Universidad de Valladolid

Facultad de Derecho

Grado en Derecho

Tratamiento procesal de la ciberdelincuencia: En particular el caso "ALCASEC"

Presentado por:

Marina Cueto Cebrián

Tutelado por:

María del Coral Arangüena Fanego

Valladolid, 7 de Julio de 2025

RESUMEN

La creciente digitalización de nuestra sociedad ha traído consigo una nueva dimensión de la criminalidad: la ciberdelincuencia. Mi interés por este fenómeno, y particularmente la elección de este Trabajo de Fin de Grado, surgió de la curiosidad que me despertó el caso "Alcasec". Conocer la figura de este ciberdelincuente y la forma en que sus actividades fueron investigadas y perseguidas judicialmente me llevó a cuestionar cómo nuestro sistema legal aborda este tipo de desafíos.

Es por ello que el presente estudio se orienta, en primer lugar, a ofrecer un breve pero necesario panorama del tratamiento penal que reciben los ciberdelitos en el ordenamiento jurídico español. Sin embargo, el objetivo principal de este trabajo es adentrarse en el tratamiento procesal de la ciberdelincuencia, examinando los mecanismos y herramientas jurídicas que se utilizan para investigar, enjuiciar y obtener prueba en un entorno digital en constante evolución. A lo largo de sus páginas, exploraremos las particularidades y complejidades que presenta la fase procesal, buscando comprender si el marco legal actual es suficiente o si requiere de adaptaciones para garantizar una respuesta judicial eficaz frente a esta forma de criminalidad tan particular.

PALABRAS CLAVE

Delitos informáticos; ciberdelitos; Tecnologías de la Información y la Comunicación (TIC´s); Internet; reforma penal; daños informáticos; estafa informática; privacidad; Internet; prueba digital; hacking; Ley de Enjuiciamiento Criminal (LECrim); responsabilidad jurídica; ciberacoso; amenazas; Alcasec.

ABSTRACT

The increasing digitalization of our society has brought forth a new dimension of criminality: cybercrime. My interest in this phenomenon, and particularly the choice of this Final Degree Project, stemmed from the curiosity sparked by the "Alcasec" case. Learning about this cybercriminal and how his activities were judicially investigated and prosecuted led me to question how our legal system addresses these kinds of challenges.

Therefore, this study primarily aims to offer a brief but necessary overview of the penal treatment cybercrimes receive within the Spanish legal framework. However, the main objective of this work is to delve into the procedural treatment of cybercrime, examining the mechanisms and legal tools used to investigate, prosecute, and obtain evidence in a constantly evolving digital environment. Throughout its pages, we will explore the particularities and complexities presented by the procedural phase, seeking to understand whether the current legal framework is sufficient or if it requires adaptations to ensure an effective judicial response to this highly unique form of criminality.

KEYWORDS

Informatic crime; cybercrime; Information Technology and Communication (ICT); Internet; criminal law reform; computer-related damage; computer fraud; privacy; Internet; digital evidence; hacking; Criminal Procedure Act (LECrim); legal liability; cyberbullying; threats; Alcasec.

ÍNDICE DE ABREVIATURAS

AP:	Audiencia Provincial.
BOE:	Boletín Oficial del Estado.
CC:	Código Civil.
CE:	Constitución española.
CP:	Código Penal.
Dir:	Directiva.
ed:	Edición.
Ej.:	Ejemplo.
LEC:	Ley de Enjuiciamiento Civil.
LECrim:	Ley de Enjuiciamiento Criminal.
LO:	Ley Orgánica.
LOPJ:	Ley Orgánica del Poder Judicial.
pg:	Página.
RD:	Real Decreto.
STC:	Sentencia del Tribunal Constitucional.
STS:	Sentencia del Tribunal Supremo.
ss:	Siguientes.
TC:	Tribunal Constitucional.
TICs:	Tecnologías de la información y la comunicación.
TS:	Tribunal Supremo.
INCIBE:	Instituto Nacional de Ciberseguridad

ÍNDICE

1. INTRODUCCIÓN

2. CIBERDELINCUENCIA

2.1- Definición

2.2- Características

2.3- Marco normativo

2.4- Tratamiento penal

2.4.1- Ciberdelincuencia económica

2.4.2- Ciberdelincuencia intrusiva

2.4.3- Ciberespionaje

2.5- Tratamiento procesal

2.5.1- Investigación: medidas previstas en la Ley de Enjuiciamiento Criminal (LECrim)

2.5.2- Cooperación judicial en ciberdelincuencia internacional

2.5.3- Particularidades en la denuncia

2.5.4- Fase de instruccion y práctica de la prueba

3. EL CASO ALCASEC Y SUS IMPLICACIONES PROCESALES

3.1 Contexto del caso Alcasec y hechos relevantes

3.2 Análisis procesal del caso

3.2.1- Procedimientos policiales y judiciales

3.2.2- Pruebas digitales: recolección, autenticidad y cadena de custodia

3.2.3- Estrategias de defensa y acusación

3.3 Implicaciones legales y éticas

3.3.1- Protección de derechos fundamentales

3.3.2- Ciberseguridad y protección de infraestructuras críticas

3.3.3- Responsabilidad penal de los menores en delitos informáticos

4. PROPUESTAS DE MEJORA EN LA LUCHA CONTRA LA CIBERDELINCUENCIA.

4.1- Reformas legales para el tratamiento de delitos informáticos

4.2- Necesidades de formación en ciberseguridad para operadores jurídicos

4.3- Estrategias para prevenir y mitigar el hacking

5. CONCLUSIONES

6. REFERENCIAS BIBLIOGRÁFICAS

1. INTRODUCCIÓN

En la actualidad, vivimos en una sociedad cada vez más interconectada a nivel global, donde, a medida que avanzan los años y se desarrollan la economía, la sociedad, la cultura y la tecnología, los diferentes Estados se vinculan de manera creciente entre sí, lo que genera una serie de consecuencias en diversos ámbitos.

Desde el ámbito político hasta el demográfico, la globalización ha acercado a los Estados, permitiendo que sus interacciones sean más frecuentes y que puedan influenciarse mutuamente de manera más directa.

Entre las múltiples causas que impulsan este fenómeno, la tecnología destaca como factor clave y podemos observar sus efectos a través de los nuevos mecanismos e instrumentos que facilitan y simplifican nuestras vidas.

No obstante, este progreso no ha estado exento de consecuencias negativas. En los últimos años, debido a la rápida evolución de las tecnologías, ha emergido un fenómeno conocido como los "ciberdelitos" o delitos informáticos[1], que se refieren a aquellas conductas delictivas dirigidas contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.

Estos delitos tienen un impacto directo sobre todos nosotros, tanto a nivel individual como en diversos aspectos de nuestro desarrollo social. Estos afectan a derechos fundamentales como la intimidad, la protección de datos, y la libertad de expresión e información. Además, inciden en derechos de naturaleza socioeconómica, tales como la propiedad digital o el teletrabajo. En este contexto, la legislación no puede permanecer ajena a estos desafíos, ni nosotros podemos ignorarla (*ignorantia iuris non excusat*).

Mi interés por este fenómeno, y particularmente la elección de este Trabajo de Fin de Grado, surgió de la curiosidad que me despertó el caso "Alcasec". Este caso, de actualidad reciente, es un ejemplo claro de cómo el incesante avance de la tecnología ha propiciado el surgimiento de una nueva clase de delitos que desafían los marcos legales existentes. Conocer la figura de este ciberdelincuente y la forma en que sus actividades fueron investigadas y perseguidas judicialmente me llevó a cuestionar cómo nuestro sistema legal aborda este tipo de desafíos.

