRUEBA

Si, ante la aportación de la fuente de prueba electrónica o digital en cualquiera de las modalidades que hemos visto (incluso una simple impresión de un pantallazo), la parte contraria a la que perjudica no impugna su autenticidad y/o integridad, ésta podría alcanzar pleno valor probatorio, y, en base a ella, el juez podría dar por probada la existencia, autoría y contenido de la comunicación electrónica en cuestión. Y ello, sin necesidad de ninguna prueba adicional sobre su autenticidad o integridad. Además, a estos efectos, por no impugnación cabe entender tanto la ratificación o reconocimiento expreso de la existencia y contenido de la comunicación por parte de los interlocutores, como el silencio de la parte a la que perjudica la prueba[35].

Que alcance o no este valor probatorio pleno dependerá de la aplicación que haga el juez del criterio de la libre valoración de la prueba, que

---

de criterio racional, es decir, de forma ajustada a las reglas de la lógica, los principios de la experiencia y los conocimientos científicos. En cuarto lugar, el alto componente tecnológico de la prueba electrónica determinará con frecuencia la importancia de los conocimientos científicos en su valoración, por lo que la prueba pericial tiene una especial relevancia en este ámbito. En quinto lugar, en la valoración conforme a la sana crítica el Juez habrá de tener en cuenta la postura procesal de cada una de las partes en relación con la concreta prueba electrónica: especialmente, si ha existido impugnación por la parte no proponente y el fundamento de dicha impugnación" En el mismo sentido, FISCALÍA GENERAL DEL ESTADO, *Dictamen n.º 1/2016 sobre la valoración de las evidencias…*, *op. cit.*, p. 8.

34. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer…", *op. cit.*, p. 26; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, pp. 3 y 4; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 20.

35. *Vid.*, STS 469/2017, de 22 de junio (RJ 2017, 3569); SAP de Córdoba 159/2014, de 2 de abril (JUR 2014, 168647); o SAP de Teruel 23/2017, de 21 de junio (ARP 2017, 1057).

deberá motivar en la sentencia. Y, como dijimos, a tal efecto será determinante la facilidad de manipulación del tipo de tecnología de comunicación utilizada, la confianza sobre la autenticidad e integridad que proporcione el concreto medio de prueba utilizado, así como el resto de las pruebas válidamente practicadas en el proceso.

Este valor probatorio responde a la máxima de experiencia conforme a la cual, si la parte a la que perjudica la prueba no impugna la autenticidad o integridad de la comunicación, el juez puede tenerla por cierta y acreditada; y ello, aunque en la realidad pueda haber sido falseada. Pero, si la parte a la que perjudica la prueba no la impugna, no existe razón alguna que justifique gravar a la parte que la aporta con la carga de tener que aportar un informe pericial informático u otra prueba adicional sobre la autenticidad e integridad de la comunicación que nadie ha cuestionado[36].

2. LA PARTE CONTRARIA IMPUGNA LA AUTENTICIDAD Y/O INTEGRIDAD DE LA FUENTE DE PRUEBA

Si la parte contraria, a la que perjudica la prueba electrónica o digital, la impugna[37], poniendo en cuestión su autenticidad y/o integridad, no por ello pierde automáticamente todo su valor probatorio, porque continúa rigiendo el principio de libre valoración de la prueba. Por tanto, pese a la impugnación, a partir de la valoración conjunta de toda la prueba aportada, y de todas las circunstancias concurrentes, el tribunal puede dar por probada igualmente la existencia, autoría y contenido de la comunicación.

Es decir, la impugnación de la prueba no conlleva la sustitución automática del principio de libre valoración de la prueba por una distribución formal de la carga de la prueba, en el sentido de que se produzca una "inversión de la carga de la prueba", de modo que, si la parte a la que beneficia la prueba no consigue acreditar fehacientemente su autenticidad e integridad, el juez no pueda tenerla por válida. No, sigue rigiendo el principio de libre valoración de la prueba, conforme a las reglas de la sana crítica y las máximas de experiencia. Pero, precisamente por eso, las alegaciones impugnatorias con suficiente seriedad por la parte adversa

36. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer…", *op. cit.*, p. 26; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 20; GONZÁLEZ LAGE, J., "La prueba pericial en la práctica judicial penal: las redes sociales en el proceso penal", en *Peritaje y prueba pericial* (Dir., Picó i Junoy, J.), Bosch, Barcelona, 2017, p. 565. *Vid.*, asimismo, STS 300/2015, de 19 de mayo (RJ 2015, 1920).

37. Sobre el momento y forma de impugnar la prueba electrónica o digital, *Vid.*, MAGRO SERVET, V., "¿Cómo aportar la prueba digital…?", *op. cit.*, p. 5.

de la validez de esta prueba, puede determinar la necesidad de reforzarla con otra actividad complementaria tendente a acreditar o afianzar la existencia, autenticidad e integridad de la comunicación. Es decir, a la parte a la que favorezca la prueba ya no le basta con aportarla por alguno de los medios que hemos visto, sino que deberá aportar prueba complementaria sobre la autenticidad e integridad de la comunicación[38].

Pero, a este respecto, se plantean dos cuestiones importantes. La primera es, ¿cómo debe ser la impugnación?; es decir, ¿basta con negar la autenticidad o integridad de la comunicación o debe estar fundamentada tal impugnación? Y, la segunda, ante tal impugnación, ¿qué medios se pueden utilizar para tratar de acreditar la autenticidad e integridad cuestionada?

Por lo que se refiere al primer interrogante, cabe destacar que no cualquier impugnación de la autenticidad e integridad de la fuente de prueba electrónica va a determinar la necesidad de una actividad probatoria complementaria para acreditar tales extremos. Ha de tratarse de una impugnación con suficiente seriedad. Y, a los efectos de valorar la seriedad de tal impugnación, deben tenerse en cuenta, al menos, dos elementos[39].

En primer lugar, se deberá atender al contenido y fundamento de la impugnación, es decir, tal impugnación ha de tener un respaldo alegatorio, ha de estar fundada en argumentos e indicios serios, claros y exhaustivos, que permitan poner en duda la autenticidad e integridad de la comunicación[40]. Así, por ejemplo, la SAP de Vizcaya 90308/2014, de 24 de julio, considera insuficiente a estos efectos la mera alegación genérica de que "el WhatsApp es fácilmente manipulable"[41].

38. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer…", *op. cit.*, pp. 30 y 31; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, pp. 5 y 6; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 25.

39. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer…", *op. cit.*, pp. 31 y 32; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, p. 6.; GONZÁLEZ LAGE, J., "La prueba pericial en la práctica judicial penal…", *op. cit.*, pp. 565 y 566.

40. Como señala ARRABAL PLATERO ("La prueba documental…", *op. cit.*,), si bien la jurisprudencia no pide un "principio de prueba" a la parte impugnante, sí le pide que introduzca elementos de duda sobre la autenticidad e integridad de la prueba aportada de opuesto que se adicionen al acervo probatorio y contribuyan a desacreditar la prueba impugnada, descartando las tesis impugnatorias que resultan del todo rocambolescas y ausentes de más justificación que las únicas afirmaciones del impugnante.

41. Señala la SAP de Vizcaya 90308/2014, de 24 de julio (JUR 2014, 268182) que "la mera protesta de que el WhatsApp es manipulable y de que las conversaciones pudieron ser mantenidas por el anterior titular, es manifiestamente insuficiente para alterar la

Y, en segundo lugar, también se deberá valorar la diligencia de la parte que impugna la prueba a la hora de proponer otros medios probatorios que puedan poner en cuestión la autenticidad e integridad de la prueba digital. Por ejemplo, se podría cuestionar la autoría del mensaje, si se acredita que, en el momento del envío de tal mensaje, el teléfono estaba extraviado y no tenía contraseña de acceso, de modo que cualquier persona que lo tuviera en su poder podría haber enviado dicho mensaje.

En este sentido, la STS 300/2015, de 19 de mayo, desestimó la impugnación de la autenticidad de una conversación mantenida en Tuenti, formulada por la defensa, entre otros motivos, porque la acusación particular puso a disposición del Juzgado de Instrucción las claves personales de la víctima en Tuenti para que, si la conversación era cuestionada, se pudiese oficiar a Tuenti España para que se certificara el contenido de esa conversación, sin que la defensa hubiese hecho petición alguna al respecto[42].

A su vez, en cuanto a los medios que se pueden utilizar por la parte proponente para tratar de acreditar o corroborar la autenticidad e integridad de la comunicación electrónica impugnadas, ello dependerá de cuál haya sido el canal o medio tecnológico que se ha utilizado para dicha comunicación, pues a tal efecto resultan determinantes las específicas características técnicas de unos y otros.

2.1. En el caso de aplicaciones de mensajería instantánea (Whatsapp)

La aplicación de mensajería instantánea de Whatsapp presenta dos importantes vulnerabilidades que repercuten en la fiabilidad de sus mensajes como fuente de prueba y en el modo en que se puede tratar de acreditar la misma[43].

La primera es la facilidad con la que pueden ser manipulados los mensajes de Whatsapp, de modo que incluso existen aplicaciones que permiten crear conversaciones de Whatsapp ficticias (por ejemplo, Whatsapp

---

valoración probatoria en el sentido interesado en el recurso. Todo apunta a la autoría de la receptación por el acusado, ya que los objetos sustraídos aparecen en su teléfono que él dice adquirido de segunda mano, sin dar ningún dato sobre a quién, persona desconocida que además habría resultado ser el autor de los mensajes de WhatsApp. En opinión del Tribunal, esta versión no tiene el relieve necesario ni la credibilidad mínima para representar una hipótesis alternativa razonable a la que la sentencia ha elevado a categoría de hechos probados en la sentencia sobre la base de la prueba practicada en el juicio oral".

42. *Vid.*, STS 300/2015, de 19 de mayo (RJ 2015, 1920).

43. *Vid.*, CUAIRÁN, J., "La aportación de WhatsApp como medio de prueba…", *op. cit.*, p. 2 y 3.

Fake Chat). De ella se hacen eco, entre otras, las SSTS 300/2015, de 19 de mayo, 375/2018, de 19 de julio y 332/2019, de 27 de junio[44], señalando que "la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria".

Y la segunda vulnerabilidad referida, radica en que las conversaciones de Whatsapp no quedan almacenadas en ningún servidor externo del proveedor del servicio, sino únicamente en los dispositivos de envío y recepción, por lo que no es posible solicitar copias de los mensajes ni certificación de sus contenidos al proveedor. El proveedor del servicio únicamente conserva una información limitada sobre datos de tráfico o los relativos a identificación de usuarios, número de abonado telefónico o identificación de direcciones IP. Por tanto, la única forma de acreditar indubitadamente la autenticidad e integridad de los mensajes de Whatsapp, es decir, su existencia, autoría y contenido original, será a través de un análisis pericial consistente en el cotejo de los terminales de envío y recepción. Pero, si los comunicantes eliminan los mensajes de sus terminales, será muy difícil la práctica de una pericia informática capaz de acreditar al cien por cien su autenticidad e integridad.

Pero, aun en este caso, cabría alguna posibilidad de corroborar la autenticidad e integridad de los mensajes en ciertos supuestos[45]. Ello es así porque la aplicación de Whatsapp permite al usuario usar servicios de almacenamiento en la nube (ICloud o Google Drive) para hacer copias de seguridad de los mensajes, que se suelen hacer automáticamente. En tal caso, se podría solicitar a estos proveedores copia de los mensajes guardados y cotejarlos con las evidencias aportadas al proceso. Pero lo que no se podría es acreditar que tales mensajes no han sido manipulados antes de hacerse la copia de seguridad. Además, en el caso de conversaciones

44. *Vid.*, SSTS 300/2015, de 19 de mayo (RJ 2015, 1920); 375/2018, de 19 de julio (RJ 2018, 3771); y 332/2019, de 27 de junio (RJ 2019, 2792).

45. *Vid.*, CUAIRÁN, J., "La aportación de WhatsApp como medio de prueba…", *op. cit.*, pp. 3 y 4; FISCALÍA GENERAL DEL ESTADO, *Dictamen n.º 1/2016 sobre la valoración de las evidencias en soporte papel…*, *op. cit.*, pp. 9 y 10.

mantenidas a través de un grupo de Whatsapp, todos los usuarios del grupo han recibido el mensaje, por lo que la aportación de una copia de esta conversación, junto con la declaración testifical de varios miembros del grupo sería de gran relevancia para acreditar la autenticidad e integridad de la comunicación.

Con todo, la imposibilidad de esta prueba pericial, no implica que estos mensajes pierdan todo su valor probatorio en caso de impugnación. Es decir, la prueba pericial informática no es el único e indispensable medio de dotar de valor probatorio al mensaje de Whatsapp, porque continúa rigiendo el principio de libre valoración de la prueba, por lo que el convencimiento del juez sobre la autenticidad e integridad de los mensajes puede apoyarse en otros elementos probatorios, como la declaración de testigos, o las manifestaciones de las partes[46].

2.2. En el caso de plataformas de redes sociales (Facebook, Instagram…)

Las plataformas de redes sociales presentan otras características y vulnerabilidades a efectos de su utilización como fuente de prueba distintas a las de las aplicaciones de mensajería instantánea, lo que determina que su tratamiento sea distinto a estos efectos.

En principio, por sus propias características, no plantea excesiva dificultad corroborar la integridad de la comunicación difundida a través de estas plataformas, es decir, el contenido de la comunicación, porque, aunque los usuarios pueden establecer distintos niveles de privacidad, en principio están destinadas a la difusión pública de los contenidos, por lo que, si se impugna la integridad de la comunicación, ésta se puede corroborar a partir de la información facilitada por cualquier de los usuarios que hayan tenido acceso al mismo.

Además, la información publicada a través de estas redes sociales suele conservarse en los servidores de los operadores de las mismas (durante aproximadamente 90 días), aunque el perfil correspondiente se haya eliminado, por si el usuario desea activarlo de nuevo. Por ello, se podrá obtener de los mismos, con autorización judicial, la información conservada cuando sea necesario verificar la integridad de las fuentes de prueba o evidencias aportadas por las partes al proceso. Y, a estos efectos, la propia policía podrá ordenar al operador la conservación de la información

46. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer…", *op. cit.*, pp. 30 y 31; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, pp. 24 y 25.

almacenada en sus servidores hasta obtener la autorización judicial para la cesión de la misma (art. 588 octies LECrim)[47].

Más complejo puede ser verificar la autoría o autenticidad de la comunicación difundida. Como es sabido, para acceder y operar a través de estas plataformas y redes es necesario crear una cuenta de dominio, un perfil, con nombre de usuario y contraseña; y, frecuentemente, sobre todo para delinquir, se utilizan identidades falsas o seudónimos.

Pero, al utilizar estas plataformas, con cada acto de comunicación, se generan unos datos de tráfico y localización que quedan almacenados y que los operadores de servicios de comunicaciones electrónicas deben conservar (normalmente, durante 12 meses desde la fecha de la comunicación) y, en su caso, ceder con fines de investigación y enjuiciamiento penal, conforme a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[48]. Por tanto, a partir de estos datos, se puede hacer un rastreo que permita identificar al verdadero autor de la comunicación[49].

Este rastreo se puede hacer a partir de los datos almacenados y cedidos por parte de los operadores de servicios de comunicación, para lo cual será necesario contar con la correspondiente autorización judicial (arts. 1 y 7 Ley 25/2007 y 588 ter j) LECrim). Y hasta que se obtenga tal autorización, el MF o la policía podrán ordenar la conservación y protección de tales datos (art. 588 octies LECrim)[50].

---

47. *Vid*., FISCALÍA GNERAL DEL ESTADO, *Dictamen n.º 1/2016 sobre la valoración de las evidencias en soporte papel…*, *op. cit*., pp. 11 y 12.

48. Los datos que los operadores deben conservar son los previstos en el art. 3 Ley 25/2007: a) datos para rastrear e identificar el origen de la comunicación (identificación de usuario y número de teléfono asignados); b) datos para identificar el destino de la comunicación; c) datos para determinar la fecha, hora y duración de la comunicación; d) datos para identificar el tipo de comunicación (servicio de internet utilizado); e) datos para identificar el equipo de comunicación; o, f) datos necesarios para identificar la localización del equipo de comunicación.

49. *Vid*., FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, pp. 30 a 32.

50. A este respecto, es necesario recordar que la Ley 25/2007, de 18 de octubre, se aprobó con objeto de transponer la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, que fue declara inválida por la sentencia del TJUE (Gran Sala) de 8 de abril de 2014, *Digital Rights Ireland*, C-293/12, sobre la base de que el Derecho de la Unión Europea se opone a medidas legislativas nacionales que establezcan, con carácter preventivo, una conservación generalizada e indiferenciada de los datos de tráfico y de localización relativos a las comunicaciones electrónicas con fines de lucha contra la delincuencia grave. Si bien la referida Ley no se ve anulada como efecto directo de esta sentencia, pues no está así previsto en el Derecho Comunitario, no puede obviarse la repercusión que la misma puede tener en los procedimientos judiciales en los que se haga uso de esta conservación y cesión de datos

Pero también se puede hacer a partir de otros datos que puede recabar directamente la policía, sin necesidad de autorización judicial, conforme a los arts. 588 ter k) a m) LECrim: a) acceso por la policía a una dirección IP (y luego solicitar autorización judicial para la cesión por el proveedor de servicios de los datos que permitan la identificación y localización del equipo y la identificación del usuario); b) captación por la policía de números IMSI o IMEI o de cualquier otro dato que identifique un equipo de comunicación o la tarjeta de acceso a la red de comunicaciones (y luego pedir autorización judicial para intervenir las comunicaciones); y, c) solicitar de los prestadores de servicios de comunicaciones la identificación del titular de un número de teléfono o el número de teléfono de un determinado titular o los datos identificativos de cualquier medio de comunicación[51].

Finalmente, si no fuese posible la corroboración de la autenticidad de la fuente de prueba impugnada a través de los medios tecnológicos señalados, todavía sería posible acreditarla por otras vías. Por ejemplo, si las partes o testigos admiten o declaran que el seudónimo utilizado en la comunicación es el que utiliza habitualmente el acusado; o si los testigos declaran que el acusado había anunciado su intención de comunicarse por esta vía con la víctima. Por tanto, como señala FUENTES SORIANO, aun cuando la autenticidad de la comunicación aportada como fuente de prueba no se hubiese podido acreditar en virtud de una investigación tecnológica, sería posible otorgar valor probatorio, más o menos contundente, a esa comunicación a partir del acervo probatorio existente en el caso concreto. Ahora bien, dada la relativa facilidad con que puede adverarse la información transmitida a través de estas plataformas de redes sociales (a diferencia de lo que sucede con las aplicaciones de mensajería instantánea), el valor probatorio que pueda alcanzar dicha comunicación a partir de otros posibles medios de prueba practicados debería ser totalmente fiable e incuestionado, y reflejarse así en la fundamentación de la sentencia[52].