[1]ROSSO PEREZ, M. E. (10 de febrero, 2020). "Delitos informáticos o a través de medios telemáticos (I)"en *LegalToday*

Por ello el presente estudio se orienta, en primer lugar, a ofrecer un breve pero necesario panorama de cómo se encuentran actualmente regulados los ciberdelitos en nuestro Código Penal (CP), sirviendo de contextualización fundamental. Posteriormente, nos adentraremos en el tratamiento procesal de la ciberdelincuencia, examinando los mecanismos y herramientas jurídicas que se utilizan para investigar, enjuiciar y obtener prueba en un entorno digital en constante evolución. Asimismo, abordaremos a grandes rasgos el particular caso "Alcasec" como ilustración práctica de las complejidades que presenta la fase procesal. Finalmente, y basándonos en el análisis realizado, propondré diversas propuestas de mejora para potenciar la lucha eficaz contra estos delitos tan particulares.

2. CIBERDELINCUENCIA

2.1- Definición

En un contexto de interconexión constante, debido en parte al vertiginoso avance que han sufrido las tecnologías de la información y la comunicación (TIC) y la expansión de Internet a finales del siglo XX han surgido nuevas formas de conductas delictivas, que reciben el nombre de *ciberdelincuencia*.

Cuando se hace referencia a los delitos informáticos, se está aludiendo a una categoría delictiva que se caracteriza por la intervención de elementos tecnológicos en su comisión. En otras palabras, se trata de conductas ilícitas en las que intervienen dispositivos o sistemas informáticos como medio o fin del delito.

Cabe señalar que, en el ordenamiento jurídico español, no existe una definición explícita del término *ciberdelincuencia*. La Ley Orgánica 10/1995, de 23 de noviembre, del CP, a lo largo de sus 36 títulos, no contempla una delimitación conceptual específica de esta forma de criminalidad. No obstante, es posible identificar diversas conductas que, por sus características, pueden enmarcarse dentro de lo que comúnmente se entiende por ciberdelincuencia, como podrían ser el fraude informático (art. 248 del CP), delitos contra la intimidad y la seguridad informática (Art 197 y ss del CP), delitos contra la propiedad intelectual e industrial (Art 270 y ss del CP), entre otros.

No obstante, de acuerdo con la definición proporcionada por Ortiz Pradillo, la ciberdelincuencia puede entenderse como un *"fenómeno delictivo de rápida propagación bajo el cual se englobarían todos aquellos delitos que puedan cometerse por medio de un equipo conectado a una red informática"*[2]. Por tanto, esta modalida delictiva se distingue por la utilización del ciberespacio[3] como vehículo para ejecutar múltiples actividades ilícitas o, incluso, como medio de ataque a los archivos o programas de los propios sistemas informáticos[4].

El ámbito delictivo en el entorno digital es amplio y diverso, pudiéndose incluir conductas como amenazas, estafas, acoso..… No obstante, algunos autores sostienen que la mera utilización de herramientas tecnológicas para la comisión de un delito no cambia ni su naturaleza ni las reglas tradicionales de la vigencia espacial de la ley penal.

---

[2] ORTIZ PRADILLO, J.C.(2013), *Problemas procesales de la Ciberdelincuencia*, Cólex, p. 17.
[3] Entorno virtual conformado por páginas web, servicios en línea, chats y usuarios interconectados a través de Internet.
[4] ORTIZ PRADILLO, J.C.(2013), *Problemas procesales…* op.cit, p. 18.

2.2- Características

Tal y como establece Velasco Núñez, la delincuencia informática presenta un conjunto de peculiaridades respecto de la delincuencia tradicional. Por ello, es preciso un tratamiento procesal y penal que lo caracterice y diferencie los demás tipos delictivos; de lo contrario, la situación puede llegar a producir una verdadera impunidad, si no se articulan los remedios adecuados [5].

Estas características, entre otras, son:

- No existe una única forma de comisión de este delito. Este abarca una gran variedad de conductas que comparten como característica común, la utilización de algún tipo de medio tecnológico para su ejecución (ordenadores, teléfonos móviles u otros medios telemáticos) .

- Se cometen a distancia, sin posibilidad de recibir una reacción por parte de la víctima.

- Se llevan a cabo de forma instantánea en el tiempo.

- Pueden ser delitos masa que, ya que pueden afectar a un número elevado de víctimas que normalmente son anónimas y desconocidas.

En este sentido, se alude al concepto de "delito masa", entendido como aquel por el cual el sujeto activo, mediante una sola acción o por varias acciones que, consideradas independientemente, constituiría cada una de ellas un delito o falta, pone en ejecución un designio criminal único encaminado a defraudar a una masa de personas[6].

Esta circunstancia abre la posibilidad de acumulación procesal de los delitos, conforme a lo dispuesto en el artículo 17 de la Ley de Enjuiciamiento Criminal (LECrim).

- Los autores de estos delitos no son necesariamente individuos con avanzados conocimientos técnicos o especializados en informática, como pueden ser los conocidos *hackers* o *crackers*. En muchos casos, los responsables son personas sin formación específica en tecnología, pero con acceso a Internet y habilidades básicas en el uso de dispositivos digitales[7].

---

[5] DÍAZ GÓMEZ, A. (2010) El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest, REDUR 8. [En línea], p,174 <http://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf > [Consulta: 7 julio 2025].

[6] SAINZ CANTERO, J. A. (1971). "El delito masa". *Anuario de Derecho Penal y Ciencias Penales,* p. 664.

[7] GÓMEZ TOMILLO, M. (1998), *Libertad de información y teoría de la codelincuencia. La autoría y la participación en los delitos cometidos a través de los medios de comunicación de masas,* Comares, Granada, pp. 126 y ss.

- Suelen tener un claro componente internacional, ya que afectan a personas ubicadas en zonas geográficas diferentes, y puede atacarse a múltiples bienes jurídicos protegidos (la seguridad, la intimidad, la dignidad, el patrimonio…)[8] .Lo que genera en ocasiones conflictos en cuanto a la determinación de la ley aplicable.

Ante este tipo de conflictos, la doctrina y la jurisprudencia han recurrido, por regla general, a la denominada *teoría de la ubicuidad,* permitiendo atribuir competencia al Estado tanto en el lugar en que se inició la acción delictiva como en aquel donde se materializó su resultado. En este sentido, y conforme a dicha teoría, España sería competente para conocer de estos delitos si en su territorio se llevó a cabo parte de la acción ilícita o se produjo el efecto delictivo.

De este modo, mientras internet se ha convertido en un medio de comunicación mundial, el espacio por el que este se extiende es plurijurisdiccional, repartido entre una multitud de órganos judiciales que desarrollan sus funciones en ámbitos territoriales concretos y que incluso llegan a alcanzar, como máximo, el espacio del Estado al que pertenecen [9].

- Como ya mecionamos anteriormente, estos delitos no se encuentran sistematizados de forma unificada en el CP español. Se hallan dispersos en diferentes Títulos de la parte especial, lo que complica su identificación y clasificación. Esta dispersión normativa exige, en ocasiones, una interpretación extensiva de determinados tipos penales, especialmente cuando estos no contienen expresamente elementos tecnológicos, como sucede, por ejemplo, con el delito de injurias.

- Por último, uno de los principales desafíos que plantea la ciberdelincuencia radica en la dificultad para la investigación y verificación de los hechos delictivos. Estas dificultades afectan tanto a la posibilidad de identificar y procesar a los responsables como a la adopción de medidas eficaces para prevenir o mitigar los efectos de estas conductas. Ello se debe, en gran medida, a la facilidad con la que los autores pueden ocultar su identidad en la red, recurriendo a herramientas de anonimato, encriptación y sistemas de codificación avanzada

[8] VELASCO NÚÑEZ, E. (2010), *Delitos cometidos a través de Internet. Cuestiones procesales*, La Ley, Madrid, p. 47.
[9] MUÑOZ MACHADO, S. (2000). *La regulación de la red. Poder y Derecho en Internet.* Taurus, Madrid, p. 221.

2.3- Marco normativo

Antes de analizar la normativa aplicable, conviene reflexionar sobre el tratamiento jurídico que recibe la ciberdelincuencia. El desarrollo de las TIC ha transformado profundamente la sociedad, generando debate en la doctrina sobre si nos encontramos ante una forma autónoma de criminalidad o si, por el contrario, se trata de conductas tradicionales cometidas a través de nuevos medios. Aunque no existe una posición unánime, lo cierto es que en España esta evolución ha llevado al legislador a adaptar el marco legal, ampliando su alcance para dar respuesta a los retos del entorno digital**.**

Pese a que el ordenamiento jurídico español no reconoce los delitos informáticos como una categoría penal diferenciada, sí existen numerosas disposiciones legales, tanto a nivel interno como internacional, que regulan conductas vinculadas a la criminalidad digital. Por ello, este apartado se centrará en examinar el marco normativo nacional, los tratados internacionales ratificados por España y las directrices emanadas de la Unión Europea, todos ellos relevantes para la lucha contra los ciberdelitos.

Asimismo, se abordará brevemente el papel de la Estrategia de Seguridad Nacional en materia de ciberseguridad, como instrumento clave para la prevención y gestión de amenazas en el ámbito digital.

En cuanto al marco normativo nacional, resaltar la existencia de un Código de Derecho de la Ciberseguridad. Este constituye una recopilación sistemática de normas relacionadas con el entorno digital, especialmente aquellas enfocadas en la protección de la seguridad nacional, las infraestructuras críticas, la seguridad pública, las telecomunicaciones y el comercio electrónico.

Este compendio también incluye referencias a legislación específica vinculada a la persecución penal de ciberdelitos, como la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, la Ley General de Telecomunicaciones y la Ley de Seguridad Nacional.

El código fue elaborado y publicado por el Instituto Nacional de Ciberseguridad (INCIBE) en colaboración con la Agencia Estatal del Boletín Oficial del Estado, cuya edición más reciente data de mayo de 2024. Cabe destacar que este documento no constituye una ley autónoma, sino una compilación organizada de normas vigentes, tanto de origen nacional como internacional, con el fin de facilitar el acceso a la legislación aplicable en materia de ciberseguridad.

Su contenido se organiza en cinco grandes bloques temáticos:

1. Marco normativo general, que incluye la normativa básica sobre ciberseguridad, tales como la Ley de Seguridad Nacional, la legislación sobre protección de infraestructuras críticas y el Esquema Nacional de Seguridad.

2. Protección de la información y de los sistemas, donde se recogen normas sobre protección de datos, seguridad de la información, y seguridad de redes y sistemas.

3. Regulación penal y garantías digitales, que abarca disposiciones como el Código Penal y la mencionada Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

4. Ciberdefensa, centrado en la normativa relativa a la defensa nacional en el entorno digital, entre ellas la Estrategia Nacional de Ciberseguridad.

5. Cooperación internacional, donde se incluyen instrumentos como el Convenio de Budapest sobre ciberdelincuencia, clave para la armonización normativa en el ámbito global.

La relevancia de este código radica en su capacidad para integrar y sistematizar normativa dispersa, ofreciendo una herramienta útil tanto para operadores jurídicos como para instituciones públicas y privadas. Además, contribuye al fortalecimiento del marco normativo nacional en materia de ciberseguridad y al fomento de un uso responsable de las TIC.

Y en lo relativo a la normativa europea, según la web oficial del Consejo Europeo *"se espera que 41.000 millones de dispositivos en todo el mundo estén conectados a la internet de las cosas de aquí a 2025"*, por lo que esta tendencia incrementara en los años venideros.

Esta proyección pone de manifiesto la magnitud del desafío que representa la cibercriminalidad y la necesidad urgente de establecer un marco legal sólido y coordinado a nivel internacional.

Uno de los instrumentos más relevantes en este ámbito es el Convenio sobre la Ciberdelincuencia, comúnmente conocido como el Convenio de Budapest, firmado en esa ciudad el 23 de noviembre de 2001. Este tratado internacional, promovido por el Consejo de Europa, se orienta a reforzar la cooperación entre Estados en la lucha contra la delincuencia digital, especialmente en lo relativo al acceso ilícito a sistemas, la integridad de los datos, la utilización indebida de redes y el tráfico de contenido ilegal.

El Convenio reconoce la profunda transformación provocada por la digitalización, la convergencia tecnológica y la globalización de las comunicaciones, y responde a ello proponiendo mecanismos para:

- Garantizar la protección de la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos.
- Tipificar penalmente conductas relacionadas con el uso fraudulento de las tecnologías de la información.
- Facilitar la cooperación internacional en la investigación, persecución y enjuiciamiento de los delitos cometidos en el entorno digital.

Asimismo, el tratado establece un equilibrio entre los poderes del Estado en la persecución penal y la necesidad de respetar los derechos fundamentales, entre ellos la libertad de expresión, la protección de datos personales y el derecho a la privacidad.

Junto al Convenio de Budapest, destaca la Directiva 2013/40/UE, aprobada el 12 de agosto de 2013 por el Parlamento Europeo y el Consejo. Esta norma reemplaza a la anterior Decisión Marco 2005/222/JAI, y tiene como finalidad armonizar la legislación penal de los Estados miembros en relación con los ataques dirigidos contra sistemas de información.

La Directiva establece:

- Definiciones comunes de infracciones penales relacionadas con la cibercriminalidad.
- Sanciones mínimas que los Estados deben aplicar.
- Mecanismos para mejorar la cooperación entre las autoridades competentes y entidades europeas especializadas como Europol, Eurojust y ENISA (Agencia de la Unión Europea para la Ciberseguridad).

La protección de los sistemas de información se considera un elemento esencial para asegurar la estabilidad del mercado interior europeo y fomentar una economía innovadora, competitiva y segura en el contexto digital actual.

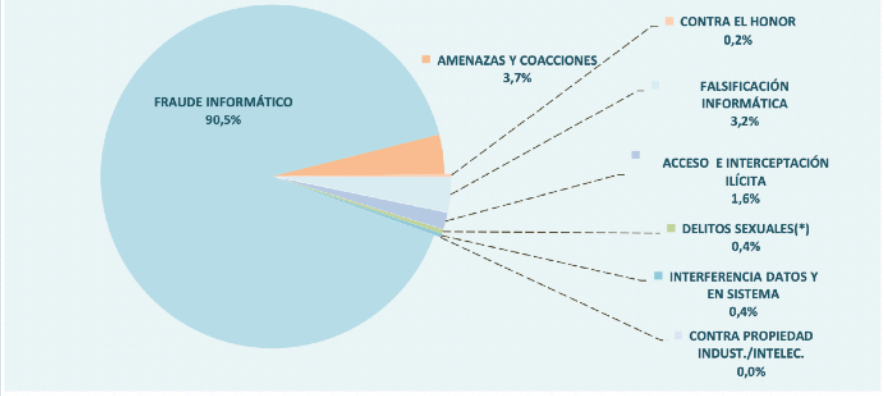
2.4- Tratamiento penal

La constante evolución de la criminalidad, especialmente en el ámbito digital, también exige una respuesta contundente por parte del Derecho Penal. Su objetivo primordial es controlar y prevenir estos nuevos comportamientos delictivos, priorizando la protección de bienes jurídicos a través de la prevención de acciones que generen riesgos. Este enfoque se alinea con la doctrina del "peligro abstracto"[10].