No obstante, estas formas de corroborar la autenticidad de la comunicación aportada como fuente de prueba plantean en la práctica dos problemas.

---

reguladas por esta Ley. Por tanto, deberán ser los jueces y tribunales españoles los que valoren caso por caso la aplicación de la Ley 25/2007, de 18 de octubre, tratando de ajustarse al principio de proporcionalidad en los términos fijados en la referida sentencia del TJUE.

51. *Vid.*, LARO GONZÁLEZ, M.ª E., "Prueba electrónica: situación actual en el proceso penal y perspectivas de futuro", en (Dir., Conde Fuentes, J. y Serrano Hoyo, G.), *La justicia digital en España y en la Unión Europea*, Atelier, Barcelona, 2019, p. 248.
52. FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 32.

En primer lugar, conforme al art. 1 Ley 25/2007, la obligación de los operadores de servicios de comunicaciones electrónicas de conservar y ceder los datos de tráfico que se generan y tratan se limita a la investigación y enjuiciamiento de "delitos graves", por lo que quedarían fuera de su ámbito un buen número de delitos cometidos constitutivos de esta violencia de género digital, que no tienen la consideración de graves conforme a los arts. 13 y 33 CP.

No obstante, a este respecto, a raíz del AAP de Madrid 131/2015, de 25 de febrero[53], se va consolidando la tesis de que, a estos efectos, la "gravedad" del delito no puede medirse exclusivamente atendiendo a su "penalidad"; sino que, habrá que tener en cuenta también otros criterios tales como la importancia y relevancia social del bien jurídico protegido, la trascendencia social de los efectos del delito o su comisión por organizaciones criminales. Por tanto, a la vista de estas circunstancias, se podrían utilizar estos medios de investigación aun tratándose de delitos que, por su penalidad, tengan la consideración de "menos graves"[54].

El segundo problema apuntado se refiere a que la mayoría de estos proveedores de servicios de comunicaciones electrónicas tienen su sede fuera de nuestro país, generalmente en EEUU, lo que obligará a acudir a solicitudes de auxilio judicial internacional[55]. A estos efectos, será importante la próxima aprobación del Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal[56], y de la Directiva

53. AAP de Madrid 131/2015, de 25 de febrero (JUR 2015, 66473). Declara este Auto que "entendemos que los "delitos graves" a que se refiere la Ley 25/2007 no son exclusivamente los delitos castigados con pena superior a cinco años, sino que también han de incluirse en tal expresión aquellos otros delitos castigados con pena inferior y que, por tanto, tienen la calificación legal de "delitos menos graves", pero que merezcan la consideración de graves en atención a otros parámetros, tales como la importancia del bien jurídico protegido, la trascendencia social de los efectos que el delito genera o la inexistencia de medios alternativos, menos gravosos, que permitan su investigación y esclarecimiento. En este punto no puede desconocerse que los efectos socialmente nocivos de determinados hechos delictivos pueden verse incrementados exponencialmente desde el momento en que se alcanza la convicción social de su impunidad, con el consiguiente fracaso de los fines preventivos que su tipificación penal persigue".
54. FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, pp. 27 y 28.
55. *Vid.*, FISCALÍA GENERAL DEL ESTADO, *Dictamen n.º 1/2016 sobre la valoración de las evidencias en soporte papel…*, *op. cit.*, p. 12.
56. *Vid., Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal* (COM(2018) 225 final) (https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0006.02/DOC_1&format=PDF).

del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales[57]. En ella, se contempla la obligación de los proveedores de servicios de comunicaciones electrónicas o de la sociedad de la información que presten sus servicios en la UE de designar un representante legal en la UE que será el responsable de recibir, cumplir y ejecutar las órdenes de entrega y conservación de esas pruebas penales electrónicas.

57. *Vid., Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales* (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018PC0226&from=ES).

Capítulo 19

Análisis de las medidas impuestas a menores infractores por delitos informáticos en España y Portugal[1]

Paula Martínez Molares

Investigadora Área de Derecho Procesal
Universidad de Vigo

I. INTRODUCCIÓN

La delincuencia juvenil en toda Europa presenta un cambio de naturaleza en cuanto a los tipos delictivos, destacando un aumento de la violencia en su comisión, una mayor participación de las mujeres jóvenes y un destacado protagonismo de los menores infractores adolescentes de más edad[2]. No obstante, no se aprecia, en los últimos años un aumento del número de infracciones cometidas por menores.

Asimismo, en cuanto a la tipología de delitos, se constata tanto en España como en Portugal, un aumento de los delitos relacionados con la violencia filio-parental y aquellos cometidos a través de las Tecnologías de la Información y la Comunicación (en adelante TIC), o, en otras palabras, cibercrímenes.

1. Este trabajo ha sido elaborado en el marco del proyecto de investigación "Respuesta jurídica y socioeducativa a la violencia de género ejercida por menores. Protección de la víctima e intervención con el menor agresor, subvencionado por el Ministerio de Ciencia e Innovación, Proyectos de I+D+I" dentro de los Programas Estatales de Generación de Conocimiento y Fortalecimiento Científico y Tecnológico del Sistema de I+D+I y de I+D+I orientada a los Retos de la Sociedad en la convocatoria de 2019, (Ref. PID2019-106700RB-I00).

2. ABADÍAS SELMA, A., CÁMARA ARROYO, S. y SIMÓN CASTELLANO, P. *Tratado sobre delincuencia juvenil y responsabilidad penal del menor: a los 20 años de la Ley Orgánica 5-2000, de 12 de enero, reguladora de la responsabilidad penal de los menores*, La Ley, 2021.

En primer lugar, es preciso definir "cibercriminalidad". Es preciso destacar que, en Europa no existe una terminología única sobre lo que se debe entender como ciberdelincuencia y tampoco existe un catálogo concreto de delitos que deben encuadrarse dentro de la misma. En el caso de España, se ha optado por regular la ciberdelincuencia en el propio Código Penal, desechando la opción de una Ley penal especial. Así, en las sucesivas reformas del Código Penal se han ido introduciendo nuevos tipos penales de carácter informático[3].

A los efectos de este estudio, partiremos del concepto de cibercriminalidad adoptado por la Estrategia Nacional de Ciberseguridad 2019[4], aprobada por el Consejo de Seguridad Nacional y publicada en el BOE n.º 103 de fecha 30 de abril de 2019, mediante la Orden PCI/487/2019, de 26 de abril, en la que se define a ésta como *"el conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo"*.

Asimismo, se alude a que *"son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: (i) el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; (ii) el ciberespacio como medio clave para su comisión; y (iii) el ciberespacio como medio u objeto directo de investigación de cualquier tipo de hecho ilícito"*.

En lo que respecta al ordenamiento jurídico portugués, con relación al concepto de "*cibercrime*", se puede definir éste como el hecho tipificado en la ley como crimen que es practicado a través de la utilización de un sistema informático, conforme dispone el artículo 2.º, al. a) de la Ley 109/2009, de 15 de septiembre (*Lei do Cibercrime)* o en el que el sistema informático es el objeto de la acción, instrumento del crimen o cuya

3. Uno de ellos fue la reforma de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en el año 2015. La otra fue la ratificación por España del Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo, el 28 de enero de 2003 (entró en vigor 1 de abril de 2015).

4. La Estrategia Nacional de Ciberseguridad 2019 establece la posición de España ante una nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional. La importancia que otorga la Estrategia Nacional de Ciberseguridad a la cibercriminalidad se ve corroborada por el establecimiento como Línea de Acción 3 el "*Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio*", esgrimiéndose una serie de medidas al respecto.

comisión está significativamente ligada a la utilización de un sistema informático[5].

En virtud de ello, el concepto de "*cibercrime*" en derecho portugués, englobará aquellos crímenes que atenten contra bienes directamente ligados al medio informático, que protejan el propio uso de la informática y sus aspectos característicos como el software o la navegación por internet, los delitos que atenten contra bienes jurídicos tradicionales (como la honra o el patrimonio) y aquellos que sean cometidos a través del uso de sistemas informáticos.

De los anteriores conceptos, se desprende que tanto el legislador español como el portugués parecen decantarse por un concepto amplio de cibercriminalidad, aplicable, por extensión, al derecho penal de menores.

Si bien se puede decir que la delincuencia juvenil ha ido descendiendo en los últimos años, la importancia de la cibercriminalidad entre menores va creciendo año tras año, como lo demuestran el aumento del número de hechos conocidos y el peso proporcional que va adquiriendo dentro del conjunto de la criminalidad[6].

De los datos obrantes en el Portal Estadístico de Criminalidad del Ministerio del Interior se desprende que la evolución de los ciberdelitos desde los años 2011 a 2020 sigue una curva de crecimiento, y si bien, el mayor porcentaje de víctimas se sitúa en el rango de edad comprendido entre 26 a 40 años (34,71%), el número de víctimas menores de edad se ha incrementado en un 335,29% desde el año 2011 al 2020.

En cuanto a detenciones e investigados por causa de cibercriminalidad y por grupo edad, el valor de la variable se concentra, nuevamente, en la franja de edad de 26 a 40 años (41,91%), mientras que el número de detenidos e investigados menores de edad ha crecido en un 239,68%.

Esto se debe al uso generalizado y cada vez a una edad más temprana de las nuevas tecnologías por parte de los menores, tal y como ponen de manifiesto las estadísticas más recientes.

Concretamente, la Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares (año 2020), elaborada por el Instituto Nacional de Estadística (INE), dirigida a las personas de 16 y más años residentes en viviendas familiares, recoge información sobre los diversos productos de tecnologías de información y comunicación de

5. RODRIGUEZ NUNES, D. *Os crimes previstos na Lei do Cibercrime*, GESTLEGAL, Coimbra, 2020.

6. Estudio sobre la cibercriminalidad en España, año 2019, elaborado por la Secretaría de Estado de Seguridad del Ministerio del Interior, en colaboración con el Sistema Estadístico de Criminalidad.

los hogares españoles, así como los usos que hacen los españoles de estos productos, de internet y del comercio electrónico, dedicando una atención especial al uso que los niños hacen de la tecnología.

Precisamente, los grupos de edad más temprana (de 10 a 15 años) son los que más hacen uso de las tecnologías. El uso de ordenador es muy elevado (91,5% de los menores frente al 89,7% en 2019) y aún más el uso de internet (el 94,5%, el 92,9% en 2019).

Por su parte, el 69,5% de la población de 10 a 15 años dispone de teléfono móvil frente al 66,0% en 2019.

La misma encuesta analiza por sexo el uso de las TIC, haciendo referencia a que son las niñas las que usan en mayor medida las nuevas tecnologías. Por edad, el uso de TIC crece a medida que aumentan los años de los menores, sobre todo a partir de los 13.

En lo que respecta a Portugal, según los datos del Instituto Nacional de Estadística[7], en 2021, las familias con menores de hasta 15 años registran tasas de acceso a internet (98,2%) y de acceso en banda ancha (97,0%), más elevados que la generalidad de las familias.

En 2021, al igual que en el año anterior, la población portuguesa de 16 a 74 años que utilizó internet, lo hizo principalmente para comunicarse y acceder a información: 91,4% (vía WhatsApp, Messenger, etc.), el 87,6% enviaron o recibieron emails; el 86,7% buscaron información sobre productos o servicios y el 81,3% leyeron noticias.

El informe también destaca que la proporción de personas que utilizaron internet para telefonear o hacer llamadas de vídeo fue la que más aumentó, de 70,5% en 2020 a 79,7% en 2021.

Además, oír música continúa siendo el principal motivo de entretenimiento en el uso de internet (69,0%).

A modo comparativo entre la sociedad portuguesa y la española, en cuanto al uso de nuevas tecnologías y acceso a internet, cabe destacar que mientras Portugal continúa estando por debajo de la media de la Unión Europea en cuanto a usuarios de internet en 2020, con un 88%; España, por primera vez, se encuentra por encima de la media, con un 91% frente al 90% de la Unión Europea (UE-28)[8].

7. *Inquérito à utilização de tecnologias da informação e da comunicação pelas famílias 2021*, Instituto Nacional de Estatística, Statistics Portugal.
8. Comparación de la sociedad española con las tecnologías de la información en relación a los demás países de la Unión Europea, en función de la información obtenida de EUROSTAT.

Los datos anteriormente expuestos que ponen de manifiesto el alto uso que los menores realizan de las TIC, conllevan inevitablemente a concluir que son éstos el colectivo más vulnerable a convertirse en víctimas de los ciberdelitos, pero también a ser, cada vez, más susceptibles de cometerlos.

Conforme se establece en la Estrategia Nacional de Ciberseguridad, reseñada anteriormente, el ciberespacio es un espacio común global caracterizado por su apertura funcional y su dinamismo. La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan, lo convierten en un escenario donde entran en conflicto la información y la privacidad de los datos.

Asimismo, el ciberespacio constituye hoy en día el contexto básico de socialización para los adolescentes digitales, pero también se configura como un nuevo espacio de oportunidad criminal en el que niños, niñas y jóvenes continúan siendo víctimas y pueden devenir también fácilmente ciberagresores[9].

En los últimos años se ha evidenciado la tendencia de algunos menores a ser también victimarios, debido a que son los jóvenes, tal y como se ha puesto de manifiesto, quienes tienen un mayor acceso a esta clase de tecnologías y, además, muchos de los delitos que cometen los menores de edad tienen como víctimas a otros menores de edad, frecuentemente pertenecientes a su grupo social cercano.

El perfil habitual de este victimario suele ser el de un menor de edad temprana (alrededor de 14-15 años), varón y usuario experto de medios de comunicación virtuales, con conocimientos de informática (frecuentemente autodidactas y limitados) y manejo de programas maliciosos. Normalmente actuará mediante el uso de herramientas secundarias, esto es, programas no creados por él mismo[10].

II. DELITOS INFORMÁTICOS COMETIDOS POR MENORES EN ESPAÑA Y PORTUGAL

Con respecto a la tipología de delito, es preciso distinguir qué tipos de delitos informáticos son más susceptibles de ser cometidos contra

9. MONTIEL JUAN, I., "Cibercriminalidad social juvenil: la cifra negra" en el Monográfico *Ciberdelincuencia y cibervictimización, Revista de Internet, Derecho y Política*, Universitat Oberta de Catalunya, IDP N.º 22, 2016.
10. CÁMARA ARROYO, S. (2015): Apuntes de delincuencia y criminología juvenil: adaptados a la docencia del Plan Bolonia. Logroño: UNIR.

menores, es decir, en cuales las víctimas son menores, de aquellos en los que es el menor el sujeto activo del delito.

Entre los primeros, destacan los delitos de tipo sexual, sobre los que existe una gran preocupación en todos los países de la Unión Europea que se ha traducido en diferentes programas de prevención y que progresivamente se han ido sumando al catálogo de hechos ilícitos de los diferentes ordenamientos jurídico-penales.

En el caso de España, tal y como muestran los estudios más recientes, entre ellos el Informe sobre delitos contra la libertad e indemnidad sexual en España, elaborado por el Ministerio del Interior[11]; durante los siete últimos años la tendencia muestra un patrón acusado de crecimiento de los mismos, que rompe la tónica general de años anteriores.

El fenómeno conocido como *sexting* ha sido definido de forma diversa por la comunidad científica. El término proviene de la contracción de "sex" y "texting", y en las distintas definiciones que se han venido utilizando se incluían el envío, la recepción o el reenvío o difusión, tanto de mensajes sexualmente explícitos, como de imágenes de los protagonistas en las que aparecen desnudos, semidesnudos o de forma sexualmente sugerente, realizándose dicha comunicación a través de teléfonos móviles.

En el ordenamiento jurídico español, esta figura delictiva fue introducida por la LO 1/2015 de 30 de marzo por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Se incluye dentro del Título X del Libro II del Código Penal dedicado a los "*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*" y, más concretamente, en el Capítulo Primero, bajo la rúbrica "*Del descubrimiento y revelación de secretos*", el apartado 7 del artículo 197 de dicho Cuerpo Legal, que castiga con pena alternativa de prisión o multa a quien, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona; previéndose una agravación de la pena cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun

11. Informe sobre delitos contra la libertad e indemnidad sexuales en España, Ministerio del Interior. Gobierno de España, 2017, cuyos datos han sido obtenidos del Sistema Estadístico de Criminalidad (SEC); teniendo en cuenta para su cómputo los hechos de los que han tenido conocimiento los siguientes cuerpos policiales: Guardia Civil, Cuerpo Nacional de Policía, Policías dependientes de las diferentes comunidades autonómicas (Ertzaintza, Mossos d'Esquadra y Policía Foral de Navarra) y las Policías Locales que facilitan datos al SEC.

sin convivencia, la víctima fuera menor de edad o persona con discapacidad necesitada de especial protección o los hechos se hubieran cometido con una finalidad lucrativa.

Como indicaba el legislador al regular esta nueva figura delictiva, su finalidad era solucionar los problemas de falta de tipicidad de algunas conductas en respuesta a aquellos supuestos en los que las imágenes o grabaciones de otra persona se obtienen con su consentimiento, pero son luego divulgados contra su voluntad, cuando la imagen o grabación se haya producido en un ámbito personal y su difusión, sin el consentimiento de la persona afectada, lesione gravemente su intimidad.

Otro de los delitos que ha adquirido una gran relevancia, especialmente desde la pandemia, es el *online grooming*, también conocido como ciberacoso sexual[12]. Se trata de aquella conducta llevada a cabo generalmente por un adulto mediante el uso de las TIC, con la finalidad de engañar, manipular o embaucar a un menor para un futuro contacto sexual online u offline.

El *online grooming* en sí mismo no implica necesariamente una actividad sexual, sino que constituye la estrategia de cortejo o seducción empleada por el agresor para acercarse al menor, captar su atención e interés[13]. En definitiva, será punible la mera toma de contacto con el menor en internet con fines sexuales. En este tipo delictivo se incluyen elementos habituales como el hostigamiento, la intimidación, el abuso de poder, el engaño, así como el inevitable componente sexual en el que culmina el proceso.

En el Convenio del Consejo de Europa (CE) para la protección de los niños contra la explotación y el abuso sexual infantil, de 25 de octubre de 2007, también conocido como Convenio de Lanzarote[14], ya se empieza a hablar de este fenómeno y advertir de la necesidad de su legislación. De hecho, dentro de la normativa europea, existen disposiciones de lucha

12. La doctrina internacional también ha optado por otros términos tales como: *baby grooming, online child grooming, Internet child grooming, grooming virtual* o *grooming informático*.

13. PÉREZ FERNÁNDEZ, F. "El grooming como factor de impacto en tiempo de pandemia", *Diario La Ley*, N.º 9752, Sección Tribuna, 11 de diciembre de 2020, Wolters Kluwer.

14. En el Artículo 23 del mencionado Convenio se indica: "*Cada Parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito el hecho de que un adulto, mediante las tecnologías de la información y la comunicación, proponga un encuentro a un niño que no haya alcanzado la edad fijada en aplicación del apartado 2 del artículo 18 con el propósito de cometer contra él cualquiera de los delitos tipificados con arreglo al apartado 1.a del artículo 18 o al apartado 1.a) del artículo 20, cuando a dicha proposición le hayan seguido actos materiales conducentes a dicho encuentro*".

contra los delitos tecnológicos cometidos contra los menores de edad, especialmente cuando el adulto tenga intenciones de realizar actividades sexuales con un niño.

Esta conducta delictiva podría considerarse un derivado tecnológico de lo que tradicionalmente se conoce como "acoso", su variante cibernética sobre menores incluye elementos habituales como el hostigamiento, la intimidación, el abuso de poder, el engaño, que juega el papel fundamental en estos casos, así como el inevitable componente sexual en el que culmina el proceso.

En el Código Penal español, se tipifica esta conducta en el artículo 183 Bis[15], cuyo tenor literal es el siguiente: "*El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño*".

El uso del anglicismo "grooming" permite individualizar este delito y diferenciarlo de otros delitos que se producen en un contexto similar, como el ciberacoso y el sexting.

Por otro lado, estarían los delitos que más son cometidos por menores, sin que existan diferencias en este sentido entre España y Portugal.

El espacio criminógeno más habitual utilizado por los jóvenes son las Redes Sociales y las nuevas TICs (teléfonos móviles, tablets, etc.). Los delitos más frecuentes cometidos por estos menores son los que atentan contra la propiedad intelectual (piratería), la tranquilidad y la libertad (amenazas, injurias, calumnias, ciber acoso o ciber bullying y ciber acecho o ciber stalking), la intimidad (descubrimiento y revelación de secretos), y la indemnidad sexual (sexting).

15. El delito de *child grooming* fue introducido en el Código Penal español por la reforma operada por la Ley Orgánica 5/2010, de 22 de junio, como consecuencia de la firma y ratificación del Convenio de Lanzarote y de la previsible aprobación de la Directiva 2011/92/UE. La Ley Orgánica 1/2015, de 30 marzo, ha cambiado su ubicación sistemática y ha previsto algunos aspectos novedosos en el art. 183 *ter*. Concretamente, las modificaciones que ha llevado a cabo son las siguientes:
    1. La edad de la víctima, que se ha elevado de 13 a 16 años; y
    2. El fin o propósito perseguido por el autor (la comisión de determinados delitos), que ha pasado de efectuarse una remisión a los arts. 178 a 183 y 189, a una remisión más restringida de los delitos de los arts. 183 y 189.

Dentro de los anteriores, el ciberacoso entre menores o cyberbullying se define como "aquellas conductas agresivas repetidas en el tiempo, llevadas a cabo intencionadamente a través de dispositivos electrónicos, con la finalidad de agredir a una víctima que no puede defenderse fácilmente". Algunos autores consideran el cyberbullying como una mera extensión al mundo online del bullying (o acoso tradicional), mientras que otros lo entienden como un fenómeno en parte independiente.

No obstante, aunque el foco esté puesto en el acoso cibernético entre iguales en el colegio, conviene no olvidar que, cada vez con más frecuencia, los docentes también están siendo víctimas de tales conductas.

III. MEDIDAS IMPUESTAS POR LA COMISIÓN DE DELITOS INFORMÁTICOS

1. ORDENAMIENTO JURÍDICO ESPAÑOL

En cuanto a España, las medidas aplicables a menores infractores están enumeradas en el art. 7 de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores (en adelante, LORPM), primero de los que integran el Título II, en el que, bajo la rúbrica "de las medidas", se incluye un amplio catálogo de medidas, que oscilan entre la simple amonestación judicial y el internamiento en régimen cerrado.

El objetivo de dichas medidas responderá a la finalidad de resocialización y reeducación a través de la implementación de un proyecto educativo acorde al delito cometido, edad y circunstancias sociales y familiares, teniendo en cuenta la naturaleza sancionadora y especialmente educativa de la ley.

Además, con respecto al internamiento en centro de menores, debe destacarse que independiente de la naturaleza del delito que cometa el menor infractor, la imposición de esta medida, además de los requisitos legales para su imposición, que son de carácter flexible y atendiendo siempre al interés superior del menor recogido tanto en la LORPM como en el Real Decreto 1774/2004 por el que se aprueba su Reglamento, se tendrán en cuenta factores como su edad y sus circunstancias personales, sociales y familiares.

Asimismo, se concede una gran discrecionalidad al Juez para la elección de la medida o medidas a imponer, su sustitución, así como la suspensión de la ejecución del fallo contenido en la sentencia. En todo caso, la duración de las medidas privativas de libertad, esto es, las contempladas en las letras a), b), c), d) y g) del art. 7.1, no podrá exceder "*del tiempo que*

hubiera durado la pena privativa de libertad que se le hubiere impuesto por el mismo hecho, si el sujeto, de haber sido mayor de edad, hubiera sido declarado responsable, de acuerdo con el Código Penal" (art. 8, segundo párrafo).

En 2020 fueron condenados por sentencia firme 11.238 menores, según los datos procedentes del Registro Central de Sentencias de Responsabilidad Penal de los Menores, de los cuales, por amenazas 1711, coacciones 228, contra la intimidad y derecho a la propia imagen 171, contra la libertad e indemnidad sexuales 477. Las cifras de dicho año 2020, suponen un descenso del 20,4% respecto del año anterior, coincidiendo el descenso más acusado con los meses de confinamiento.

Igualmente, también ha descendido un 6,3% el número de adolescentes que han sido condenados por delitos sexuales. En total fueron 390 los condenados que cometieron 477 delitos, entre ellos siete considerados como violación, uno más que en 2019, y 47 por agresión sexual. Asimismo, 159 menores fueron condenados por abusos sexuales y 177 por abusos y agresiones sexuales a menores de 16 años. Por prostitución y corrupción menores los condenados fueron 56.

Según la Memoria de la Fiscalía de 2020, durante ese año disminuyeron las denuncias por acoso en el ámbito escolar sin que, paralelamente, aumentaran de modo significativo las denuncias por estos comportamientos en redes sociales.

La pandemia supuso un incremento de delitos contra la intimidad, especialmente el tipo del art. 197.7 CP, por difusión de material de contenido sexual. Si bien en adultos la difusión de imágenes de contenido sexual va asociada frecuentemente a una ruptura de pareja, entre menores se toma como "un puro juego", pues se facilitan imágenes sin relación previa sentimental alguna. Estamos hablando de menores de 12 o 13 años asumen esas conductas sin llegar a percibir sus riesgos.

2. ORDENAMIENTO JURÍDICO PORTUGUÉS

Las estadísticas portuguesas van a la par que las españolas en cuanto a tipos de ciberdelitos cometidos por menores, concentrándose el mayor número en los delitos de ciberacoso, amenazas, contra la propia imagen y contra la indemnidad sexual.

Igualmente, la Memoria del Ministerio Público portugués de 2020, en materia de menores, también pone el foco sobre los delitos en el medio escolar y practicados en el ambiente digital, lo que le ha llevado a implementar programas de prevención como son:

el proyecto impulsado por el Gabinete da Familia, da Criança e do Jovem denominado "*Os teus direitos no ambiente digital*"[16], como una serie de orientaciones del Consejo de Europa para respetar, proteger y concretizar los derechos del menor en el ambiente digital de una forma clara y un lenguaje dirigido a estos menores a fin de que puedan identificar los riesgos.

Por otro lado, destaca también el proyecto "*Tu e a internet*"[17] elaborado Gabinete Cibercrime da Procuradoria-Geral da República, con la finalidad de explicar a los menores los tipos de delitos informáticos, que existen según el Código Penal portugués.

Antes de analizar las concretas medidas impuestas a los menores condenados por ciberdelitos en Portugal, es preciso analizar la regulación de la responsabilidad penal del menor en Portugal, que se instrumenta mediante la Lei Tutelar Educativa (en adelante, LTE)[18], cuyo ámbito de aplicación se concentra en los menores entre 12 y 16 años que cometan un hecho calificado por la ley como crimen, que evidencie la necesidad de que el menor sea "*educado para el derecho*"[19], lo que dará lugar a la aplicación de la medida tutelar educativa que corresponda según lo dispuesto en la propia ley[20].

En este punto, es preciso destacar que, en el ordenamiento jurídico portugués, el concepto de "*criminalidade juvenil*" hace referencia, en realidad, a una criminalidad cometida por adultos, toda vez que los jóvenes de edad igual o superior a16 años son juzgados como adultos en virtud de la ley penal, es decir, que la mayoría de edad penal en Portugal se sitúa en los 16 años[21]. Por otro lado, en lo que respecta al sistema de justicia juvenil para menores inimputables (entre los 12 y los 16 años), el término adecuado sería "*delinquencia juvenil*"[22].

16. www.coe.int/children.
17. https://www.ministeriopublico.pt/.
18. Lei núm. 166/99 – Diário da República núm. 215/1999, Série I-A de 1999-09-14.
19. Véase: *Educar para o direito: uma forma de (também) proteger, Guião de Procedimentos de Comunicação*, elaborada por el *Gabinete da Familia, da Criança e do Jovem del Ministerio Público* (https://www.ministeriopublico.pt/sites/default/files/documentos/pdf/educar_para_o_direito_guiao_de_procedimentos_de_comunicacao.pdf).
20. Artículo 1 de la Lei Tutelar Educativa*: âmbito da lei*.
21. En Portugal, son considerados inimputables los adolescentes entre 12 y 16 años, conforme a la *Lei Tutelar Educativa* (Ley núm. 4, de 15 de enero de 2015, primera reforma de la Ley núm. 166/99, de 14 de septiembre de 1999). Asimismo, existe un régimen penal especial para jóvenes adultos, así consideradas las personas entre 16 y 21 años, de conformidad con lo previsto en el *Decreto-lei núm. 401*, de 23 de septiembre de 1982.
22. LEOTE DE CARVALHO, M. J., "Reflexões e debates emergentes sobre justiça juvenil", *DESIDADES: Revista Científica da Infância, Adolescência e Juventude*, Núm. 29, 2021, pp. 259-274.

La LTE, partiendo del principio de legalidad establece en su artículo 4.º las medidas tutelares educativas que pueden ser impuestas al menor, distinguiéndose aquellas que suponen una privación de libertad y, por tanto, que revisten de especial gravedad: el internamiento en un centro educativo, en régimen abierto, semiabierto y cerrado. Los artículos 9 a 18, establecen las bases mínimas del contenido de cada una de estas medidas, dejando al arbitrio del juez[23] el contenido concreto de las mismas, de acuerdo con la necesidad educativa de cada menor infractor.

Trasladando este articulado al sistema penal del menor español, se puede determinar que las medidas de privación de libertad aplicadas en Portugal tienen su homólogo en las medidas establecidas en la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores, que en su artículo 7 y ordenadas de mayor a menor restricción de derechos, distingue también en internamiento en régimen, cerrado, semiabierto y abierto[24].

La principal diferencia entre ambos ordenamientos jurídicos es el ámbito de aplicación de la ley que contempla la responsabilidad penal del menor. Pues tal y como establece el artículo 1 de la citada Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los

23. En Portugal, la intervención tutelar educativa es competencia de los *Tribunais de Familia e Menores*, a los que compete en exclusiva la verificación de los presupuestos que justifican y fundamentan la aplicación de medidas tutelares necesarias y adecuadas a la educación de los jóvenes para el respeto del derecho y su inserción de forma digna y responsable en la vida en comunidad. El Ministerio Público, junto con el *Tribunal de Família e Criança* ordenará la instrucción del procedimiento (*inquérito tutelar educativo*).

24. *Artículo 7: "Definición de las medidas susceptibles de ser impuestas a los menores y reglas generales de determinación de las mismas:*

1. Las medidas que pueden imponer los Jueces de Menores, ordenadas según la restricción de derechos que suponen, son las siguientes:

a) Internamiento en régimen cerrado. Las personas sometidas a esta medida residirán en el centro y desarrollarán en el mismo las actividades formativas, educativas, laborales y de ocio.

b) Internamiento en régimen semiabierto. Las personas sometidas a esta medida residirán en el centro, pero podrán realizar fuera del mismo alguna o algunas de las actividades formativas, educativas, laborales y de ocio establecidas en el programa individualizado de ejecución de la medida. La realización de actividades fuera del centro quedará condicionada a la evolución de la persona y al cumplimiento de los objetivos previstos en las mismas, pudiendo el Juez de Menores suspenderlas por tiempo determinado, acordando que todas las actividades se lleven a cabo dentro del centro.

c) Internamiento en régimen abierto. Las personas sometidas a esta medida llevarán a cabo todas las actividades del proyecto educativo en los servicios normalizados del entorno, residiendo en el centro como domicilio habitual, con sujeción al programa y régimen interno del mismo".

menores, ésta se aplicará para exigir la responsabilidad de las personas mayores de 14 años y menores de 18 por la comisión de hechos tipificados como delitos o faltas en el Código Penal o las leyes penales especiales.

La medida tutelar educativa portuguesa consistente en el internamiento en centro educativo tiene como objetivo proporcionar al joven, por medio del alejamiento temporal de su medio habitual y de la utilización de programas y métodos pedagógicos, la interiorización de valores conformes al derecho y la adquisición de recursos que le permitan, en el futuro, conducir su vida de un modo social y jurídicamente responsable.

El régimen abierto será de aplicación en el caso de que el menor haya cometido hechos tipificados como crímenes menos graves, siendo la duración mínima de la medida de 6 meses y máxima de 2 años. En este régimen, los jóvenes residen en el centro educativo, pero frecuentan, preferencialmente en el exterior, las actividades formativas y socioeducativas. De acuerdo con la evaluación de su comportamiento, el menor podrá ser autorizado a salir, sin acompañamiento y pasar fines de semana y festivos con los progenitores, representante legal o persona que tenga atribuida su guarda de hecho.

Por su parte, el régimen semiabierto está reservado a aquellos hechos tipificados por la ley penal portuguesa como delitos contra las personas o en aquellos casos en los que el menor cometa dos hechos o más calificados como delitos a los que les corresponda lo que se denomina "*pena máxima*", esto es, superior a 3 años. La duración mínima de la medida también será de 6 meses y la máxima de 2 años.

Se diferencia del régimen abierto en cuanto a que el menor realizará sus actividades formativas y educativas en el centro y las salidas, sin acompañamiento y los permisos de fines de semana y festivos con los progenitores, representante legal o persona que tenga atribuida su guarda de hecho se supeditan a la evolución positiva del comportamiento del menor.

Finalmente, para la aplicación de la medida de internamiento en régimen cerrado, deben cumplirse los siguientes presupuestos: el haber cometido un hecho tipificado por la ley penal como delito al que le corresponda una pena máxima de prisión superior a 5 años o haber cometido dos o más hechos calificados como delitos contra las personas cuya pena sea superior a tres años. Además, el menor deberá contar con una edad igual o superior a 14 años en el momento de comisión de los hechos.

En este caso, la medida de internamiento tendrá una duración mínima de 6 meses y máxima de 3 años.

El menor reside en el centro y es allí donde realiza todas sus actividades formativas y socioeducativas, quedando reservadas las salidas (siempre con acompañamiento) al cumplimiento de obligaciones judiciales, necesidades de salud o motivos excepcionales.

El Estado portugués cuenta con estadísticas mensuales[25] procedentes de los centros educativos, elaboradas por la *Direçao Geral de Reinserçao e Serviços Prisionais (DGRSP)*[26], del Ministerio de Justicia, que arrojan información detallada sobre la situación de los menores internos: nacionalidad, edad, género, tipología del delito cometido,

En el informe más reciente (diciembre de 2021), que engloba los datos de todo el año y realiza una comparativa con los años anteriores) se pueden destacar dos cuestiones:

En primer lugar, con respecto al número de menores internos, cabe destacar que, en dicho año, se encontraban internos un total de 150 menores. No obstante, resulta necesario relacionar esta cifra con el cómputo total de medidas tutelares educativas impuestas en el año inmediatamente anterior (2020).

De los *inquéritos* o procesos instruidos en los que se declaró la apertura de la fase jurisdiccional por parte del Ministerio Público (un total de 869), fueron archivados 45 conforme el artigo 93.º, núm. 1, al. b), de la LTE una cifra de 45 y requirieron la aplicación de una medida no institucional un total de 708 (23 de amonestación, 163 de prestación de servicios a favor de la comunidad, 272 de acompañamiento educativo y 250 otras medidas) y de una medida privativa de libertad un total de 116 (16 de internamiento

25. *Relatorios de estatística mensal dos centros educativos*, publicados por el *Centro de Competências de Comunicação e Relações Externas da Direçao Geral de Reinserçao* e Serviços Prisionais, *Ministerio de Justiça*.

26. Organismo resultante de la fusión de la *Direção-Geral dos Serviços Prisionais* y la *Direção Geral de Reinserção Social*, conforme lo dispuesto en el *Decreto-Lei* n.º 123/2011, de 29 de diciembre.

Su estructura orgánica se establece en el *Decreto-Lei* núm. 215/2012, de 28 de septiembre, complementado por la *Portaria* núm. 300/2019, de 11 de septiembre, en la que se define la estructura nuclear y las competencias de las respectivas unidades orgánicas.

La DGRSP se estructura en unidades orgánicas cuyas atribuciones se centran en la ejecución de penas y medidas, en el ámbito penal y tutelar educativo, correspondientes a servicios centrales y descentralizados, siendo éstos los constituidos por establecimientos prisionales, delegaciones regionales de reinserción, que integran los equipos de reinserción social, equipos de vigilancia electrónica y centros educativos. Integran el área operativa las unidades orgánicas cuya actividad se asienta en la fase de ejecución de penas y medidas, privativas de la libertad o de ejecución en la comunidad, de forma directa (establecimientos prisionales, equipos de reinserción social y de vigilancia electrónica, centros educativos) o indirecta (apoyo técnico a la actividad operativa, funciones de coordinación, monitorización y evaluación). Dispone además de un conjunto de unidades instrumentales que apoyan el desarrollo de la actividad operativa.

en régimen abierto, 88 de internamiento en régimen semiabierto y 12 de internamiento en régimen cerrado)[27].