De acuerdo con los datos proporcionados por el Ministerio del Interior[11], en 2023 más de 17.000 personas fueron detenidas/investigadas por la comisión de delitos informáticos, siendo el fraude, el delito más cometido, a una considerable distancia del de las amenazas y coacciones, así como las injurias y calumnias.

HECHOS CONOCIDOS	2019	2020	2021	2022	2023
ACCESO E INTERCEPTACIÓN ILÍCITA	4.004	4.653	5.342	5.578	7.367
AMENAZAS Y COACCIONES	12.782	14.066	17.319	15.982	17.472
CONTRA EL HONOR	1.422	1.550	1.426	1.191	1.174
CONTRA PROPIEDAD INDUST./INTELEC.	197	125	137	114	64
DELITOS SEXUALES(*)	1.774	1.783	1.628	1.646	1.804
FALSIFICACIÓN INFORMÁTICA	4.275	6.289	10.476	12.569	15.137
FRAUDE INFORMÁTICO	192.375	257.907	267.011	335.995	427.448
INTERFERENCIA DATOS Y EN SISTEMA	1.473	1.590	2.138	1.662	1.659
Total HECHOS CONOCIDOS	**218.302**	**287.963**	**305.477**	**374.737**	**472.125**

(*)Excluidas las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



Cabe señalar que, la cifra de denuncias sigue siendo relativamente baja, muchas de las personas afectadas por estos delitos no los denuncian debido a la complejidad que presenta la persecución de los delincuentes, ocultos en el ámbito virtual. De este modo, se estima que el número real de delitos informáticos es considerablemente mayor al reflejado en las estadísticas.

[10] BUSTOS RUBIO, M. (2017). *Delitos acumulativos y delitos de peligro abstracto: el paradigma de la acumulación en el derecho penal.* ADPCP. Universidad de La Rioja, La Rioja. pp. 296–303.

[11] MINISTERIO DEL INTERIOR (2023). Informe sobre la cibercriminalidad en España 2023. https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf

A diferencia de otros contextos del Derecho penal, como los delitos relacionados con la integridad física o el patrimonio (por ejemplo, una pelea o un hurto), las víctimas de ciberdelitos no suelen identificarse como tales. Además, no son plenamente conscientes de la gravedad que estos delitos implican para la sociedad, dado que las consideran normales y frecuentes.

En lo relativo al marco jurídico que regula esta materia, decir que, este ha experimentado una evolución significativa en relación con las nuevas realidades tecnológicas, desde las reformas de los códigos penal y procesales, hasta las normativas que regulan la firma electrónica y el comercio electrónico. Entre las normativas más relevantes se encuentran la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, el Real Decreto-ley 12/2018, de 7 de septiembre, sobre la seguridad de redes y sistemas de información, así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

El Derecho interno debe regular los diversos aspectos derivados de las nuevas formas de convivencia, o más específicamente, del uso que posibilita esa convivencia digital. Sin embargo, el Derecho no debe avanzar al mismo ritmo que la tecnología. Su objetivo debe ser asegurar una permanencia en el tiempo, lo cual no puede lograrse si se intenta abordar de inmediato cada nueva innovación que surge en nuestra vida cotidiana.

A efectos de una mayor claridad expositiva, procederé a efectuar una triple distinción y a examinar la clasificación aportada en la doctrina, en las instituciones y en las normas (la económica, la intrusiva y el ciberespionaje). Todas estas clasificaciones responden a distintas maneras de interpretar el contenido de estos delitos. Además esta exposición nos ayudará a relacionar y contextualizar el marco teórico, con el caso práctico que analizaremos posteriormente: el caso *Alcasec*.

2.4.1- Ciberdelincuencia económica

La ciberdelincuencia económica abarca una serie de actividades ilícitas que tienen como objetivo principal la obtención de un beneficio económico apropiándose de bienes ajenos, utilizando para ello las TIC.

Este tipo de delincuencia se ha disparado en los últimos años debido a la digitalización de la sociedad y la economía, presentándose en múltiples formas como fraudes, estafas, blanqueo de capitales a través de criptomonedas, ataques a sistemas bancarios, entre otros.

Según Eloy Velasco Núñez *"esos tipos penales estadísticamente suponen cerca del 80% de los delitos informáticos que se denuncian"*

En el caso de los delitos económicos cometidos en entornos digitales, el bien jurídico protegido presenta un carácter complejo o pluriofensivo.

Por un lado, se vulnera directamente el patrimonio de la víctima, conforme a lo dispuesto en el Título XIII del CP español, que regula los delitos contra el patrimonio y el orden socioeconómico. Por otro lado, se produce una afectación a derechos colectivos o difusos, como la seguridad del entorno digital y la confianza en las TIC.

En el contexto español, un porcentaje significativo de los escritos de acusación formulados por el Ministerio Fiscal corresponde a delitos de estafa cometidos a través de medios informáticos. Se estima que aproximadamente el 45 % de estas acusaciones están vinculadas a estafas de carácter digital, lo que evidencia la creciente relevancia de esta tipología delictiva en el ámbito de la ciberdelincuencia[12].

Además de las conductas anteriores, el CP español recoge también, entre otros:

- La defraudación de servicios (art. 255 CP), que ocurre cuando una persona utiliza servicios como luz, agua o internet sin autorización del titular.

- El hurto de tiempo de telecomunicaciones (art. 256 CP), mediante el uso no autorizado de terminales informáticos.

- El daño informático y denegación de servicio (art. 264 CP), que sanciona tanto la alteración o eliminación de datos como la interrupción de sistemas ajenos, especialmente cuando estas acciones afectan servicios esenciales o se realizan en el contexto de organizaciones criminales.

- Los delitos contra la propiedad intelectual e industrial (art. 270 CP), que penalizan la reproducción, distribución o plagio de obras protegidas a través de medios digitales sin el consentimiento de sus autores, incluyendo también modalidades como la elusión de sistemas de protección digital.

[12] MINISTERIO DEL INTERIOR. (2022). Balance de criminalidad: Informe anual sobre delitos informáticos. Gobierno de España.

El caso Alcasec es un ejemplo paradigmático y altamente relevante para comprender la ciberdelincuencia económica. Este individuo, fue investigado por la naturaleza de sus acciones, una serie de intrusiones informáticas, como el acceso no autorizado a sistemas, la extracción de datos y el potencial de su monetización, situándolo por tanto de esta forma, en el ámbito de la ciberdelincuencia económica.

2.4.2- Ciberdelincuencia intrusiva

Esta rama de la ciberdelincuencia comprende aquellas conductas delictivas cometidas a través de medios tecnológicos que suponen una intromisión ilegítima en la esfera personal de las personas, especialmente cuando se ven afectados datos sensibles, la vida íntima, o la dignidad sexual, en particular de personas vulnerables como los menores. En este contexto, el bien jurídico protegido por el Derecho Penal es la privacidad, la integridad moral y, en ciertos casos, el desarrollo psicoafectivo y sexual del individuo.