Estos datos permiten apreciar como la justicia juvenil portuguesa ha ido tendiendo hacia la limitación de las medidas tutelares educativas privativas de libertad, partiendo del principio de última ratio en la imposición de este tipo de medidas por parte de los jueces de menores[28].

El segundo dato relevante es la edad de los menores. Así, el porcentaje de menores internos con edades de 16 y 17 años es el más alto (en torno a un 35%).

Por otro lado, en cuanto a la tipología de delitos por los que los menores se encuentran cumpliendo la medida de internamiento: el mayor porcentaje (56, 46%) se concentra en los delitos contra las personas y el 37, 36% contra el patrimonio.

Dentro de los delitos contra las personas, durante el año 2021 se ha visto un aumento de menores internos condenados por delitos relacionados con amenazas, coacciones, injurias y calumnias, especialmente en el ámbito escolar y también por medios informáticos. De los 201 internos, 87 lo fueron por este motivo.

Sin embargo, se aprecia también un número muy reducido de los menores internos por motivo de otros delitos cometidos a través de medios informáticos, como el delito conocido como "*devassa por meio de informática*[29]" (fraude informático) (únicamente 2 menores internos por este motivo) o el delito de "*burla informática e nas comunicações*"[30] (únicamente 3 menores).

---

27. Datos extraídos del *Relatório de Síntese do Ministério Público de Portugal, Procuradoria-Geral da República* (www.ministeriopublico.pt), año 2020.

28. La propia Exposición de Motivos de la *Lei Tutelar Educativa* en su apartado 7 ya declara que el primer principio que inspira esta Ley es el de intervención mínima y añade, en relación con los presupuestos de la intervención tutelar educativa, que "*el primer presupuesto es el de la existencia de una ofensa a bienes jurídicos fundamentales, traducido en la comisión de un hecho considerado por la ley como crimen* (…). *Por otro lado –es este el segundo presupuesto–, siendo la finalidad de la intervención tutelar la educación del menor para el derecho y no la retribución por el crimen, no podrá aplicarse medida tutelar sin que se aprecie, en el caso concreto, la necesidad de corregir la personalidad del menor en el plano del deber-ser jurídico manifestada en la práctica del hecho*".

29. Contemplado en el artículo 193 del Código Penal portugués:
"1 – Quem criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica, é punido com pena de prisão até dois anos ou com pena de multa até 240 dias".

30. Contemplado en el artículo 221 del Código Penal portugués:
"1 – Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, mediante interferência no resultado de tratamento de

Esto nos lleva concluir, que existe un aumento real de los delitos contra las personas, especialmente amenazas y coacciones cometidos por menores en el ámbito escolar y muchos de ellos a través de las TIC, que llevan a la imposición de medidas de privación de libertad, pero paralelamente también se aprecia en las estadísticas del Ministerio Público, un aumento de la imposición de medidas de otro tipo como el acompañamiento educativo.

Esta medida se engloba dentro de las medidas no institucionales o no privativas de libertad y dentro de las mismas, se califica como la medida más gravosa o limitativa de la autonomía, debiendo dirigirse contra aquellos jóvenes con mayores necesidades de educación para el derecho o que presentan un riesgo de reincidencia general moderado o alto.

El contenido de la misma se establece en el artículo 16 de la LTE que lo define como la ejecución de un proyecto educativo personal (PEP), específico e individualizado para cada menor, que se implanta con la finalidad de reeducación y corrección en derecho.

Se elabora por los servicios de Reinserción Social, quienes también se encargarán de velar por su cumplimiento, junto con la participación del propio menor y sus progenitores o representantes legales, abarcando todas aquellas áreas de intervención fijadas por el Tribunal.

La duración mínima es de 3 meses y la máxima de 2 años, durante los cuales se acompañará el PEP con programas formativos y con un seguimiento pormenorizado de la vida social, familiar y educativa del menor, a través de entrevistas periódicas con éste y con su entorno familiar y escolar.

Finalmente, es preciso destacar que en Portugal se han hecho varios estudios sobre la reincidencia de menores[31], tras el cumplimiento de este tipo de medidas de acompañamiento educativo y también aplicables a

dados, estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.

2– A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações".

31. Véase, por ejemplo: *Avaliação do percurso dos jovens após a cessação da medida tutelar de internamento: Follow-up* Instituto de Reinserção Social, Lisboa o el *Estudo eficácia de Medidas. Relatório do 3.º Momento de Avaliação (2 anos follow-up pós termo de medida)*, elaborado por el Centro de Investigação em Psicologia (CIPSI), Escola de Psicologia de la Universidade do Minho.

los delitos informáticos, que son muy positivos, por cuanto muestran un porcentaje general muy bajo de reincidencia, destacando la eficacia y la obtención de resultados satisfactorios tras aplicar este tipo de medidas de acompañamiento educativo frente a la comisión de tipos delictivos relacionados con el ciberacoso y las amenazas y coacciones en el ámbito educativo.

Capítulo 20

La facultad moderadora de la responsabilidad civil en el proceso penal de menores por delitos cometidos a través de internet[1]

Tomás Farto Piay

Profesor Ayudante Doctor de Derecho Procesal
Universidad de Vigo

I. INTRODUCCIÓN

La generalización del uso de las nuevas tecnologías y las herramientas vinculadas a éstas en nuestra sociedad es un fenómeno que, evidentemente, no resulta ajeno a los jóvenes, sino que, por el contrario, es parte indisoluble de su proceso formativo, social y vital.

Las indudables ventajas de la digitalización, del uso de internet, de las TIC y de las redes sociales, que se han convertido, sin duda, en indispensables, conllevan, por otro lado, y de forma inherente, el aumento de la comisión de ilícitos penales derivados, vinculados o con ocasión de su utilización. Es notorio el aumento de los ciberdelitos, delitos informáticos o de los delitos cometidos a través de internet, y, en consecuencia, el incremento en la comisión de tales hechos delictivos entre nuestros jóvenes[2]. Delitos de los que, en su caso, emana la correspondiente responsabilidad

1. Este trabajo ha sido elaborado en el marco del proyecto de investigación "Respuesta jurídica y socioeducativa a la violencia de género ejercida por menores. Protección de la víctima e intervención con el menor agresor", subvencionado por el Ministerio de Ciencia e Innovación, Proyectos de I+D+I dentro de los Programas Estatales de Generación de Conocimiento y Fortalecimiento Científico y Tecnológico del Sistema de I+D+I y de I+D+I orientada a los Retos de la Sociedad en la convocatoria de 2019, (Ref. PID2019-106700RB-I00).

2. La Circular FGE 9/2011, de 16 de noviembre, sobre criterios para la Unidad de Actuación Especializada del Ministerio Fiscal en materia de Reforma de Menores, advertía

civil que, en muchas ocasiones, puede adquirir una magnitud muy considerable.

Entre los delitos de comisión más frecuente a través de internet, sin ánimo de exhaustividad, pueden citarse los delitos contra el patrimonio y el orden socioeconómico, como estafas cometidas a través del denominado *phishing*, u otros como los delitos de daños informáticos. Asimismo, cabe destacar los delitos contra la intimidad y el derecho a la propia imagen, como el delito de revelación y descubrimiento de secretos; delitos contra la integridad moral, como el acoso o *stalking*; o los delitos contra el honor, injurias y calumnias, delitos que, en multitud de ocasiones, son cometidos a través de las redes sociales, con la difusión que ello supone.

Pues bien, en relación con los delitos cometidos por los jóvenes mayores de catorce años y menores de dieciocho, es la Ley Orgánica 5/2000, de 12 de enero, Reguladora de la Responsabilidad Penal de los Menores (en lo sucesivo LORPM), la norma que se ocupa de regular su responsabilidad penal, con unas previsiones específicas en materia de responsabilidad civil *ex delicto*.

En este sentido, sin perjuicio de la respuesta sancionadora-educativa que propugna la LORPM, lo cierto es que los hechos delictivos cometidos por el menor generan la obligación de reparación o indemnización de los daños y perjuicios que, en su caso, se hubiesen causado. Esto es, la obligación de hacer frente a la responsabilidad civil derivada del delito para reparar o resarcir a la víctima o perjudicado. Esta responsabilidad civil del menor infractor, y de los demás responsables que deberán responder con éste, se encuentra regulada en los art. 61 a 64 LORPM, con una previsión expresa relativa a la facultad de moderación de la responsabilidad civil de los responsables solidarios, prevista en el art. 61.3 LORPM.

II. LA RESPONSABILIDAD CIVIL EN LA LORPM

1. CUESTIONES PRELIMINARES

El art. 19 CP dispone que los menores de dieciocho años no serán responsables criminalmente con arreglo al CP, de forma que "cuando un menor de dicha edad cometa un hecho delictivo podrá ser responsable con arreglo a lo dispuesto en la ley que regule la responsabilidad penal del menor", dicha normativa ha sido materializada en la LORPM[3].

---

de manifestaciones delictivas que son reflejo de fenómenos como la utilización de Internet y las nuevas tecnologías para la comisión o difusión de delitos.

3. El apartado 4 de la Exposición de Motivos de la LORPM se refiere al art 19 CP, precepto que fija la mayoría de edad penal en los dieciocho años y exige la regulación

Así, el art. 1.1 LORRPM dispone su aplicación "para exigir la responsabilidad de las personas mayores de catorce años y menores de dieciocho por la comisión de hechos delictivos tipificados como delitos o faltas (*ahora delitos leves*) en el Código Penal o las leyes especiales". De este modo, como sujetos pasivos del ámbito de la LORPM quedan excluidos tanto los menores de 14 años, como prevé expresamente el art. 3 LORPM, por ser inimputables penalmente, como los mayores de 18 años de edad[4].

En este orden de cosas, partiendo de la premisa general de que, según se desprende de los arts. 109 y 116.1 CP, toda persona criminalmente responsable de un delito lo es también civilmente si del hecho se derivan daños y perjuicios, con la obligación de reparación, lo cierto es que el menor infractor que resulte penalmente condenado queda afectado por la obligación de responder civilmente de los daños y perjuicios irrogados por el ilícito penal cometido, disponiendo el art 61.3 LORPM que cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho.

2. RÉGIMEN LEGAL

La LORPM dedica su Título VIII, integrado por los arts. 61 a 64, a la regulación de la responsabilidad civil. Así, dentro de las reglas generales que establece el art. 61, su apartado 1 dispone que la acción para exigir

---

expresa de la responsabilidad penal de los menores de dicha edad en una Ley independiente. Asimismo advierte que la responsabilidad penal de los menores precisa de otro límite mínimo a partir del cual comience la posibilidad de exigir esa responsabilidad y que se ha concretado en los catorce años, con base en la convicción de que las infracciones cometidas por los niños menores de esta edad son en general irrelevantes y que, en los escasos supuestos en que aquéllas pueden producir alarma social, son suficientes para darles una respuesta igualmente adecuada los ámbitos familiar y asistencial civil, sin necesidad de la intervención del aparato judicial sancionador del Estado.

4. En relación a ello, advertir que aún cuando el art. 69 CP señala que "al mayor de dieciocho años y menor de veintiuno que cometa un hecho delictivo, podrán aplicársele las disposiciones de la ley que regule la responsabilidad penal del menor en los casos y con los requisitos que ésta disponga" lo cierto es que la posibilidad de aplicar dicho precepto fue suprimida por LO 8/2006, de 4 de Diciembre, por la que se modificó la LO 5/2000, quedando el art. 69 CP sin efecto y, en consecuencia, la LORPM no es aplicable a personas de entre 18 y 21 años. Así, la STS 438/2021, de 20 de mayo, señala que "la LO 8/2006, de 12-1, Reguladora de la Responsabilidad Penal de los Menores, suprimió definitivamente la posibilidad de aplicar la LO 5/2000 a los comprendidos entre 18 y 21 años, a partir de su entrada en vigor, el 6-2-2007. Así, el art. 1 de esta Ley Orgánica, circunscribe su objeto de aplicación a los menores de 18 años. Por tanto, el art. 69 CP quedó sin efecto". En el mismo sentido, la STS 11/2016, de 21 de enero.

la responsabilidad civil se ejercitará por el Ministerio Fiscal, salvo que el perjudicado renuncie a ella, la ejercite por sí mismo en el plazo de un mes desde que se le notifique la apertura de la pieza separada de responsabilidad civil o se la reserve para ejercitarla ante el orden jurisdiccional civil conforme a los preceptos del Código Civil y de la Ley de Enjuiciamiento Civil.

Asimismo, el art. 61.2 prevé la tramitación de una pieza separada de responsabilidad civil por cada uno de los hechos imputados, previendo el apartado 4 del precepto la aplicación, en su caso, de lo dispuesto en el art. 145 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, remisión que habrá de entenderse referida al art. 36 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público por derogación del anterior, y en la Ley 35/1995, de 11 de diciembre, de ayudas y asistencia a las víctimas de delitos violentos y contra la libertad sexual, y sus disposiciones complementarias.

Por su parte, el art. 61.3 LORPM, además de establecer que responderán solidariamente con el menor sus padres, tutores, acogedores y guardadores legales o de hecho, prevé la posibilidad de que su responsabilidad pueda ser moderada por el Juez, según los casos, cuando aquellos no hubieren favorecido la conducta del menor con dolo o negligencia grave, de suerte que contempla la facultad moderadora del órgano judicial de la responsabilidad civil de los obligados solidarios con el menor infractor.

En cuanto a la extensión de la responsabilidad civil el art. 62 LORPM se remite a la regulación prevista en el capítulo I del Título V del Libro I CP, esto es, a los arts. 109 a 115 del texto penal sustantivo, por lo que la responsabilidad civil comprenderá la restitución, la reparación del daño y la indemnización de perjuicios, tanto materiales como morales.

El art. 63 LORPM prevé la responsabilidad civil directa de los aseguradores hasta el límite de la indemnización legalmente establecida o convencionalmente pactada, sin perjuicio de su derecho de repetición contra quien corresponda[5].

Por último, a modo de cierre del Título VIII LORPM, el art. 64 establece unas reglas de procedimiento en la tramitación para la exigencia de

5. Es un precepto de similar alcance al art. 117 CP, que señala que "Los aseguradores que hubieren asumido el riesgo de las responsabilidades pecuniarias derivadas del uso o explotación de cualquier bien, empresa, industria o actividad, cuando, como consecuencia de un hecho previsto en este Código, se produzca el evento que determine el riesgo asegurado, serán responsables civiles directos hasta el límite de la indemnización legalmente establecida o convencionalmente pactada, sin perjuicio del derecho de repetición contra quien corresponda".

la responsabilidad civil[6]: 1.ª Tan pronto como el Juez de Menores reciba el parte de la incoación del expediente por el Ministerio Fiscal, ordenará abrir de forma simultánea con el proceso principal una pieza separada de responsabilidad civil, notificando el secretario judicial a quienes aparezcan como perjudicados su derecho a ser parte en la misma, y estableciendo el plazo límite para el ejercicio de la acción; 2.ª En la pieza de referencia, que se tramitará de forma simultánea con el proceso principal, podrán personarse los perjudicados que hayan recibido notificación al efecto del Juez de Menores o del Ministerio Fiscal, conforme establece el art. 22, y también espontáneamente quienes se consideren como tales. Asimismo, podrán personarse las compañías aseguradoras que se tengan por partes interesadas, dentro del plazo para el ejercicio de la acción de responsabilidad civil. En el escrito de personación, indicarán las personas que consideren responsables de los hechos cometidos y contra las cuales pretendan reclamar, bastando con la indicación genérica de su identidad; 3.ª El secretario judicial (ahora LAJ) notificará al menor y a sus representantes legales, en su caso, su condición de posibles responsables civiles; 4.ª Una vez personados los presuntos perjudicados y responsables civiles, el Juez de Menores resolverá sobre su condición de partes, continuándose el procedimiento por las reglas generales; 5.ª La intervención en el proceso a los efectos de exigencia de responsabilidad civil se realizará en las condiciones que el Juez de Menores señale con el fin de preservar la intimidad del menor y que el conocimiento de los documentos obrantes en los autos se refiera exclusivamente a aquellos que tengan una conexión directa con la acción ejercitada por los mismos.

Ciertamente, tras la reforma operada en la LORPM por la LO 8/2006 estas previsiones sobre la incoación y tramitación de la pieza de responsabilidad civil han quedado limitadas a la determinación, en su caso, de las posibles partes civiles. En tal sentido, el sistema previsto inicialmente en la LORPM se ha modificado toda vez que, a diferencia del régimen anterior, tras la LO 8/2006 el régimen legal del proceso penal de menores prevé el ejercicio acumulado de las pretensiones penales y civiles de manera conjunta y que serán decididas en la misma sentencia[7].

Es así, en relación con lo expresado, además de las citadas previsiones la LORPM contiene otras disposiciones que afectan y guardan relación

6. *Vid.* GARCIANDÍA GONZÁLEZ, P. M., "Tratamiento procesal de la responsabilidad civil en el proceso penal de menores tras la reforma de 2006: reflexiones a la luz de la Circular de la Fiscalía General del Estado 1/2007, de 26 de noviembre", *REDUR*, núm. 5, 2007, pp. 33-38.

7. Sobre este tema, *vid.* GUZMÁN FLUJA, V., "Responsabilidad civil en el proceso penal de menores", en GONZÁLEZ PILLADO, E. (Coord.), *Proceso penal de Menores*, Tirant lo Blanch, Valencia, 2009, pp. 318-330.

con la responsabilidad civil y con su exigencia o a efectos de su determinación en el proceso penal de menores.

De entre ellas, procede destacar que el art. 4 LORPM, relativo a los derechos de las víctimas y de las personas perjudicadas, establece el derecho de éstas a personarse y ser parte en el expediente, a cuyo fin el LAJ les informará según lo previsto en los arts. 109 y 110 LECrim, así como de su derecho a nombrar dirección letrada o instar su nombramiento de oficio en caso de ser titulares del derecho a la asistencia jurídica gratuita. Asimismo, se les informará de que, de no personarse ni hacer renuncia ni reserva de acciones civiles, el Ministerio Fiscal las ejercitará si correspondiere. Una vez personadas, prevé el precepto que podrán tomar conocimiento de lo actuado e instar la práctica de diligencias y cuanto a su derecho convenga.

En cuanto al procedimiento previsto en la LORPM, por su incidencia en cuanto a la responsabilidad civil, destacar el art. 31 que prevé que una vez recibido el escrito de alegaciones, o acusación, del MF el Juez de Menores procederá a abrir el trámite de audiencia, para lo cual se dará traslado simultáneamente a quienes ejerciten la acción penal y la civil para que en un plazo común de cinco días hábiles formulen sus respectivos escritos de alegaciones y propongan las pruebas que consideren pertinentes.

Una vez evacuado el trámite de alegaciones de las acusaciones, el art. 31 LORPM dispone que el LAJ dará traslado de todo lo actuado al letrado del menor y, en su caso, a los responsables civiles, para que en un plazo de cinco días hábiles formule a su vez escrito de alegaciones y proponga la prueba que considere pertinente.

Asimismo, en cuanto a la sentencia que se dicte, si existe conformidad del menor y su letrado, así como de los responsables civiles, la cual se expresará en comparecencia ante el Juez de Menores, se dictará sentencia sin más trámite, si bien si no existiese conformidad con la responsabilidad civil, sea por el menor y su letrado o la persona o personas contra quienes se dirija la acción civil, se sustanciará el trámite de la audiencia practicándose la prueba propuesta sólo en lo relativo a esta cuestión (arts. 32 y 36.4 LORPM).

La sentencia, como prevé el art. 39 LORPM, resolverá sobre la responsabilidad civil derivada del delito, con el contenido indicado en el art. 115 CP, es decir, estableciendo razonadamente las bases en que se fundamenta la cuantía de los daños e indemnizaciones, pudiendo fijarla en la propia resolución o en el momento de su ejecución[8]. Hay que reseñar, en este

8. La Circular FGE 9/2011, de 16 de noviembre, sobre criterios para la unidad de actuación especializada del Ministerio Fiscal en materia de reforma de menores advierte

punto, que el derecho a la presunción de inocencia no opera en sede de responsabilidad civil puesto que la petición de indemnización mantiene su naturaleza estrictamente civil aun cuando se determine en el juicio penal, de forma que el principio de presunción de inocencia es aplicable exclusivamente en el ámbito del proceso penal en la formulación del juicio sobre la culpabilidad o inocencia[9].

3. RESPONSABILIDAD SOLIDARIA

El art. 61.3 LORPM dispone que "cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho, por este orden. Cuando éstos no hubieren favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el Juez según los casos". De esta forma, se viene a establecer una responsabilidad solidaria de los sujetos obligados por el precepto con el menor infractor, solidaridad que se refrenda en el apartado 8 de la Exposición de Motivos de la ley al advertir que, en atención a los intereses y necesidades de las víctimas, se "introduce el principio en cierto modo revolucionario de la responsabilidad solidaria con el menor responsable de los hechos de sus padres, tutores, acogedores o guardadores, si bien permitiendo la moderación judicial de la misma"[10].

Se trata, en consecuencia, de una responsabilidad solidaria, si bien ello resulta, en parte, modulado por la facultad judicial de moderación de la responsabilidad civil[11].

---

que "resulta posible diferir para la fase de ejecución la determinación de la cuantía concreta de la indemnización. Ello no obstante, es necesario fijar en la sentencia las bases para la determinación de esa cuantía".

9. STC 30/1992, de 18 de marzo; SSTS 925/2021, de 25 de noviembre; 168/2020 de 19 de mayo; 302/2017, de 27 de abril; 639/2017, de 28 de septiembre.

10. Sobre la responsabilidad civil en el proceso penal de menores, *vid.* BONILLA CORREA, J., *La responsabilidad civil ante un ilícito penal cometido por un menor. Aspectos sustantivos*, Tirant lo Blanch, Valencia, 2009, pp. 195-235; DE LA ROSA CORTINA, J. M., *Responsabilidad civil por daños causados por menores. Aspectos sustantivos y procesales*, Tirant lo Blanch, Valencia, 2012, pp. 37-68; DOLZ LAGO, M. J., "La responsabilidad civil derivada del delito en la LORPM seminario de especialización en menores: protección y reforma", 2013, pp. 10-14 (http://cej-mjusticia.es, última consulta: 11/06/2022); YZQUIERDO TOLSADA, M. M. "¿Por fin menores civilmente responsables? reflexiones a propósito de las reformas de 2015", *Foro: Revista de ciencias jurídicas y sociales*, Vol. 19, núm. 2, 2016, pp. 46-48; GUZMÁN FLUJA, V., "Responsabilidad civil…", pp. 297-310; PAÑOS PÉREZ, A., *La responsabilidad civil de los padres por daños causados por menores e incapacitados*, Atelier, Barcelona, 2010, pp. 148-165.

11. En este sentido, BONILLA CORREA (*La responsabilidad civil ante un ilícito…*, *op. cit.*, pp. 206-207) expone que se trata de determinar si, en caso de varios responsables

Como obligación solidaria, el acreedor resulta legitimado para reclamar el cumplimiento íntegro a cualquiera de los obligados y, en consecuencia, cada uno de los deudores solidarios deviene obligado al pago, sin perjuicio, en principio, del derecho del deudor que haya satisfecho la responsabilidad civil a reclamar del resto la parte que le corresponda a cada uno de ellos en vía de regreso. Ahora bien, esta premisa general referida al ejercicio de la acción de regreso propia de las obligaciones solidarias genera no pocos problemas de interpretación en relación al art. 61.3 LORPM y a cuál ha de ser la normativa de aplicación en el proceso civil en el que se ejercita la citada acción[12].

Asimismo, puede señalarse que se trata de una responsabilidad de carácter objetivo, o cuasi-objetivo[13], pues tal naturaleza también resulta matizada por la posibilidad de moderación de la responsabilidad *ex* art. 61.3 LORPM, en caso de que no se hubiese favorecido la conducta del menor con dolo o negligencia grave[14].

---

solidarios, la solidaridad alcanza a todos parta responder de forma conjunta y por igual cuantía, o, por el contrario, es posible la moderación de forma independiente. Y señala el autor que en estos supuestos la solidaridad quiebra por la facultad de moderación, el introducir el factor de culpa para fijar y modificar la cuantía hace que, con base en esta culpa, que no tiene que ser igual en ambos, se pueda moderar más o menos la cantidad por la que deba responder el responsable solidario, que, para el caso en que sean dos, pensemos en padres o tutores, la cuantía, en atención a esa culpa, podría ser diferente. En este caso, la solidaridad existirá respecto de la cantidad a que haya sido condenado el progenitor que menos culpa o negligencia haya tenido, respecto del resto no hay solidaridad, y esto afectará no sólo a las relaciones internas, sino también a la relación externa, incluso con el propio perjudicado. Esto supone fraccionar la responsabilidad civil en aquellos casos en que la conducta de las diferentes personas a responder haya sido diferente; existiendo solidaridad en aquella cantidad en la que ambos responden de igual manera, y respecto del exceso de cantidad de la que deba responder uno sólo por una mayor culpa por su parte la responsabilidad no será solidaria con respecto del otro cónyuge, sino sólo respecto de con el menor.

12. DE LA ROSA CORTINA, J. M., *Responsabilidad civil por daños…, op. cit*., pp. 450-451.
13. La SAP Alicante 41/2017, de 6 de febrero, señala que "la responsabilidad de los padres puede calificarse de cuasi-objetiva. A ellos corresponderá, por tanto, justificar los motivos en que se sustenta la solicitud de moderación". La SAP Madrid 158/2021 de 7 de mayo se refiere a un sistema cuasi-objetivo.
14. DOLZ LAGO ("La responsabilidad civil derivada del delito…", *op. cit*., pp. 10-14) considera que "esta responsabilidad tiene un carácter objetivo y quiebra el principio de culpabilidad civil o penal, sustrato de toda responsabilidad civil, en nuestro ordenamiento jurídico (art. 1.902 del CC y arts. 109 a 126 del CP, en especial, art. 116). Incluso el art. 1903 del Código Civil, que sanciona la responsabilidad por actos de aquellas personas de quienes se debe responder (v.gr. hijos), declara exenta esta responsabilidad 'cuando las personas en él mencionadas prueben que emplearon toda la diligencia de un buen padre de familia para prevenir el daño', justificación que no se admite en la responsabilidad solidaria del art. 61.3 de la LORPM aunque el precepto si permita su moderación cuando los padres no hayan favorecido la conducta

Es, por ende, una responsabilidad civil que se configura de forma más gravosa para los responsables solidarios respecto de otras previstas en nuestro ordenamiento jurídico penal[15], como la prevista en los arts. 116.2, 120 o 121 CP[16], lo que determina un beneficio para los intereses de víctimas y perjudicados.

Y es que, en relación con lo anterior, en cuanto su fundamento, o fines, esta responsabilidad aboga por, de un lado, amparar, más y mejor, el derecho de las víctimas, al no tener que probar la culpa del responsable civil y consiguiendo por ello la indemnización de los daños sufridos, protegiéndola asimismo de la más que probable insolvencia del menor infractor y, de otro, conseguir una mayor implicación de los padres y demás sujetos responsables en el proceso de socialización de los menores[17].

Por ende, existe un doble fundamento, la protección de las víctimas al liberarles de la prueba de la culpa del responsable civil, con un sistema objetivo o cuasi-objetivo; y la mayor implicación de los padres, tutores o guardadores con la imposición de consecuencias reparadoras de las infracciones que éstos cometan[18].

4. SUJETOS RESPONSABLES CIVILES

En lo que atañe a los sujetos responsables, además del menor infractor, que es responsable civil directo, el art. 61.3 LORPM prevé la responsabilidad civil, solidaria, de los padres, tutores, acogedores y guardadores legales o de hecho[19], por este orden, de lo que se colige que el menor es, en todo caso, responsable civil como responsable del hecho delictivo[20].

---

del menor con dolo o negligencia grave, lo que no evita la condena civil que siempre acontecerá con mayor o menor quantum". Por su parte, DE LA ROSA CORTINA (*Responsabilidad civil por daños…*, *op. cit.*, p. 39) se refiere al carácter cuasiobjetivo de la responsabilidad.

15. YZQUIERDO TOLSADA ("¿Por fin menores civilmente…", *op. cit.*, p. 46) advierte que la norma resulta mucho más severa que CC y CP, una responsabilidad objetiva.
16. Así, el art. 120 CP dispone que "Son también responsables civilmente, en defecto de los que lo sean criminalmente…", o el art. 121 CP que prevé que Estado, la Comunidad Autónoma, la provincia, la isla, el municipio y demás entes públicos, "responden subsidiariamente" de los daños causados por los penalmente responsables.
17. SAP Jaén 222/2020, de 9 de diciembre.
18. SAP Madrid 158/2021, de 7 de mayo.
19. Sobre la responsabilidad de los sujetos obligados, *vid*. BONILLA CORREA, J., *La responsabilidad civil ante un ilícito…*, *op. cit*., pp. 285-405; DE LA ROSA CORTINA, J. M., *Responsabilidad civil por daños…*, *op. cit*., pp. 69-156; GUZMÁN FLUJA, V., "Responsabilidad civil…", *op. cit*., pp. 299-306.
20. GARCIANDÍA GONZÁLEZ, P. M., "Tratamiento procesal de la responsabilidad civil…", *op. cit.*, p. 6.

Con carácter previo ha de reseñarse que, además del menor responsable de los hechos y los obligados previstos en el art. 61.3 LORPM, pueden existir otros sujetos que también deban responder civilmente, si bien al margen del proceso penal de menores. Es el caso tanto de la concurrencia de un responsable penal mayor de 18 años por los mismos hechos objeto de condena del menor, cuya responsabilidad, penal y civil, se ventilaría ante la jurisdicción penal ordinaria, como del posible responsable menor de 14 años que, al no ser imputable penalmente, deberá responder ante la jurisdicción civil por la vía de la responsabilidad extracontractual del art. 1902 CC y, por aplicación del art. 1903 CC, los padres bajo cuya guarda se encuentre el menor.

En cuanto a los responsables solidarios *ex* art. 61.3 LORPM, esto es, padres, tutores, acogedores y guardadores legales o de hecho, cumple reseñar que para la determinación de quienes ostentan la condición de tutores, acogedores y guardadores legales o de hecho habrá de acudirse a la regulación prevista en el Código Civil[21].

En cuanto a esa relación de responsables, es cuestión controvertida si dicha enumeración constituye una lista tasada o, por el contrario, se admiten otros posibles responsables, como es el caso de los centros de enseñanza o escolares, no previstos en el precepto de la LORPM, a diferencia del art. 1903 CC que sí los contempla expresamente. Pues bien, en relación con ello lo cierto es que, pese a que no figuren expresamente designados, los centros escolares pueden ser responsables civiles solidarios en los procesos penales de menores, y así lo entiende la doctrina[22], por razones de economía procesal y de protección de las víctimas, y ello bien considerando al centro escolar como guardador de hecho del art. 61.3 LORPM como en aplicación supletoria de los arts. 120 CP y 1903 CC. Esta posición que admite la responsabilidad de los centros de enseñanza ha sido acogida por la denominada jurisprudencia menor[23].

Otra cuestión relevante, y discutida en cuanto a su aplicación y efectos, es la que atañe a si la responsabilidad de los diferentes obligados solidarios, en caso de concurrencia de varios, es excluyente o cumulativa, esto es, cual haya de ser el sistema de responsabilidad que disciplina el art. 61.3 LORPM, toda vez que el precepto se refiere a los responsables "por este orden", expresión que genera la citada controversia sobre la que se ha dado en denominar responsabilidad en cascada[24].

21. DOLZ LAGO, M. J., "La responsabilidad civil derivada del delito…", *op. cit.*, p. 6.
22. DE LA ROSA, J. M., *Responsabilidad civil por daños…, op. cit*., p. 283.
23. SAP Cantabria 94/2003, de 23 de diciembre; SAP Álava 120/2005, de 27 de mayo; SAP La Rioja 43/2005, de 7 de marzo; SAP Málaga, 572/2009, de 9 de noviembre.
24. DOLZ LAGO ("La responsabilidad civil derivada del delito…", *op. cit.*, p. 12) se refiere a responsabilidad en cascada, a la vista de la expresión "por este orden"; DE LA ROSA, José Miguel, *Responsabilidad civil por daños…*, *op. cit.*, p. 55.

Sobre esta cuestión se han planteado tres sistemas diferentes: a) orden excluyente, que supone que la existencia de sujetos de un grupo anterior excluye a los siguientes; b) orden acumulativo, que admite una responsabilidad solidaria de sujetos de distintas categorías; c) tesis de la gestión efectiva del proceso educativo, de suerte que serán responsables civiles solidarios los sujetos que en el momento de suceder los hechos delictivos eran los gestores reales del proceso educativo del menor, con independencia de la concurrencia de personas o entidades de categorías anteriores[25].

Al respecto, la doctrina imperante Audiencias Provinciales es que, pese a que una interpretación literal del art. 61.3 LORPM llevaría a una responsabilidad excluyente en atención al orden que establece, una interpretación lógica y sistemática conduce a entender que el legislador ha pretendido que la responsabilidad de orden civil recaiga, de entre aquellas personas que el artículo 61.3 enumera, en la que en el momento de los hechos cometidos por el menor ejerciera sobre el mismo los contenidos de la patria potestad, o alguno de ellos. Así, el fundamento de esa responsabilidad conjunta y solidaria por parte de personas o entidades integradas en distintas categorías de sujetos respondería al control, siquiera potencial, que pueden ejercer sobre la conducta del menor y por tanto la posibilidad que tienen para prevenir y evitar sus actos ilícitos generadores de una conducta dañosa, de ahí que el orden previsto legalmente no supone un orden de exclusión automática y sucesiva, de modo que existiendo padre se excluya al tutor, al acogedor o guardador, pues ello sólo sería así, si la existencia de este va acompañada del ejercicio de la totalidad o haz de facultades conjuntas que integran la patria potestad. Por el contrario, si parte de las facultades se delegan manteniendo una facultad de superior vigilancia y cuidado, lo propio es compartir responsabilidades, debiendo en todo caso responder de forma solidaria y sin perjuicio de las acciones civiles que puedan corresponder entre sí a los corresponsables solidarios[26].

La Circular FGE 1/2007, de 23 de noviembre, sobre criterios interpretativos tras la reforma de la legislación penal de menores de 2006, señala que "pese a que ciertamente el sistema que ha sido doctrinalmente denominado de responsabilidad solidaria en cascada conforme al que responden solidariamente con el menor de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho, por este orden sigue siendo objeto de controversia, sin que la dispersa jurisprudencia menor haya llegado a una solución uniforme en su alcance e interpretación".

25. DURÁN SILVA, C., "Acerca de la legitimación de los padres y tutores en el proceso penal de menores: examen de su régimen de intervención", en ASENCIO MELLADO, J. M; FERNÁNDEZ LÓPEZ, M. (Coords.), *Proceso y daños. Perspectivas de la justicia en la sociedad del riesgo*, Tirant lo Blanch, Valencia, 2022, pp. 208-210.

26. SAP Cáceres 216/2021, de 30 de julio; SAP Guipúzcoa 101/2021, de 23 de julio; SAP Baleares 113/21, de 16 de marzo. En el mismo sentido, SSAP de Málaga 572/2009,

Esto es, no existe un orden excluyente *per se* sino que ante la concurrencia de distintos responsables habrá de determinarse su participación en el proceso de gestión educativa del menor y el ejercicio sobre éste de un control, aunque sea potencial o cuasi-potencial, de su comportamiento, de lo cual emana la responsabilidad conjunta y solidaria[27].

5. ESPECIAL REFERENCIA A LA RESPONSABILIDAD CIVIL DE LOS PADRES

Toda vez que en la mayoría de los supuestos los obligados solidarios junto al menor son sus padres, deviene preciso realizar una referencia específica a la responsabilidad de éstos.

Es así que los padres, según se ha expuesto, responderán solidariamente con sus hijos por mandato del art. 61.3 LORPM, con un régimen específico de responsabilidad que difiere de la responsabilidad extracontractual del CC[28].

El precepto únicamente se refiere a la condición de padres para determinar su responsabilidad solidaria junto al menor, sin que se circunscriba expresamente tal responsabilidad a la titularidad de la patria potestad, o se anude a la guarda o custodia del menor, o a la convivencia, lo cual genera problemas interpretativos y de aplicación[29].

---

de 9 de noviembre, y 654/2011, de 10 de diciembre; SAP de Santa Cruz de Tenerife 248/2010 de 12 de mayo, SAP 202/2011, de Almería de 8 de julio, SAP de Álava 46/2009, de 13 de febrero y SAP de Pontevedra 43/2011, de 22 de febrero.

27. La Circular FGE 9/2011, de 16 de noviembre, sobre criterios para la unidad de actuación especializada del Ministerio Fiscal en materia de reforma de menores, señala que "En el momento de elaborar el escrito de alegaciones deberá promoverse la exigencia de responsabilidad civil a todos los potenciales responsables civiles (art. 61.3 LORPM)", si bien advierte que "no obstante, no se ejercitarán acciones civiles frente a personas o entidades respecto de las que haya quedado claro que no tenían ninguna responsabilidad en la formación, custodia o vigilancia del menor".