Este tipo de ciberdelitos se caracteriza por vulnerar derechos fundamentales mediante el uso de tecnologías digitales, afectando gravemente la intimidad y seguridad de las víctimas. Algunos de los delitos más representativos en esta categoría son:

- Las amenazas y coacciones informáticas (art. 169 y 172 del CP)
- La distribución de material pornografíco y pornografía infantil (art. 186 a 189 del CP), que sanciona la producción, distribución, adquisición o posesión de material sexualmente explícito donde intervienen menores de edad.
- El descubrimiento y revelación de secretos (art. 197 CP).
- Las injurias y calumnias informáticas (art. 205 a 216 CP), consistente en el acoso o captación de menores por parte de adultos con fines sexuales.
- El descubrimiento y revelación de secretos (art. 197 CP), que penaliza la obtención y difusión no autorizada de información confidencial.

2.4.3- Ciberespionaje

El espionaje informático se enmarca dentro de los delitos contra el patrimonio y el orden socioeconómico, se tratan de ataques por medio de medios informáticos contra intereses supraindividuales. Constituyen el tipo de ataques más graves, que afectan de forma indiscriminada a intereses generales de la población con la intención de crear pánico y terror para subvertir el sistema político o de convivencia generalmente aceptado.

Apenas tienen incidencia estadística, pero su realización, por afectar a la población en general, genera una alta intranquilidad y desasosiego. También cabría incluir dentro de este grupo, la usurpación de funciones públicas (art. 402 CP) o el descubrimiento y revelación de secretos relativos a la defensa nacional (arts. 598 y 603 CP)

Las TIC han potenciado la capacidad de transferir rápidamente estos fondos entre jurisdicciones, empleando plataformas digitales, criptomonedas o cuentas offshore, dificultando su rastreo y facilitando su legitimación aparente. En este ámbito, el artículo 301 del CP contempla penas severas para quienes participen en actividades destinadas a ocultar o encubrir el origen ilícito de los bienes.

Alcasec fue acusado de haber accedido ilegalmente a bases de datos de la Seguridad Social, universidades, empresas de telecomunicaciones y hospitales. En muchos casos, no lo hizo para robar dinero, sino para: obtener datos personales, sanitarios o académicos; analizar estructuras de las plataformas digitales o crear herramientas para acceder a otras redes más complejas.

Lo cual encajaría con los fines típicos del ciberespionaje, ya que se infiltra para obtener un gran volumen de información sensible sin autorización, aunque no la usara directamente con fines políticos.

2.5- Tratamiento procesal

La ciberdelincuencia presenta una serie de particularidades que intensifican tanto su complejidad como su impacto, lo que la convierte en un desafío significativo para el ordenamiento jurídico. La evolución constante del entorno digital ha puesto de manifiesto la necesidad de una respuesta normativa ágil y eficaz. En este sentido, el papel del legislador es fundamental, ya que debe adaptar el marco legal vigente a los nuevos riesgos, incorporando tanto agravantes genéricas

como específicas que respondan adecuadamente a la naturaleza de estas conductas delictivas [13].

El vertiginoso avance tecnológico y su rápida incorporación en la vida cotidiana han obligado a replantearse la protección de determinados derechos fundamentales. Aunque estos derechos conservan su primacía constitucional, la forma en que deben ser garantizados en el ámbito digital requiere una revisión profunda.

En el caso español, aún se detectan deficiencias normativas en el tratamiento de la ciberdelincuencia. Parte de esta debilidad normativa se debe a la falta de actualización de instrumentos internacionales relevantes, como el Convenio sobre la Ciberdelincuencia del Consejo de Europa y la Directiva 2013/40/UE. Esta situación genera espacios de impunidad y subraya la urgencia de reformar tanto el Código Penal como las normas procesales, para tipificar de forma precisa las nuevas manifestaciones delictivas que surgen en el ciberespacio [14].

2.5.1- Investigación: medidas previstas en la Ley de Enjuiciamiento Criminal (LECrim)

La fase inicial de una investigación penal en el ámbito de la ciberdelincuencia suele originarse a partir de una denuncia formulada por las personas afectadas. En otros supuestos, la actuación policial puede motivar una petición formal al órgano judicial para que autorice determinadas diligencias dirigidas a los proveedores de servicios de Internet. Estas diligencias tienen como finalidad identificar a los titulares de direcciones IP concretas y rastrear las conexiones realizadas desde ellas.

Una vez aceptada la solicitud, el órgano judicial pone en marcha el procedimiento legal correspondiente y, en función de la gravedad del caso y de los indicios obtenidos, puede autorizar actuaciones más intrusivas, como el registro de un domicilio o sede relacionada con la línea investigada, o incluso la intervención de comunicaciones. Estas actuaciones permiten el acceso a dispositivos electrónicos y la recopilación de copias de archivos relevantes para la investigación.

Debido al notable crecimiento de las infracciones cometidas a través de medios tecnológicos, las fuerzas y cuerpos de seguridad han desarrollado unidades especializadas en ciberdelincuencia, tanto en la Policía Nacional como en la Guardia Civil, así como en algunas policías autonómicas.

[13] VELASCO NÚÑEZ, E. (2021). *Delitos tecnológicos. Cuestiones penales y procesales.* Wolters Kluwer España S.A, Madrid, pp 30-32.
[14] VELASCO NÚÑEZ, E. (2021). *Delitos tecnológicos…* op.cit, pp 32-35.

Además, partiendo del modo en el que participan las tecnologías de la información y comunicación, desde el año 2011, existe la llamada Fiscalía General del Estado en la Instrucción 2/2011, del Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías, en las que se establece una clasificación de delitos para tratar de diferenciar los delitos informáticos en sentido estricto de aquellos en los que la informática simplemente aparece de forma incidental.

Se establece un catálogo inicial de delitos informáticos en los que intervendrán fiscales especializados, pero sin limitar en un nu*merus claussus* los tipos penales susceptibles de encuadrarse en la categoría de criminalidad informática, pues según la propia Instrucción (…)*"Es más que previsible la aparición, en un futuro más o menos próximo, de nuevas formas de delincuencia o nuevos mecanismos de comisión de ilícitos ya tipificados, en los que el elemento determinante sea también utilización de las tecnologías de la información y la comunicación, de forma tal que su análisis y valoración de mande de conocimientos específicos que hagan aconsejable su especialización".*

Conforme al artículo 299 de la LECrim, la fase instructora abarca todas las diligencias orientadas a preparar el juicio y a verificar la existencia del delito, así como las circunstancias que influyen en su tipificación y en la determinación de la responsabilidad penal de los autores. Asimismo, esta fase puede incluir la adopción de medidas cautelares para garantizar tanto la presencia de los investigados como la cobertura de eventuales responsabilidades civiles o patrimoniales.

En el contexto actual, marcado por el constante avance tecnológico, resulta indispensable contar con el apoyo de profesionales especializados para llevar a cabo investigaciones eficaces en materia de ciberdelincuencia. Aunque esta colaboración implica un aumento en los costes económicos y en los plazos de actuación, se considera una inversión necesaria para dar una respuesta adecuada a los desafíos que plantea la criminalidad digital y cumplir con las expectativas de la ciudadanía en términos de seguridad y justicia [15].

[15] BALLESTEROS, M. C. R., & HERNÁNDEZ, J. A. G.(2014) "Cibercrimen: particularidades en su investigación y enjuiciamiento." *Anuario Jurídico y Económico Escurialense,* (47), pp, 209-234.

A nivel europeo, también se han desarrollado organismos clave en la lucha contra los delitos informáticos. Entre ellos destacan Europol, Eurojust y la Agencia de la Unión Europea para la Ciberseguridad (ENISA), cuya labor es esencial para la cooperación transnacional y la armonización de políticas en el ámbito de la seguridad digital[16].