28. La SAP Madrid 42/2021, de 15 de febrero dice que "el régimen de la responsabilidad civil de los progenitores contemplado en el artículo 61.3. de la Ley Orgánica 5/2000, de 12 de enero, Reguladora de la Responsabilidad Penal de los Menores, señalando que se trata de un régimen especial que excluye la aplicación del régimen de la responsabilidad extracontractual regulado en el Código Civil, añadiendo que tal especialidad no sólo se desprende de la referida ley orgánica, sino también de lo dispuesto en los artículos 1.902 y 1.903 del Código Civil".

29. BONILLA CORREA (*La responsabilidad civil ante un ilícito…, op. cit.*, p. 285) señala que el art. 61.3 LORPM emplea la dicción padres, ni patria potestad ni guarda, ni especifica ningún otro requisito, como la compañía o convivencia. La cuestión es si, pese a la terminología, la Ley, cuando habla de padres, quiere referirse a patria potestad, o bien el hecho determinante para responder es la paternidad, sin que sea necesario que el menor se encuentre sometido a la patria potestad, o, por último,

En tal sentido, se ha venido circunscribiendo la responsabilidad de los padres en base a dos criterios de imputación, la culpa *in educando,* más relacionada con el ejercicio de la patria potestad, *y* la culpa *in vigilando* que entronca con la guarda y custodia del menor[30], cuestión que se acentúa o adquiere especial relevancia en caso de separación o divorcio de los progenitores[31].

Con carácter general puede sostenerse que la responsabilidad de los padres guarda relación con el deber de educación y con el deber de guarda, así como del ejercicio de las facultades de corrección de forma apropiada, de suerte que del incumplimiento, cumplimiento inadecuado o inobservancia de los citados deberes emana su responsabilidad civil. Partiendo de tales consideraciones, la responsabilidad recae en ambos progenitores, aunque se encuentren separados o divorciados, con tal que no hayan sido privados de las funciones inherentes a la patria potestad[32], y siempre que la privación de la patria potestad sea, por las circunstancias concurrentes en cuanto a tiempo y motivos de dicha privación, causa que determine la no atribución de responsabilidad.

De esta forma el deber de educación, inherente a la patria potestad[33], con independencia de la atribución concreta del deber de guarda o de la custodia en el momento de la comisión del hecho delictivo por el menor infractor, se erige en un factor o criterio de atribución de responsabilidad civil más amplio[34], lo cual es

que lo decisivo sea el requisito de la guarda. Tampoco hace mención a la trascendencia de que los padres estén casados; o si el régimen económico matrimonial tiene alguna repercusión a estos efectos; ni si la separación, nulidad o divorcio tiene algún alcance.

30. Sobre esta cuestión, *vid*. BONILLA CORREA, J., *La responsabilidad civil ante un ilícito…*, *op. cit*., p. 294.

31. *Vid*. DE LA ROSA CORTINA, J. M., *Responsabilidad civil por daños…*, *op. cit*., pp. 132-141.

32. Así lo refiere expresamente la SAP Guipúzcoa 101/2021, de 23 de julio.

33. Las Conclusiones y propuestas de las Jornadas de Magistrados de Menores de octubre de 2010 defienden que la regla mayoritaria es la responsabilidad de ambos progenitores, al entender que la patria potestad integra no solo los deberes de guarda y custodia, sino también de educación y formación integral, con independencia de si tiene o no régimen de visitas, vacaciones, si está o no localizable, si no se relaciona con el hijo desde la infancia.

34. BONILLA CORREA (*La responsabilidad civil ante un ilícito…*, *op. cit.*, pp. 322-323) considera preferible encauzar la responsabilidad de los padres sobre la base de la patria potestad frente a la guarda, pues, entiende, ambos padres pueden ser declarados responsables en los casos de separación, nulidad o divorcio, con independencia de haber atribuido a uno u otro la guarda y custodia del menor. DE LA ROSA CORTINA (*Responsabilidad civil por daños…*, *op. cit.*, p. 132) señala que un supuesto especialmente complejo es el del tratamiento de la responsabilidad de padres separados, de hecho o de derecho o divorciados, pues el art. 61.3 LORPM, a diferencia de lo que establece el art. 1903 CC, no exige para que surja la responsabilidad de los padres o tutores que el menor esté bajo la guardia de los mismos, por lo que la tesis de la responsabilidad

más acorde con la naturaleza objetiva y el fundamento de la responsabilidad civil diseñada por la LORPM[35].

No obstante, cabe matizar que la concreta guarda y custodia puede desplegar, en determinados supuestos, efectos en orden a poder justificar la moderación de la responsabilidad civil por aplicación del art. 61.3 LORPM respecto de alguno de los progenitores, más en concreto de quien no tuviese la guarda en el momento de los hechos ilícitos[36].

Por su parte, también se plantea la incidencia de los supuestos de extinción de la patria potestad por emancipación del menor responsable de los hechos en relación con la responsabilidad civil de los padres y su posible exoneración. Pues bien, relación a esta cuestión las posiciones pueden ser diversas en función no sólo de las causas de emancipación, sino de los verdaderos fines perseguidos y si éstos son exclusivamente elusivos de la responsabilidad civil de los padres[37].

---

solidaria de ambos progenitores aún en supuestos en los que el menor conviva con uno solo de ellos adquiere mayor fuerza.

35. DURÁN SILVA ("Acerca de la legitimación de los padres…", *op. cit.*, p. 196) advierte que la *culpa in educando* es el fundamento empleado por la LORPM para atribuir la responsabilidad a los padres.

36. Como refiere DE LA ROSA CORTINA (*Responsabilidad civil por daños…*, *op. cit.*, pp. 139-140), el hecho de que los padres no convivan y, por tanto, la consecuencia que de uno de ellos no tenga bajo su guarda al menor en el momento de cometerse los hechos puede generar consecuencias. La responsabilidad alcanzará tanto al progenitor que tenga atribuida la guarda y custodia, como al que no, sin perjuicio de las facultades de moderación del Juez que, en estos casos, pueden justificadamente desplegar su operatividad. En cuanto a la operatividad de la moderación, advierte el autor que como regla general el progenitor que no tuviera la guarda efectiva podrá ver moderada su responsabilidad, debiendo interpretarse con flexibilidad qué ha de entenderse por tener al hijo bajo la guarda, que podrá abarcar situaciones transitorias derivadas del derecho de visita o del propio convenio. Puede ser principal responsable de los daños causados por el hijo el progenitor quien, aun no ostentando la guarda y custodia, estuviera ejerciendo el derecho de visitas. En todo caso, como premisa, cree que cuando la guarda y custodia se ejerciera únicamente por uno de los progenitores por dejación de las obligaciones del otro parece claro que el progenitor no custodio debe responder *in integrum* pues, en otro caso, se daría un tratamiento privilegiado al progenitor que incumple las obligaciones de la patria potestad y las obligaciones de vigilar y educar. Para otros supuestos, habrá de distinguirse en el caso de padres que no vivan juntos si el daño puede fundarse en culpa *in vigilando* o en culpa *in educando*. Si trae causa en culpa *in vigilando*, habrá de responder con carácter principal el progenitor que en el momento tuviere bajo su guarda al menor: bien el progenitor que tuviera atribuida la guarda y custodia, bien el progenitor que, pese a no tenerla atribuida se encontrara disfrutando de derecho de visitas, y el otro progenitor habrá de ver su responsabilidad moderada.

37. Sobre la emancipación del menor en relación a la responsabilidad civil, *vid.* BONILLA CORREA, J., *La responsabilidad civil ante un ilícito…*, *op. cit.*, pp. 327-332.

Así, en sede de la modalidad de emancipación por concesión de quienes ejerzan la patria potestad, que requiere que el menor tenga dieciséis años cumplidos y la consienta (art. 241 CC) o ante la equiparación a la emancipación del hijo mayor de dieciséis años que, con el consentimiento de los progenitores, viviere independientemente de estos (art. 243 CC), como situaciones que habilitan al menor para regir su persona y bienes como si fuera mayor, con excepciones (art. 247 CC), parece que esa finalización de los deberes inherentes a la patria potestad por emancipación puede determinar la exoneración de los padres como responsables civiles del hijo emancipado[38]. No obstante ello, esa premisa general quiebra en situaciones de emancipaciones ficticias o fraudulentas, apartadas de una situación real de base para la emancipación, cuyo verdadero objetivo radica en evitar, precisamente, la declaración de responsabilidad de los padres del emancipado[39].

En determinados supuestos los padres del menor son a su vez las víctimas o perjudicados del delito perpetrado por su hijo. En tales supuestos se plantean diversas situaciones en relación con la responsabilidad civil dimanante de los hechos delictivos que pueden determinar la no exigibilidad de responsabilidad civil por los hechos a los progenitores que a su vez resultan ser víctimas o perjudicados por el propio delito cometido[40].

38. Así, GUZMÁN FLUJA, V., "Responsabilidad civil…", *op. cit.*, pp. 306-307.

39. En este sentido la Circular FGE 9/2011, de 16 de noviembre, sobre criterios para la unidad de actuación especializada del Ministerio Fiscal en materia de reforma de menores, expone que**: "**Los supuestos de emancipación tácita por vida independiente, prevista en el art. 319 CC, no suponen la exclusión de la responsabilidad civil solidaria de los padres.

    Tras la formal emancipación del menor de edad por matrimonio, por concesión judicial o por concesión de los padres, cesa la responsabilidad civil de sus padres o tutores respecto de hechos cometidos con posterioridad. No obstante, este principio general debe excepcionarse en los supuestos en los que por las propias circunstancias concurrentes, pudiera llegarse a la conclusión de que la emancipación formalmente declarada por concesión de los padres ha sido realizada en fraude de Ley".

40. En este sentido, DOLZ LAGO ("La responsabilidad civil derivada del delito…", *op. cit.*, p. 12) hace referencia al dictamen 11/2010 de la Fiscalía de Sala Coordinadora de Menores sobre cómo actuar cuando los padres son víctimas del delito cometido por el menor, concluyendo que: "1.ª En aquellos supuestos en que como consecuencia de la agresión de un hijo menor a alguno de sus progenitores aparezca como perjudicado una entidad sanitaria, por los gastos prestados de asistencia médica, no se entiende procedente que por la Fiscalía se dirija contra dicho progenitor, al ser víctima del hecho, la acción para exigir la responsabilidad civil solidaria del art 61-3 LORPM, sin perjuicio de que la entidad sanitaria, si lo estimase oportuno, pueda personarse y ejercitar la acción civil conforme al artículo 61-1 LORPM.

    2.ª Respecto al otro progenitor que, en los mismos casos, conviva en el núcleo familiar, pero no hubiera recibido asistencia sanitaria, tampoco deberá ejercitarse dicha acción civil si resultase ser también uno de los sujetos pasivos por los hechos típicos de violencia doméstica cometidos por el menor. En el caso de que no fuese reputado

III. LA FACULTAD DISCRECIONAL DE MODERACIÓN JUDICIAL DE LA RESPONSABILIDAD CIVIL

La facultad judicial de moderar la responsabilidad civil dimana del art. 61.3 LORPM, precepto que dispone que cuando los responsables solidarios (padres, tutores, acogedores y guardadores legales o de hecho) no hubiesen favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el Juez, según los casos.

La previsión legal de una facultad judicial de moderación de la responsabilidad civil no es cuestión exclusiva de la LORPM pues existen otras disposiciones legales que prevén una posibilidad de moderación. Así, el art. 1103 CC dispone que la responsabilidad que proceda de negligencia podrá moderarse por los Tribunales según los casos. Por su parte el art. 114 CP prevé que, si la víctima hubiere contribuido con su conducta a la producción del daño o perjuicio, los Jueces o Tribunales podrán moderar el importe de su reparación o indemnización.

Esta última facultad moderadora prevista en el art. 114 CP deviene aplicable al proceso penal de menores, y así resulta de la remisión expresa efectuada por el art. 62 LORPM. Ello determina que es posible que la responsabilidad civil a establecer en sentencia resulte moderada por la contribución de la víctima en el resultado lesivo o dañoso.

La facultad de moderación de la responsabilidad civil de los obligados solidarios en aplicación del art. 61.3 LORPM no es, desde luego cuestión baladí, toda vez que los importes de las responsabilidades civiles a cuyo pago puede resultar condenado el menor responsable puede ser de una importancia muy relevante. Así sucede tanto con carácter general ante tipos delictivos en que se produce el fallecimiento de las víctimas (asesinato, homicidios) lesiones importantes o delitos contra la libertad e indemnidad sexual, con inclusión de la reclamación por las administraciones competentes de los gastos por asistencia sanitaria prestada a las víctimas, o ante delitos contra el patrimonio, como, con carácter particular, en los ciberdelitos o delitos cometidos a través de internet, bien sean de naturaleza patrimonial o bien afecten a bienes jurídicos de carácter personal, como sucede en delitos contra la intimidad, en los cuales las indemnizaciones en concepto de responsabilidad civil (*ad exemplum* daño moral) pueden ascender a importes elevados.

---

como víctima, se ponderarán todas las circunstancias concurrentes para excluirle o moderar ampliamente su responsabilidad civil.

3.ª Cuando en esos mismos casos no existiese convivencia entre los progenitores, no hay obstáculo para reclamar del progenitor no custodio la responsabilidad civil solidaria del art. 61-3 LORPM, valorando debidamente las circunstancias que alegase el obligado al pago y que pudieran contribuir a su moderación".

Ello determina que la posible moderación, o reducción, de la responsabilidad civil del obligado solidario revista una enorme trascendencia en cuanto al ámbito económico-patrimonial.

De otro lado, tampoco se puede obviar la repercusión que una eventual moderación de la responsabilidad civil del obligado solidario puede suponer para la víctima o el perjudicado por el delito, al afectar a las posibilidades de obtener la reparación o satisfacción total del daño o perjuicio sufrido, pues los menores no son, generalmente, solventes, ello sin perjuicio de que dicho menor queda obligado *pro futuro* a hacer frente a las responsabilidades civiles en caso de mejorar su situación económica.

1. SUJETOS CUYA RESPONSABILIDAD PUEDE SER MODERADA

En relación con los sujetos cuya responsabilidad es susceptible de ser moderada por la vía del art. 61.3 LORPM, hay que partir de que esta moderación no puede alcanzar al menor responsable del ilícito penal.

Al resto de sujetos pasivos obligados por el art. 61.3 LORPM les podrá ser de aplicación la facultad de moderación de la responsabilidad civil[41], con la minoración de la cuantía indemnizatoria a cuyo pago devienen obligados si concurren los requisitos o presupuestos precisos a tal efecto. Incluso en aquellos supuestos en que dentro de la misma categoría de responsables solidarios pueden concurrir varios sujetos, como ocurre en caso de progenitores divorciados o separados, la minoración podría operar respecto de alguno de ellos o incluso con distinto alcance en función de las circunstancias concurrentes[42].

41. BONILLA CORREA (*La responsabilidad civil ante un ilícito…*, *op. cit.*, p. 267) advierte que no faltan autores que, con el ánimo de conciliar la reparación de la víctima y los principios que informan la responsabilidad civil, y en atención a la dicción empleada por el legislador de "según los casos", proponen limitar el instituto de la moderación a determinados responsables solidarios, como acogedores o guardadores, de modo que tutores y padres serían los únicos sujetos a los que la moderación no se les aplicará, si bien señala el autor que esta limitación en función de los sujetos no casa bien con la dicción de la Ley por lo que, entiendo, la moderación no tiene ninguna limitación por razón de los sujetos.

42. BONILLA CORREA (*La responsabilidad civil ante un ilícito…*, *op. cit.*, p. 268) plantea si ante la hipótesis de varios sujetos dentro del mismo grupo de responsables, padre y madre, varios tutores, etc., se puede tener en cuenta el comportamiento individual de cada uno a fin de poder aplicar sólo a uno la moderación; es decir, si la actuación de uno ha sido diligente, y la del otro no, ver si es posible moderar la cuantía sólo al que fue diligente, y señala que sería apropiado tener en cuenta las conductas individuales.

2. PRESUPUESTO DE APLICACIÓN: NO FAVORECIMIENTO DE LA CONDUCTA CON DOLO O NEGLIGENCIA GRAVE

De acuerdo con lo previsto en el art. 61.3 LORPM la facultad de moderación procede únicamente cuando el sujeto obligado no hubiere favorecido la conducta del menor con dolo o negligencia grave[43], lo que exige una labor de interpretación de tales conceptos en orden a su concreción en el caso concreto[44]. Del precepto se colige que podría aplicarse la facultad moderadora no sólo ante una actuación diligente, sino también cuando la negligencia no haya sido grave

La citada previsión lleva a entender que en caso de negligencia, o culpa "no grave", se podría aplicar, motivadamente, la facultad de moderación o, lo que es lo mismo, supone que, pese la concurrencia de negligencia o culpa no grave del responsable civil éste va a tener que responder igualmente, si bien cabe que su responsabilidad sea moderada[45].

En tal sentido, a efectos de determinar cuál haya de ser la culpa "no grave" susceptible de generar la minoración de la responsabilidad, se ha planteado si procede su identificación con la culpa leve o si, por el contrario, únicamente puede equipararse con la denominada culpa levísima[46].

En todo caso, con independencia de si la intelección del concepto de negligencia "no grave" ha de reconducirse a las categorías civiles de culpa

43. Como considera BONILLA CORREA (*La responsabilidad civil ante un ilícito…*, *op. cit.*, p. 251), hubiese sido más afortunado términos como diligencia o cuidado, según advirtió el informe del CGPJ.

44. Sobre estos conceptos, *vid*. BONILLA CORREA, J., *La responsabilidad civil ante un ilícito…*, *op. cit.*, pp. 248-251.

45. DE LA ROSA (*Responsabilidad civil por daños…*, *op. cit.*, pp. 367-368) señala que, aunque no concurra culpa se seguirá respondiendo por los actos del menor, si bien cabrá la moderación. Por tanto, la responsabilidad de los obligados solidarios no requiere culpa pero, no obstante, la ausencia de culpa grave se tiene en cuenta, no para la exoneración pero si para reducir el quantum indemnizatorio a cargo de los responsables solidarios.

46. BONILLA CORREA (*La responsabilidad civil ante un ilícito…*, *op. cit.*, pp. 251-252) señala que el legislador habla de dolo o negligencia grave, pero no alude a la culpa o negligencia en grado leve o levísimo. La primera entendida como la omisión de la diligencia de un padre de familia medio, aquella diligencia adoptada por cualquier padre de familia. La segunda, la culpa levísima, como la omitida por un padre de familia escrupuloso y cuidadoso. En el primer supuesto, el de culpa leve, no procede la facultad de moderación, y así se podría entender si se interpreta esta cuestión con la alusión "según los casos" que emplea el precepto; encontrarnos en esta hipótesis significa que se ha omitido una diligencia "en grado medio", aquella diligencia que una persona normal no omite, por lo que no debe proceder la moderación, o por lo menos basándose en este criterio, el de la existencia o no de culpa. En cuanto a la culpa levísima, se equipararía al supuesto de comportamiento de forma diligente y, en consecuencia, el Juez o Tribunal podría hacer uso de la moderación.

leve o levísima[47], lo cierto es que a efectos de determinar la concurrencia de una actuación o comportamiento diligente o sin negligencia grave que pueda significar la moderación de la responsabilidad *ex* art. 61.3 LORPM habrá que estar y atender a las circunstancias concretas de cada supuesto, ponderando la observancia y cumplimiento por parte de los padres de los deberes, sus esfuerzos desplegados en el proceso de educación y de vigilancia o control, en sentido amplio, ello en atención a la concreta conducta delictiva y la influencia que se pueda colegir que ha tenido sobre ésta[48], con especial consideración de factores como la edad del menor a fecha de comisión, circunstancias de su personalidad o enfermedades o dolencias, comportamientos o delitos anteriores, así como referidos al propio delito: lugar, hora etc.[49].

En conexión con ello, en relación con los delitos informáticos o tecnológicos, habrá de ponderarse el cumplimiento de deberes de control o de educación en el manejo de las nuevas tecnologías y redes sociales, así como, en su caso, los mecanismos de supervisión.

3. FUNDAMENTO DE LA MODERACIÓN

Otra cuestión a la que procede prestar atención es la que atañe al fundamento de la facultad moderadora contemplada en el art. 61.3 LORPM.

47. La SAP Madrid 42/2021, de 15 de febrero, señala que la norma establece directamente la responsabilidad solidaria de los padres del menor, sin supeditarla a la negligencia en el cumplimiento de sus obligaciones, tratándose de una responsabilidad cuasi-objetiva que permite su moderación, correspondiendo a los progenitores la carga de acreditar que "no favorecieron con dolo o negligencia grave (entendidos como conceptos civiles) la conducta ilícita del menor".

48. BONILLA CORREA (*La responsabilidad civil ante un ilícito…*, *op. cit.*, pp. 253-254) advierte que es preferible emplear un concepto de negligencia referido a un incumplimiento de deberes, lo que supone necesariamente que los sujetos en cuestión debían actuar de una determinada forma y no lo hicieron. No se trata de averiguar si hubo una infracción genérica al deber de los padres, tutores o guardadores, ya sean legales o de hecho, sino establecer si esa conducta delictiva realizada por el menor tiene relación con un hipotético incumplimiento de los deberes de educación, socialización, vigilancia o control del menor.

49. DE LA ROSA CORTINA (*Responsabilidad civil por daños…*, *op. cit.*, pp. 370-371) señala de entre los criterios a tener en cuenta el de la edad (a mayor edad las exigencias del deber de vigilar se atenúan), estar o no escolarizado, la personalidad del menor (si el menor presenta alteraciones de conducta o déficits mentales deben adoptarse medidas especiales), el lugar y hora en que sucedieron los hechos (si es a altas horas o en lugares en los que concurra factores de peligro puede llegar a colegirse que el menor no era diligentemente supervisado) y la concurrencia de anteriores comportamiento indebidos por parte del menor (en estos casos es exigible un plus de diligencia por los padres en sus deberes de guarda y custodia y vigilancia de las actividades del menor).

En tal sentido, hay que partir de que la responsabilidad civil de los padres se basa en el deber de educación, lo que conlleva el ejercicio de facultades de corrección, así como en el deber de guarda y custodia, respecto del hijo menor. Como se ha señalado, el sistema de obligaciones solidarias del art. 61.3 LORPM responde la doble función de protección y la mayor implicación de los padres con la imposición de consecuencias civiles por las infracciones penales cometidas.

Ahora bien, en contrapartida a la gravosa configuración del régimen de responsabilidad civil contenido en la LORPM para los obligados solidarios, el art. 61.3 ha dispuesto una posibilidad de aplicar una moderación de la misma que mitigue sus consecuencias ante la concurrencia de circunstancias que así lo aconsejen.

De este modo, el fundamento de la facultad de moderación, y de su aplicación, reside la consideración de las conductas, actitudes y esfuerzos llevados a cabo por los padres en orden a la adecuada gestión e implicación en la educación y vigilancia de sus hijos menores, aun cuando ello no haya podido evitar la comisión del ilícito penal[50]. En suma, se trata de premiar, de algún modo, a los responsables, generalmente los padres, que han gestionado, o se han esforzado cumplidamente, en ese proceso formativo, socializador y educativo de los menores, con una reducción de su obligación solidaria[51], y más en concreto en todo aquello referido al manejo y uso de internet.

A sensu contrario, la consideración del citado fundamento determina el rechazo de la moderación ante supuestos en que se revelen procesos de inadecuada educación o deficiente control sobre el menor.

4. ALCANCE DE LA MODERACIÓN

La moderación de la responsabilidad civil no puede suponer la exclusión total de la obligación de responder de la misma. Así, un obligado solidario no podrá quedar excluido de responsabilidad en base a la aplicación de la facultad moderadora del art. 61.3 LORPM[52].

50. SAP Asturias 183/2007, de 28 de junio.
51. La SAP Alicante 328/2013, de 31 de mayo, refiere que el fundamento está en la trasgresión del deber de vigilancia, que comprende también los deberes de educación y formación integral del menor, en la tolerancia y respeto de los derechos individuales y propiedad de los demás, estimándose inadecuadas tanto las conductas de dejadez en la educación, como las actitudes de protección y de justificación a ultranza de la conducta del menor.
52. BONILLA CORREA (*La responsabilidad civil ante un ilícito…, op. cit*., p. 275) parte de que en lo que a la cuantía se refiere es complicado fijar el límite a esa moderación.

En consecuencia, la moderación únicamente puede afectar, determinando, la extensión o la cuantía de dicha moderación. A tal fin, en nuestros tribunales se ha venido aplicando un sistema de minoración porcentual de la responsabilidad de la cual se exonera al responsable civil, esto es, un sistema de porcentajes de reducción.

Ahora bien, lo cierto es que no hay criterios determinados en cuanto a la fijación de un porcentaje concreto de minoración, lo que implica que habrá que estar al caso concreto para su determinación[53]. No obstante, hay que considerar que, dado que no procede la exoneración, tampoco resultaría admisible una reducción cuasi total por vía de moderación, con un porcentaje de reducción muy elevado –próximo al 100%–, pues no se puede orillar que la moderación es excepcional[54].

De la práctica judicial se colige que no hay criterios unívocos sobre el quantum en la aplicación de esta facultad, si bien por lo general no suele exceder del 50%, sin perjuicio de resoluciones que manejan porcentajes mayores, siendo deseable que existiesen criterios más uniformes que, aun conscientes de la dificultad que supone, arrojasen más seguridad jurídica a la cuestión[55].

Además de la cuantía susceptible de moderación judicial, cabe plantearse los efectos que procede conferir a esta moderación, esto es, si la moderación despliega su eficacia sólo entre los obligados solidarios y en relación con el menor, pero sin afectar al perjudicado/víctima (eficacia *ad intra*) o si, por el contrario, surte efectos respecto del perjudicado o víctima del delito (eficacia *ad extra*).

Moderar en modo alguno significa exonerar, por lo que, en principio, debe excluirse cualquier moderación que suponga fijar una responsabilidad simbólica a los responsables solidarios pues la Ley no habla de exonerar, sino que se limita a moderar. DE LA ROSA CORTINA (*Responsabilidad civil por daños…, op. cit*., p. 385) entiende que no puede el Juez apreciar una falta total de culpa o negligencia, y correlativamente exonerar a todos los obligados solidarios de toda responsabilidad. El sistema cuasiobjetivo instaurado por la LORPM supone que los padres (y demás personas señaladas en el artículo) responden solidariamente con los menores haya o no haya dolo o negligencia, en caso de inexistencia de dolo o negligencia grave se podrá moderar la responsabilidad civil, pero ésta seguirá existiendo.

53. Así, la SAP Alicante 328/2013, de 31 de mayo, advierte que "en cuanto a los criterios para determinar el concreto porcentaje de moderación, se ha de estar al caso concreto, pero ha de tenerse en cuenta que la regla general ha de ser la no moderación o la no rebaja en absoluto, dada la dicción legal, de la que resulta la excepcionalidad de la moderación".
54. SSAP Valencia 95/2009, de 18 de febrero y 22/2010, de 14 de enero.
55. En las Conclusiones y propuestas de las Jornadas de Magistrados de Menores de octubre de 2010 se advertía de la falta de homogeneidad y contradicciones en las causas y los porcentajes de moderación, siendo oportuno unificar doctrina.

A consideración nuestra, procede interpretar que la facultad de moderación tiene efectos *ad extra*, de modo que la minoración de la responsabilidad civil del obligado determina que únicamente responderá en la medida en que la sentencia así lo haya establecido[56]. Esta es, por otro lado, la interpretación que mayoritariamente sostienen las Audiencias Provinciales[57].

5. MOTIVACIÓN

La facultad de moderación, que no exclusión, de la responsabilidad civil que norma el art. 61.3 LORPM se configura como de carácter discrecional, toda vez que el citado precepto prevé que la responsabilidad "podrá ser moderada por el Juez, según los casos"[58]. Esta discrecionalidad en una característica esencial de la moderación legalmente establecida.

Ahora bien, que sea una facultad discrecional no puede determinar que su ejercicio sea arbitrario, de forma que resulta inexcusable que el juzgador motive su decisión al respecto[59]; deber de motivación que emana, con carácter general del art. 120 CE, así como de los arts. 142.2.ª LECrim y

56. DE LA ROSA (*Responsabilidad civil por daños…, op. cit*., pp. 387-388) hace referencia a las dudas sobre la eficacia operativa de la facultad de moderación, pues algunos autores postulan interpretar la moderación de la responsabilidad no como reducción del *quantum*, sino como modificación del régimen de solidaridad, y alguna sentencia ha limitado los efectos de esta moderación al ámbito interno de la solidaridad, pudiendo reclamarse el total a los padres aunque se haya moderado su responsabilidad (SAP Madrid secc.4.ª, n.º 78/2003, de 29 julio). En opinión del autor, la facultad de moderación debe entenderse como posibilidad de reducción del *quantum* indemnizatorio en relación con aquel responsable a quien se le aplica, por lo que aún en caso de insolvencia del menor, el beneficiario de la moderación sólo responderá hasta el porcentaje asignado, por lo que la línea interpretativa correcta es la que atribuye a la moderación efectos no solo *ad intra* sino también *ad extra*, pues en los casos en que se considera que no concurre culpa de los representantes legales y se opta por moderar su responsabilidad, si la insolvencia del menor generara automáticamente la obligación de los beneficiarios de responder por el total la moderación sería poco menos que una entelequia, carente de operatividad práctica, y sus pretendidos efectos de equidad quedarían neutralizados por la insolvencia generalizada de los menores.

57. SAP Burgos 227/2010, de 11 de noviembre; SAP Asturias 154/2004, de 6 mayo.

58. La SAP Madrid 158/2021, de 7 de mayo, señala que la facultad de moderación atribuida al Juez es potestativa y no obligatoria.

59. Como advierte BONILLA CORREA (*La responsabilidad civil ante un ilícito…, op. cit*., pp. 272-273), la Ley sólo habla de una facultad de moderar la responsabilidad por parte del Juez, que no debe entenderse como arbitraria, pese a que no se establezca otro límite que el no concurrir dolo o negligencia grave de los responsables solidarios, por lo que para aplicar el instituto de la moderación debe razonarse por qué lo hace. Esto no quiere decir que se tenga que aplicar con carácter restrictivo, sino que debe estar fundamentado.

238.3.º LOPJ, así como por la previsión especifica contenida en el art. 39.1 LORPM, precepto que exige la motivación de la sentencia, lo cual entronca, asimismo, con el derecho a la tutela judicial efectiva del art. 24 CE.

En consecuencia, en base a lo solicitado por la parte obligada solidariamente y la prueba existente, el juzgador deberá adoptar una decisión, bien de rechazo bien de aceptación de la minoración, que habrá de estar debidamente motivada, justificando las razones en que sustenta su decisión en referencia a aquellas circunstancias, elementos y medios de prueba en base a los que ha alcanzado su convicción[60]. Asimismo, en caso de que decida aplicar la facultad moderadora, debería motivar su decisión sobre respecto a la concreta minoración que establece, su *quantum*, en el supuesto sometido a su consideración.

Esa necesidad, en puridad obligación, de motivar se hace más patente en supuestos en que acuerde la moderación, atendido el carácter excepcional que se confiere a dicha facultad judicial[61].

IV. ALEGACIÓN Y PRUEBA

1. PETICIÓN DE PARTE: ROGACIÓN

La aplicación judicial de la moderación de la responsabilidad civil de los obligados solidarios debe ser solicitada por aquellos que la pretenden. En consecuencia, para poder entrar a decidir y pronunciarse sobre la procedencia o no de la minoración de la misma, deviene necesario que exista una previa petición de parte, en aplicación del principio de rogación, sin que el órgano judicial pueda aplicar la facultad moderadora sin solicitud expresa, so pena de vulnerar el principio dispositivo[62].

Por ende, la facultad de moderación del art. 61.3 LORPM no puede ser aplicada de oficio, sino a instancia de parte, lo cual está en consonancia con la naturaleza disponible de la responsabilidad civil *ex delicto*.

60. Como destaca la SAP La Rioja 18/2013, de 6 de febrero, la facultad de moderar es discrecional y para su aplicación es necesario que el responsable civil despliegue una actividad probatoria, sin que valgan alegaciones genéricas.
61. La SAP Madrid 42/2021, 15 de febrero, dice que el precepto atribuye al órgano judicial una facultad discrecional de moderación, que no parece que pueda sujetarse en su aplicación a precisas reglas matemáticas, sino a meros parámetros de razonabilidad, en función de las circunstancias concurrentes, sin olvidar que la naturaleza cuasi objetiva de la responsabilidad solidaria que se contempla en el precepto y la excepcionalidad de su moderación, en garantía del resarcimiento del perjudicado.
62. SAP Valencia 22/2010, de 14 de enero; SAP Burgos 227/2010, de 11 de noviembre.

Ahora bien, deberá entenderse que si la parte obligada como responsable civil solicita su exoneración como tal dentro de su solicitud habría de entenderse incluida, siquiera implícitamente, la petición de moderación, por lo que el juzgador puede pronunciarse, y acordar, la moderación sin quiebra del principio o deber de congruencia.

2. MOMENTO PROCESAL DE ALEGACIÓN. POSTULACIÓN

Partiendo de la necesidad de solicitud de parte, lo primero que hay que determinar es el relativo al momento procesal en que puede ser invocada.

En tal sentido, hay que partir de que a los responsables civiles en la denominada pieza de responsabilidad civil (arts. 61 a 64 LORPM), como dispone la regla 3.ª del art. 64, el LAJ notificará al menor y a sus representantes legales, en su caso, su condición de posibles responsables civiles, estableciéndola regla 4.ª del citado precepto que una vez personados los presuntos perjudicados y los responsables civiles, el Juez de Menores resolverá sobre su condición de partes, continuándose el procedimiento por las reglas generales. Es evidente que, aunque no exista personación de los posibles responsables civiles, ello no determina que no pueda exigírsele la responsabilidad civil que proceda en el proceso penal en orden a su condena en sentencia.

Cabe advertir que, si bien del tenor del art. 64.4.ª LORPM pudiera desprenderse que el Juez de Menores pudiera determinar que los responsables civiles queden excluidos del proceso en esa pieza de responsabilidad civil, se antoja que tal interpretación no resulta procedente toda vez que ello deberá sustanciarse y decidirse en la audiencia o juicio tras la práctica de la prueba, a excepción de aquello supuestos que, por su evidencia, es palmario que el sujeto no ostenta la condición de responsable civil en el asunto concreto[63].

En consecuencia, de conformidad con las previsiones del proceso penal de menores, la responsabilidad civil se va a ventilar en el proceso principal, ello cuando se ejerciten las pretensiones penales y las civiles conjuntamente, sin que medie reserva ni renuncia de acciones, por lo que a los responsables civiles, los padres en este caso, de acuerdo con el art. 31 LORPM se les va a dar traslado de todo lo actuado, esto es, del Expediente de Reforma y los escritos de alegaciones con las peticiones penales y civiles formuladas por la acusación o actores civiles a fin de que, en un plazo de cinco días hábiles, formulen escrito de alegaciones y propongan la prueba que consideren pertinente.

63. Así GUZMÁN FLUJA, V., "Responsabilidad civil…", *op. cit.*, p. 329.

En el citado escrito de alegaciones de los responsables civiles, si deciden comparecer y personarse en el proceso iniciado, deberán introducir las cuestiones relativas a la responsabilidad civil en general y a la solicitud de moderación en particular, proponiendo las pruebas que estime oportunas a tal efecto y en relación, exclusivamente, a la cuestión civil debatida.

Lo anterior debe ponerse en relación con la postulación, esto es, si los padres han de actuar bajo dirección técnica letrada y procurador. Si bien la LORPM no lo prevé expresamente, toda vez que la ley únicamente prevé la designación preceptiva de letrado para para que actúe en defensa y representación del menor (art. 22.2 LORPM), igual criterio de preceptiva actuación únicamente con letrado habrá de regir tanto para la acusación particular, o actor civil, como para los responsables civiles[64].

Sobre esta actuación letrada se suscita la cuestión relativa a la posibilidad de que el menor y sus padres actúen en el proceso bajo la misma dirección letrada. Al respecto, a nuestro entender, si los padres únicamente cuestionan la existencia o procedencia de la responsabilidad, o cuestionan el importe o la reparación solicitada no existe óbice para actuar bajo idéntica defensa. Ahora bien, el problema surge si cualquiera de los padres, o ambos, peticionan la minoración de su responsabilidad frente a la que pudiera acordarse respecto de su hijo, pues en tal caso puede surgir una contraposición de intereses entre hijo y padre o padres, de suerte que ante ese conflicto resulta más adecuado que la defensa de ambas partes sea distinta.