En cuanto al ordenamiento jurídico interno, la LECrim ha sido objeto de reformas para adaptarse a las nuevas exigencias derivadas de la delincuencia tecnológica. Entre otros aspectos, se ha regulado de forma expresa la intervención de comunicaciones como medio de prueba, dada su especial relevancia en la investigación de delitos cometidos mediante el uso de tecnologías de la información.

En el marco del procedimiento abreviado, el artículo 773.2 de la LECrim autoriza al Ministerio Fiscal a llevar a cabo diligencias de investigación por iniciativa propia o a través de la Policía Judicial, incluso antes de la apertura formal de las diligencias judiciales. Una vez iniciado el procedimiento, podrá igualmente solicitar al Juzgado de Instrucción la práctica de las diligencias que considere necesarias para esclarecer los hechos.

Por su parte, el artículo 777 de la LECrim establece, con carácter general, que corresponde al Juez de Instrucción la dirección de la fase investigadora, pudiendo ordenar diligencias directamente o a través de la Policía Judicial, con el objetivo de identificar el hecho delictivo, sus circunstancias y a las personas implicadas.

Estas competencias, así como otras relacionadas con la obtención y práctica de pruebas, se desarrollan en el Libro II de la LECrim, especialmente en los artículos 301 bis, 303, 336, entre otros, que recogen las facultades del juez instructor, las medidas cautelares y los procedimientos técnicos de investigación adaptados a la complejidad de los delitos cometidos en entornos digitales.

No obstante, con la aprobación de la Ley Orgánica 13/2015, de 5 de octubre, se introdujeron importantes reformas en la LECrim, especialmente en el Título VIII del Libro II, cuyo objetivo fue actualizar los instrumentos de investigación penal ante la creciente sofisticación de ciertos delitos, en particular aquellos relacionados con terrorismo, tráfico de drogas y criminalidad cometida a través de medios tecnológicos. Este título se renombró como *"De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución"*, en referencia al derecho fundamental a la intimidad, inviolabilidad del domicilio y secreto de las comunicaciones.

[16] MIRANDA, J. J. C. (2020) *Factor Humano: La Teoría de las Actividades Cotidianas en la Ciberseguridad.* Pp, 25-26

Dentro de estas reformas se encuentran las siguientes medidas relevantes:

• Entrada y registro en lugar cerrado: Continúa siendo necesaria la autorización judicial previa, mediante un auto motivado, además de la presencia del Letrado de la Administración de Justicia (LAJ) durante la diligencia, salvo que exista consentimiento expreso del titular del inmueble. La policía está obligada a informar de forma inmediata sobre los efectos intervenidos y, en su caso, las detenciones que se hayan efectuado (Cap. I).

• Registro de libros y documentos: Según lo previsto en el Cap. II, esta actuación también requiere autorización judicial. En caso de que se considere oportuno, podrá intervenir un perito que asista en la revisión y análisis del contenido registrado.

• Detención y apertura de correspondencia escrita y telegráfica: El Cap. III regula las condiciones bajo las cuales un juez puede autorizar la intervención de comunicaciones postales y telegráficas, incluyendo faxes, burofaxes y giros postales. Cabe destacar que, conforme al artículo 579 bis de la LECrim, los resultados obtenidos a través de esta diligencia podrán ser utilizados en otros procedimientos penales diferentes al que motivó inicialmente la medida.

Estas reformas evidencian la necesidad de adaptar las formas de obtención de prueba a los nuevos métodos de comisión delictiva, especialmente aquellos facilitados por el uso de tecnologías avanzadas. Por este motivo, una de las incorporaciones más relevantes en 2015 fue la regulación detallada de las medidas de investigación tecnológica, recogidas en el Cap. IV.

• Investigación tecnológica: El Cap. IV establece un marco normativo detallado para la aplicación de medidas de investigación tecnológica. Entre las diligencias contempladas se encuentran la intervención de comunicaciones telefónicas y telemáticas, así como la captación y grabación de conversaciones orales a través del uso de dispositivos electrónicos. También se permite el empleo de tecnologías de seguimiento, geolocalización y videovigilancia, así como el registro de soportes digitales de almacenamiento masivo y el acceso remoto a sistemas informáticos. Estas medidas están comprendidas en los artículos 588 bis a) a 588 bis k) de la LECrim.

Para que estas diligencias sean válidas, es imprescindible contar con una autorización judicial mediante auto motivado, en cumplimiento estricto de los principios de especialidad, idoneidad, necesidad, proporcionalidad y excepcionalidad.

Estas medidas pueden ser solicitadas de oficio por el juzgado, a petición del Ministerio Fiscal o de la Policía Judicial, debiendo constar en la solicitud los requisitos exigidos por el artículo 588 bis b de la LECrim:

1.º La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.

2.º La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.

3.º Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.

4.º La extensión de la medida con especificación de su contenido.

5.º La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.

6.º La forma de ejecución de la medida.

7.º La duración de la medida que se solicita.

8.º El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

En caso de que se conceda la autorización, el auto judicial deberá dictarse en un plazo que no exceda las 24 horas y deberá especificar los aspectos previstos en el artículo 588 bis c:

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.

b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.

c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a.

d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.

e) La duración de la medida.

f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.

g) La finalidad perseguida con la medida.

h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

• Interceptación de las comunicaciones telefónicas y telemáticas: El Cap. V establece el marco regulador para la intervención de comunicaciones telefónicas y telemáticas como medida de investigación. Esta diligencia solo podrá ser autorizada por la autoridad judicial en aquellos supuestos en los que la investigación se refiera a alguno de los delitos contemplados en el artículo 579.1 de la propia ley, o bien cuando se trate de infracciones penales cometidas utilizando herramientas informáticas o tecnologías relacionadas con la información, comunicación o servicios telemáticos.

El alcance de esta medida se limita a ciertos ámbitos concretos (artículo 588 ter b):

1. Los terminales o medios de comunicación objeto de intervención han de ser aquellos habitual u ocasionalmente utilizados por el investigado.

2. La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario.

También podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.

A los efectos previstos en este artículo, se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga.

Además de los requisitos expuestos en el artículo 588 bis b, la solicitude de la autorización también debe presentar:

a) la identificación del número de abonado, del terminal o de la etiqueta técnica,

b) la identificación de la conexión objeto de la intervención o

c) los datos necesarios para identificar el medio de telecomunicación de que se trate.

Con el fin de concretar el alcance de la medida de interceptación, la solicitud de autorización judicial podrá referirse a alguno de los siguientes aspectos específicos:

a) La autorización para registrar y grabar el contenido de las comunicaciones, debiendo señalar el tipo o modalidad de comunicación que se pretende intervenir.

b) La posibilidad de identificar el origen y el destino de la comunicación en el momento en que esta se lleva a cabo.

c) La determinación de la ubicación geográfica tanto del emisor como del receptor en el momento de la comunicación.

d) La obtención de otros datos de tráfico, estén o no directamente vinculados a la comunicación, siempre que aporten valor relevante para la investigación. En estos casos, la petición deberá indicar de forma precisa cuáles son los datos que se pretenden recabar.

Adicionalmente, en situaciones excepcionales de urgencia vinculadas a investigaciones por delitos relacionados con organizaciones armadas o actividades terroristas, y siempre que existan indicios sólidos que justifiquen la necesidad inmediata de la intervención, la medida podrá ser ordenada directamente por el Ministro del Interior o, subsidiariamente, por el Secretario de Estado de Seguridad. En tales casos, la resolución deberá ser comunicada al juez competente de manera inmediata, y como máximo dentro de las siguientes 24 horas. Esta notificación incluirá una justificación de la urgencia, la descripción de las actuaciones realizadas, el procedimiento utilizado y los resultados obtenidos.

El juez competente, a su vez, deberá emitir una resolución motivada en la que confirme o revoque la medida adoptada, dentro de un plazo que no podrá exceder de 72 horas desde que se ordenó la intervención.

El artículo 588 ter e de la LECrim impone la obligación de colaboración y confidencialidada todos aquellos que prestan servicios de telecomunicaciones, facilitan el acceso a redes de comunicación o participan en la prestación de servicios vinculados a la sociedad de la información. Esta obligación se extiende también a cualquier persona física o jurídica que, de forma directa o indirecta, contribuya al desarrollo o transmisión de las comunicaciones objeto de investigación. Todos ellos están legalmente obligados a colaborar con las autoridades y a mantener el más estricto secreto sobre las actuaciones practicadas.

Además, este Capítulo V contempla otras formas de obtención de prueba, regulando distintos mecanismos técnicos adaptados a las características de los delitos cometidos en entornos digitales, entre los que destacan:

Datos obrantes en archivos automatizados de los prestadores de servicios (Art. 588 ter j LECrim):

1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial.

2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

La identificación mediante número IP. (Artículo 588 ter k.): Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

La identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes. (Artículo 588 ter l.):

1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.

2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 ter d. La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior.

El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 bis c.

Identificación de titulares o terminales o dispositivos de conectividad. (Artículo 588 ter m.):

Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia.

• Captación y grabación de comunicaciones orales mediante dispositivos electrónicos: El Cap. VI contempla la posibilidad de interceptar y registrar conversaciones orales utilizando medios electrónicos. Esta actuación requiere, como en los casos anteriores, una resolución judicial motivada que autorice expresamente la medida. Además, se regula la identificación de los titulares, terminales o dispositivos de conectividad involucrados en las comunicaciones.

• Captación de imágenes, seguimiento y localización: En el Cap. VII, se establece el marco legal para el empleo de tecnologías destinadas a la grabación de imágenes, así como para la utilización de dispositivos de seguimiento y localización. Estas herramientas permiten obtener información sobre la posición o desplazamientos del investigado y deben aplicarse siempre bajo control judicial y con observancia de los principios de proporcionalidad y necesidad.

• Registro de dispositivos de almacenamiento masivo de datos: Por su parte, el Cap. VIII regula el acceso y análisis de dispositivos que contienen grandes volúmenes de información digital, como discos duros, memorias externas o servidores. Estas diligencias están orientadas a recopilar pruebas electrónicas relacionadas con la actividad delictiva, y deben autorizarse también mediante auto judicial previo.

El Artículo 588 sexies a. Necesidad de motivación individualizada, establece limitaciones al acceso de información contenido en los ordenadores o teléfonos incautados en la siguiente forma:

1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.

• Registros remotos sobre equipos informáticos: el Cap. IX es la variante actualizada de la intervención telefónica aplicada a los medios telemáticos, en el artículo 588 septies se establece:

1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:

a) Delitos cometidos en el seno de organizaciones criminales.

b) Delitos de terrorismo.

c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.

d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.

e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

2. La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.

2.5.2- Cooperacion judicial en ciberdelincuencia internacional

En el ámbito de las redes informáticas, el concepto de supraterritorialidad adquiere una importancia esencial. A diferencia de los delitos tradicionales, que se producen en espacios físicos claramente delimitados, los delitos cometidos en entornos digitales no se circunscriben a una ubicación geográfica concreta. En el ciberespacio, lo relevante no son los territorios en sentido estricto, sino los nodos técnicos que componen la infraestructura digital: terminales, servidores, proveedores de servicios y las conexiones entre ellos.

Estos componentes facilitan el flujo de información a escala global, sin que existan limitaciones derivadas de fronteras nacionales. No obstante, conectar de forma precisa los elementos digitales con los espacios físicos donde residen los responsables o las víctimas puede resultar especialmente complejo [17].

Ante este escenario, se han planteado propuestas de alcance internacional con el objetivo de dar respuesta eficaz a estos desafíos. Una de ellas ha sido la creación de un tribunal penal internacional especializado en ciberdelincuencia. Sin embargo, esta alternativa conlleva importantes obstáculos, como la necesidad de armonizar la tipificación penal de las conductas delictivas, establecer criterios claros de competencia internacional, gestionar un volumen potencialmente elevado de casos y garantizar la efectividad de una jurisdicción universal en un entorno digital tan dinámico.

Frente a la posibilidad de establecer una nueva institución internacional, algunos expertos sugieren extender las competencias de la Corte Penal Internacional (CPI) para que pueda abordar los delitos informáticos más graves con impacto global. Esta opción permitiría perseguir ilícitos como las vulneraciones masivas de la propiedad intelectual, la distribución de pornografía infantil o los fraudes económicos transnacionales cometidos en línea.

Una estrategia basada en la selectividad de los delitos más lesivos, combinada con mecanismos avanzados de cooperación policial y judicial entre Estados, favorecería una mayor convergencia entre las jurisdicciones nacionales y la respuesta penal internacional. Este enfoque permitiría abordar de manera más eficaz tanto la complejidad técnicacomo la dimensión global de las conductas criminales en el entorno digital [18].

[17] PRADA, I. F.(2015) "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia". *Revista Electrónica de Ciencia Penal y Criminología,* 17, 21. Pp. 21-23.

[18] PRADA, I. F.(2015) "Prevención y solución de conflictos…", op.cit, pp. 19-20.

En el escenario actual, la cibercriminalidad se manifiesta como una problemática de escala global que requiere respuestas coordinadas y multilaterales. En este sentido, la cooperación internacional se convierte en un pilar esencial para enfrentar los retos derivados de los conflictos jurisdiccionales en el entorno digital.

La fragmentación normativa y los enfoques puramente estatales resultan claramente insuficientes para abordar con eficacia la delincuencia transnacional en el ciberespacio.

Por tanto se hace necesaria una respuesta global e integradora, que reconozca el carácter transfronterizo del fenómeno y promueva la armonización de los ordenamientos penales, con el objetivo de reducir las zonas de impunidad y establecer criterios comunes en la tipificación y persecución de los delitos informáticos.

La cooperación internacional se presenta como una herramienta clave para lograr una persecución penal efectiva en materia de ciberdelincuencia. Mediante la coordinación entre autoridades judiciales y cuerpos policiales de distintos países, es posible intercambiar información relevante, obtener pruebas transfronterizas y ejecutar detenciones, lo que refuerza relevante, obtener pruebas transfronterizas y ejecutar detenciones, lo que refuerza significativamente la capacidad de respuesta frente a los delitos cometidos en entornos digitales.

A pesar de los avances logrados en cuanto a asistencia judicial y colaboración policial internacional, todavía persisten importantes retos en el ámbito procesal, especialmente en lo relativo a la duplicidad de procedimientos penales. La existencia de causas paralelas sobre los mismos hechos en diferentes jurisdicciones no solo compromete la eficiencia del sistema, sino que también puede suponer una vulneración del principio *"non bis in ídem"*, que impide que una persona sea procesada o sancionada más de una vez por el mismo delito, tal y como reconocen los principales instrumentos de derechos humanos.