3. ACTUACIONES PROCESALES DE LOS RESPONSABLES

Al margen de lo expuesto sobre la pieza de responsabilidad civil incoada por el Juzgado de menores (arts. 61 a 64 LORPM), lo cierto es que la LORPM no prevé actuación alguna de los responsables civiles durante la fase de instrucción, o expediente de reforma en términos de la norma, pues únicamente prevé actuaciones de víctimas o perjudicados (art. 4 LORPM), de modo que no existe una previsión legal expresa para su intervención como parte civil.

En consecuencia, la primera posibilidad de intervención de los responsables civiles es la contenida en el art. 31 LORPM, referida a la presentación

64. En tal sentido, la Circular FGE 1/2007, de 23 de noviembre, sobre criterios interpretativos tras la reforma de la legislación penal de menores de 2006 advierte que "Será por tanto necesario que actor y responsable civil actúen por medio de Letrado. Teniendo en cuenta que en el proceso de menores ni el menor infractor ni la acusación particular necesitan actuar representados por medio de procurador, con más razón habrá de exonerarse de tal requisito a quien exclusivamente actúe como actor civil o como responsable civil".

del escrito de alegaciones, siempre que se hubiesen constituido como parte formal del proceso, personación que es voluntaria. En dicho escrito de alegaciones el responsable civil puede mostrar su disconformidad con las alegaciones de la acusación y actores civiles y proponer la prueba que estime pertinente sobre la cuestión relativa a la responsabilidad civil, y solicitar la aplicación de la facultad moderadora, teniendo en cuenta que si existe conformidad del menor y de su letrado pero no de los responsabilidades civiles la audiencia se celebrará exclusivamente en lo relativo a la responsabilidad civil (art. 32 LORPM). La otra posibilidad consiste en que los responsables civiles presenten escrito de alegaciones mostrando su conformidad con las pretensiones civiles.

Posteriormente, su actuación tiene lugar en la audiencia o juicio oral. En dicho acto, al inicio del mismo puede tener lugar una conformidad según lo previsto en el art. 36 LORPM, si bien si el responsable civil no está de acuerdo en los términos de la misma en cuanto a la responsabilidad civil, la audiencia deberá tramitarse únicamente respecto de ésta. Se pudiera suscitar la duda de si el acuerdo de conformidad de las partes en el que se incluya la minoración de la responsabilidad civil respecto de los padres del menor, en base a la posibilidad de moderación de la misma, vincula al juzgador toda vez que la moderación es una facultad de aplicación discrecional; a nuestro juicio, dado que la responsabilidad civil es disponible para la partes el juez de menores quedaría vinculado por el acuerdo alcanzado en orden a la determinación de la responsabilidad en sentencia.

De no haber conformidad se procedería a la celebración de la audiencia según las previsiones del art. 37 LORPM, de forma que, tras oír a las partes sobre posible vulneración de derechos fundamentales y proposición de nuevas pruebas, se procede a la práctica de la prueba y, a continuación, se oirá a las partes, lo que incluye a los responsables civiles, en aquello que les afecte, respecto de los derechos que les asisten y la valoración de la prueba. Hay que reseñar que la inasistencia, injustificada, de los responsables civiles previamente citados a tal fin, no determina la suspensión de la vista, que se celebrará sin su presencia.

En relación a la actuación en la audiencia o juicio del responsable civil, el art. 37 LORPM se limita a establecer que habrá de oírse a los responsables civiles "respecto de los derechos que les asisten", sin que se exija su previa personación con letrado, de lo que se plantea la procedencia de dicha audiencia pese a no estar personados con letrado, debiendo entenderse que procedería oírlos igualmente.

Cuestión distinta, más dudosa, es si los padres pueden solicitar la minoración de responsabilidad civil sin letrado y si pueden hacerlo en ese

momento de manera novedosa, sin haber presentado previamente en un escrito de alegaciones, partiendo de la necesaria solicitud a instancia de parte. A nuestro juicio, en interpretación estricta, la falta de presentación de escrito de alegaciones de los responsables civiles supondría que no debería ser tenida en consideración tal solicitud de minoración pues no se introduce en forma en el proceso, sea en el escrito de alegaciones inicial sea en la modificación operada en el mismo en la audiencia tras la práctica de la prueba. En cualquier caso, en interpretación menos formalista, se pudiera admitir la solicitud de moderación efectuada por los padres en el juicio, facultando así al juez para pronunciarse al respecto.

Frente a la sentencia que se dicte, los responsables civiles personados podrán formular recurso de apelación en relación con el pronunciamiento sobre la responsabilidad civil que les resulte desfavorable, entre ellos el relativo a la moderación de la responsabilidad civil del art. 61.3 LORPM, tanto si no ha sido acogida por el juzgador como si se muestra desacuerdo con el *quantum* o minoración establecida en la sentencia.

4. CARGA DE LA PRUEBA. INVERSIÓN DE LA CARGA DE LA PRUEBA

Sobre la base de que la responsabilidad establecida en el art. 61.3 LORPM es de naturaleza solidaria y objetiva, o cuasi objetiva, así como de la discrecionalidad de la moderación, concebida como facultad judicial excepcional, no sólo corresponde al responsable solidario la obligación de solicitarlo en tiempo y forma, sino que recae sobre el mismo la carga de la prueba de los presupuestos o requisitos que le hacen merecedor de la moderación[65].

De esta forma, sobre la parte que alega los hechos o circunstancias sobre los cuales construye su solicitud de moderación de la responsabilidad recae la carga de su cumplida acreditación, con la consecuencia inherente de que la falta de prueba suficiente sobre tales extremos determinará el rechazo de lo peticionado, y así se advierte de manera reiterada por parte de nuestros tribunales[66].

En relación con la carga de la prueba para la aplicación de la facultad moderadora de la responsabilidad civil, no sólo dicha carga pesa sobre los

65. DE LA ROSA CORTINA (*Responsabilidad civil por daños…*, *op. cit.*, p. 371), considera, en cuanto a la carga de la prueba, que quien alega factores fundamentadores de la moderación de la responsabilidad habrá de acreditar cumplidamente su concurrencia.

66. *Ad exemplum* SAP Madrid 89/2010, de 5 de mayo; SAP Burgos 227/2010, de 11 de noviembre; SAP Zaragoza 328/2011, de 26 de septiembre.

responsables civiles, sino que opera una inversión de la carga probatoria en el sentido de que han de ser éstos los que acrediten la concurrencia de los presupuestos precisos para acceder a tal minoración, esto es, que no favorecieron con dolo o negligencia grave la conducta del menor.

Por ende, en base a la inversión de la carga de la prueba deberán ser los padres los que prueben que han empleado las precauciones adecuadas para impedir la actuación delictiva del menor de forma que si no prueban en modo alguno que obraron con la diligencia debida en su deber de vigilancia, educación y formación integral respecto del menor, de que se han observado activamente las precauciones suficientes y adecuadas, con las medidas de control o límites adecuados[67]. En todo caso, no es suficiente su mera invocación sino una auténtica actividad probatoria[68].

Ahora bien, pese a lo anterior, no se puede obviar que ante determinadas situaciones, más bien excepcionales, en que se evidencia la inexistencia de la infracción de cualquier deber por parte de los padres se puede relajar las exigencias derivadas de la carga de la prueba y su inversión[69].

5. OBJETO DE PRUEBA

En cuanto al objeto de la prueba, los padres, y en general cualesquiera obligados solidarios, deberán intentar acreditar que no han favorecido

67. La SAP Cáceres 216/2021, de 30 de julio, señala que el art. 61.3 LORPM implica una verdadera inversión de la carga de la prueba, puesto que una vez que el Ministerio Fiscal y las acusaciones, en su caso, hayan logrado desvirtuar la presunción de inocencia y se declare culpable al menor, le corresponde a este y a sus responsables civiles solidarios demostrar que procede la moderación. Son ellos los que deben probar y acreditar que han empleado las precauciones adecuadas para impedir la actuación delictiva del menor de forma que si no prueban en modo alguno que obraron con la diligencia debida en su deber de vigilancia, educación y formación integral respecto del menor, no procederá moderación alguna; la SAP Guipúzcoa 101/2021, de 23 de julio advierte de una inversión en la carga probatoria para proceder a la moderación, de manera que es a los padres o asimilados que invocan la procedencia de la moderación, a quienes corresponde acreditar que han empleado las precauciones adecuadas para impedir la actuación delictiva del menor, de forma que cuando no prueben en modo alguno que obraron con la diligencia debida en su deber de vigilancia, educación y formación integral respecto de su hijo/a menor de edad, no procederá efectuar moderación; en el mismo sentido SAP Jaén 222/220, de 9 de diciembre; SAP Ourense 348/2012 de 26 de septiembre.

68. La SAP Guipúzcoa 101/2021, de 23 de julio, advierte que no se trata de una mera invocación sino de una auténtica actividad probatoria pues deben probar y acreditar que han empleado las precauciones adecuadas para impedir la actuación delictiva del menor de forma que, si no prueban que obraron con la diligencia debida en su deber de vigilancia, educación y formación integral respecto del menor, no procederá moderación alguna.

69. En tal sentido, citar las SSAP Madrid 36/2007, de 19 de febrero, 221/2007, de 10 de diciembre y 222/2007, de 10 de diciembre.

con su conducta la comisión del delito o, lo que es lo mismo, alegar y probar aquellos presupuestos que conduzcan a determinar que su responsabilidad ha de resultar minorada (cuando no se ha solicitado asimismo que quede excluida).

En consecuencia, como hemos señalado, será objeto de acreditación la inexistencia de dolo o negligencia grave, lo que determina la prueba de una actuación diligente en el proceso de educación y socialización, así como en la labor de supervisión, de su hijo menor, o cuando menos que se han desplegado todos los esfuerzos y se han tomado todas las medidas tendentes a su consecución, sin que la falta de recursos económicos o dificultades económicas para afrontar la indemnización sea causa para acceder a la moderación de su responsabilidad civil[70]. En este mismo sentido, también se desplegará prueba a fin de probar las circunstancias concurrentes tanto en el propio menor, personales y formativas, como respecto de los hechos acaecidos.

En relación a esas premisas generales, en el plano particular de la comisión de delitos informáticos o tecnológicos, la prueba podrá consistir en la existencia de una formación o información sobre el correcto uso de internet, sistemas o controles de seguridad tendentes a la prevención de delitos, o controles parentales o de supervisión, de los que se desprenda una actuación diligente en el proceso de educación y socialización en internet y redes sociales así como de supervisión en su uso, si bien no se puede obviar, desde luego, las dificultades y obstáculos que entraña lo anterior tanto por privacidad como por efectividad.

6. MEDIOS DE PRUEBA

Al objeto de acreditar los hechos y extremos referidos en orden a obtener la minoración judicial de la responsabilidad civil, el responsable solidario, en este caso los padres del menor infractor pueden valerse de todos los medios de prueba admitidos en Derecho[71].

De manera especial ha de resaltarse, por su valor y trascendencia a efectos probatorios, el Informe del Equipo Técnico[72], que se regula en el art. 27 LORPM y es de emisión preceptiva en el Expediente de Menores, siendo asimismo obligada la declaración de un miembro de la Equipo Técnico

70. SAP Alicante 372/2015, de 7 de septiembre.
71. DE LA ROSA CORTINA (*Responsabilidad civil por daños…*, *op. cit.*, p. 378) advierte que pueden emplearse cualesquiera medios probatorios admitidos en Derecho, incluido el informe del Equipo Técnico.
72. SAP Alicante, Sección 2.ª, 41/2017, de 6 de febrero.

en la audiencia o juicio; sin que se pueda obviar, a efectos probatorios, su consideración como prueba pericial, sin perjuicio de analizar en cada caso su contenido y el modo en que se alcanzan las conclusiones[73].

Sin perjuicio de lo anterior, la parte puede valerse de cualesquiera otros medios de prueba como prueba documental, informes o dictámenes, relativos a la conducta del menor, estudios, actividades, así como atinentes a las actuaciones o actividades de los responsables en orden a acreditar el cumplimiento de los deberes de deber de vigilancia, educación y formación respecto de los menores, tanto a nivel general como de nuevas tecnologías en particular.

V. CONCLUSIONES

Las nuevas tecnologías y el uso generalizado de internet en nuestra sociedad han determinado el aumento de la comisión de delitos tecnológicos o informáticos, la ciberdelincuencia, expansión que, como no puede ser de otro modo, también ha tenido lugar entre nuestros jóvenes. Estos tipos delictivos conllevan, en muchas ocasiones, las correspondientes responsabilidades civiles, con indemnizaciones que pueden ser cuantiosas y de las cuales han de responder, junto a los menores infractores, los padres, tutores, acogedores y guardadores legales o de hecho, como sujetos obligados solidarios.

El sistema de responsabilidad civil que ha sido pergeñado por la LORPM tiende a beneficiar a las víctimas/perjudicados, en detrimento de los responsables civiles solidarios, de suerte que para éstos resulta un régimen de responsabilidad muy gravoso.

A mitigar ese rigor contribuye, en cierto modo, la facultad de moderación de la responsabilidad civil prevista en el art. 61.3 LORPM, que es de carácter discrecional y cuya aplicación, atendida su propia configuración, deviene excepcional. En todo caso, esa moderación judicial no excluye la responsabilidad, sino que, únicamente, puede tener un efecto reductor de la misma.

73. DE LA ROSA (*Responsabilidad civil por daños…*, *op. cit.*, pp. 378-381) señala que, con frecuencia, la prueba sobre la que se articula la petición de moderación es la valoración de las circunstancias educativas y familiares incluida en el informe del Equipo Técnico, de manera que en este ámbito podríamos considerar a tal pericia como *regina probatorum* en este ámbito. Ahora bien, los datos fácticos sobre los que el Equipo llega a conclusiones pueden ser refutados por cualesquiera otros medios probatorios. No puede exacerbarse el valor de afirmaciones fácticas que en ocasiones se basan en lo que el propio menor infractor y sus padres refieren al Equipo Técnico.

En lo que atañe a la carga de la prueba para la aplicación de la facultad moderadora, recae sobre el sujeto obligado solidario, operando como una auténtica inversión de la carga de la prueba.

En cualquier caso, el régimen sobre responsabilidad civil diseñado por la LORPM es deficitario y está mal sistematizado, lo que aconseja una reforma legal del mismo que la dote de coherencia y confiera seguridad jurídica al sistema.

Guía de uso

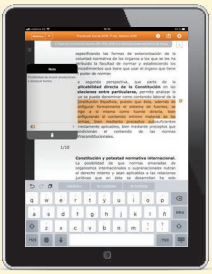
¡ENHORABUENA!

ACABAS DE ADQUIRIR UNA OBRA QUE **INCLUYE LA VERSIÓN ELECTRÓNICA.**
APROVÉCHATE DE TODAS LAS FUNCIONALIDADES.

ACCESO INTERACTIVO A LOS MEJORES LIBROS JURÍDICOS

ARANZADI

FUNCIONALIDADES



SELECCIONA Y DESTACA TEXTOS

Crea anotaciones y escoge los colores para organizar tus notas y subrayados.

USA EL TESAURO PARA ENCONTRAR INFORMACIÓN

Al comenzar a escribir un término, aparecerán las distintas coincidencias del índice del Tesauro relacionadas con el término buscado.

HISTÓRICO DE NAVEGACIÓN

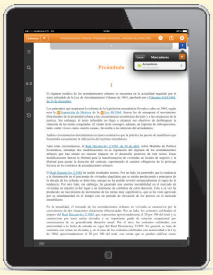
Vuelve a las páginas por las que ya has navegado.

ORDENAR

Ordena tu biblioteca por: Título (orden alfabético), tipo (libros y revistas), editorial, jurisdicción o área del Derecho.

CONFIGURACIÓN Y PREFERENCIAS

Escoge la apariencia de tus libros y revistas en ProView cambiando la fuente del texto, el tamaño de los caracteres, el espaciado entre líneas o la relación de colores.

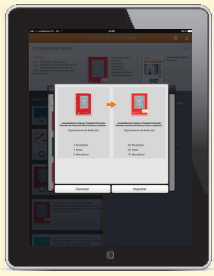


MARCADORES DE PÁGINA

Crea un marcador de página en el libro tocando en el icono de Marcador de página situado en el extremo superior derecho de la página.

BÚSQUEDA EN LA BIBLIOTECA

Busca en todos tus libros y obtén resultados con los libros y revistas donde los términos fueron encontrados y las veces que aparecen en cada obra.



IMPORTACIÓN DE ANOTACIONES A UNA NUEVA EDICIÓN

Transfiere todas sus anotaciones y marcadores de manera automática a través de esta funcionalidad.

SUMARIO NAVEGABLE

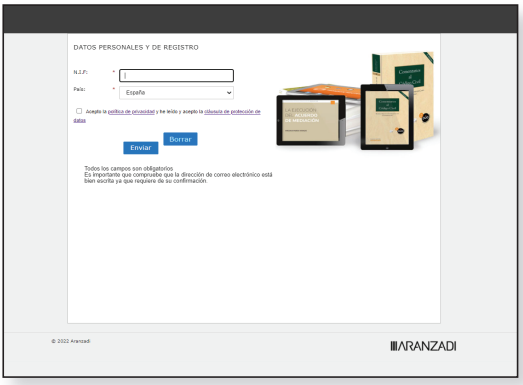
Sumario con accesos directos al contenido.

ARANZADI

INFORMACIÓN IMPORTANTE: Si has recibido previamente un correo electrónico deberás seguir los pasos que en él se detallan.

Estimado/a cliente/a,

Para acceder a la versión electrónica de este libro, por favor, accede a **http://onepass.aranzadi.es** Tras acceder a la página citada, introduce tu dirección de correo electrónico (*) y el código que encontrarás en el interior de la cubierta del libro.



A continuación pulsa enviar.

Si te has registrado anteriormente en OnePass, en la siguiente pantalla se te pedirá que introduzcas el NIF asociado al correo electrónico.

Finalmente, te aparecerá un mensaje de confirmación y recibirás un correo electrónico confirmando la disponibilidad de la obra en tu biblioteca.

Si es la primera vez que te registras en **OnePass,** deberás cumplimentar los datos para crear tu cuenta y poder acceder a tu libro electrónico.

- Los campos **“Nombre de usuario”** y **“Contraseña”** son los datos que utilizarás para acceder a las obras que tienes disponibles a través del navegador en la ruta www.proview.thomsonreuters.com

Servicio de Atención al Cliente

Ante cualquier incidencia en el proceso de registro de la obra no dudes en ponerte en contacto con nuestro Servicio de Atención al Cliente. Para ello accede a nuestro Portal Corporativo y una vez allí en el apartado del Centro de Atención al Cliente selecciona la opción de Acceso a Soporte para no Suscriptores (compra de Publicaciones).

ARANZADI