Superar estas dificultades requiere que la comunidad internacional avance en el diseño de mecanismos eficaces para reforzar la cooperación judicial. Esto supone, entre otras medidas, la necesidad de establecer criterios objetivos y consensuados que permitan determinar qué jurisdicción debe asumir la competencia principal en casos de cibercriminalidad con dimensión transnacional. Asimismo, resulta fundamental fomentar el reconocimiento mutuo de resoluciones judiciales entre Estados, lo que facilitaría la ejecución de sentencias y evitaría conflictos de competencia [19].

[19] PRADA, I. F. (2015) "Prevención y solución de conflictos…", op.cit, pp. 21-23.

En síntesis, se plantean dos propuestas para optimizar la colaboración internacional en la lucha contra los delitos informáticos: en primer lugar, la determinación de criterios jurídicos claros que permitan identificar la jurisdicción nacional más adecuada para conocer del caso cuando exista conflicto de competencias; y en segundo lugar, la creación de un procedimiento simplificado y eficaz para resolver situaciones de litispendencia penal internacional vinculadas a ciberdelitos. Ambas medidas contribuirían a mejorar la seguridad jurídica y la eficacia de las investigaciones en un entorno globalizado.

2.5.3- Particularidades en la denuncia

Uno de los principales retos en la lucha contra la ciberdelincuencia es su elevado grado de impunidad, derivado en gran medida de las dificultades para su investigación y denuncia efectiva. La ausencia de una coordinación internacional eficiente entre autoridades judiciales y policiales representa un obstáculo significativo, ya que muchos de estos delitos se producen en entornos transnacionales y con métodos que dificultan su trazabilidad.

En numerosos casos, los ciberdelitos no son denunciados por las víctimas, lo que se debe a múltiples factores: desde la desconfianza en las instituciones policiales, hasta el desconocimiento sobre los mecanismos de denuncia existentes, pasando por sentimientos de vergüenza o temor al desprestigio, especialmente cuando se trata de organizaciones o empresas que temen que la exposición pública de un incidente afecte a su imagen [20].

Para hacer frente a este problema, distintas políticas públicas han sido propuestas, entre ellas: campañas de sensibilización e información, plataformas digitales que faciliten la presentación de denuncias, fortalecimiento de los canales de cooperación con el sector privado, así como la optimización de los sistemas de intercambio de datos entre cuerpos policiales a escala nacional e internacional.

[20] TÁVORA SERRA, M. J. (2022) *Vigilancia e investigación policial en el ciberespacio: aspectos procesales del ciberpatrullaje*. Universidad de Sevilla, Sevilla. Pp 55

No obstante, el impacto real de estas estrategias aún no ha sido evaluado en profundidad, y en el ámbito empresarial se percibe una cierta reticencia a colaborar abiertamente con las autoridades, sobre todo cuando están en juego intereses reputacionales. Esta situación ha llevado a muchas compañías a implantar protocolos internos de prevención y respuesta ante incidentes de ciberseguridad. Aun así, la falta de voluntad del sector privado para comunicar estos delitos sigue siendo motivo de preocupación para los organismos encargados de su persecución.

Una de las razones que explica esta inquietud es que, al no denunciarse estos hechos, los autores pueden repetir el ataque contra la misma empresa o emplear métodos similares contra otras víctimas, ampliando así el impacto delictivo [21].

Por otro lado, otro factor que contribuye al alto grado de impunidad es la complejidad para recabar pruebas digitales. Esta dificultad no se debe únicamente a la naturaleza efímera y volátil de la información almacenada en sistemas informáticos, sino también a los problemas jurisdiccionales que surgen cuando los datos relevantes se encuentran alojados en infraestructuras ubicadas en el extranjero, lo que requiere la colaboración de otros Estados que, en ocasiones, no comparten los mismos intereses o estándares legales.

Asimismo, la presencia de redes como TOR, Freenet y otras tecnologías diseñadas para garantizar el anonimato, sumada a la estructura cada vez más sofisticada de las organizaciones delictivas en el ciberespacio, complica de manera significativa la obtención de resultados efectivos en las investigaciones. A ello se suma la necesidad de una sólida formación técnica especializada por parte de los profesionales encargados de la persecución de este tipo de criminalidad, dado el alto grado de complejidad tecnológica que caracteriza estos entornos.

En este contexto, la cooperación entre entidades públicas y privadas, tanto a nivel nacional como internacional, se ha consolidado como un elemento esencial para afrontar los retos derivados de la globalización de la ciberdelincuencia. Esta colaboración resulta clave para mejorar la capacidad operativa, compartir inteligencia y establecer protocolos conjuntos de actuación.

[21] VERA, M. D. B. (2023) “El Ciberdelito, desafíos para la ley penal y civil. Marco jurídico nacional y comparado”. *Revista Jurídica*, *7*(1). Pp. 182

Existen además otros elementos que contribuyen al elevado índice de impunidad. Entre ellos destaca la posibilidad de automatizar procesos delictivos, lo que permite que ciertas acciones se ejecuten de manera remota sin intervención directa e inmediata del autor.

También resulta especialmente problemático el uso de software que puede reconfigurarse automáticamente para eliminar rastros de actividad, así como la implementación de herramientas diseñadas para ocultar la identidad del responsable, como servidores proxy o redes de redirección que dificultan identificar la IP de origen [22].

En este escenario, cobra especial relevancia el momento inicial del procedimiento: la recepción de la *notitia criminis*, es decir, la comunicación o conocimiento de un hecho que puede revestir carácter delictivo.

Este punto de partida es fundamental, ya que la información proporcionada en esta fase, ya sea por parte de una víctima o de un tercero, puede contener datos cruciales para el éxito de la investigación.

El agente receptor, habitualmente perteneciente a las fuerzas y cuerpos de seguridad, debe procurar obtener la mayor cantidad de información posible, incluyendo las circunstancias del suceso, las características de los presuntos implicados y los medios utilizados para la comisión del delito.

En definitiva, la *notitia criminis* representa el elemento desencadenante de la actividad investigadora y su eficacia está estrechamente ligada a la calidad, coherencia y exhaustividad de los datos recogidos en ese primer contacto[23]. Una correcta recopilación inicial puede ser determinante para el desarrollo posterior del proceso penal en el ámbito de la ciberdelincuencia.

2.5.4- Fase de instrucción y práctica de la prueba

Previo a la reforma legislativa de 2015, ya analizada en el apartado correspondiente a la investigación tecnológica, la LECrim no contemplaba un marco específico para regular las técnicas de investigación en el entorno digital.

[22] TÁVORA SERRA, M. J. (2022) *Vigilancia e investigación policial*... op, cit, pp 55-57.

[23]HURTADO, M. P. R. (2013) "El Proceso Común, Vía Emblemática del Código Procesal Penal del 2004 (CPP) y su Primera Etapa: la Investigación Preparatoria". *Foro jurídico*, (12), 231-239. Pp, 235-237

Ante esta ausencia normativa, los operadores jurídicos se veían obligados a recurrir a disposiciones generales de la ley procesal, como el artículo 282 LECrim, aplicándolas por analogía a actuaciones como intervenciones telefónicas, registros domiciliarios o incautaciones de dispositivos electrónicos.

Puntializar que estas técnicas, no están reservadas exclusivamente para la investigación de ciberdelitos, sino que su alcance se extiende también a formas tradicionales de delincuencia que hoy se desarrollan o se facilitan mediante el uso de medios tecnológicos, contribuyendo así a una investigación más eficaz y adaptada a la realidad actual [24].

Además, la jurisprudencia había venido ampliando el contenido del artículo 579 de la LECrim, extendiendo su interpretación a nuevos métodos tecnológicos de investigación, como la colocación de micrófonos ocultos o incluso la instalación de software espía (troyanos) en equipos informáticos.

Podemos decir que, el desarrollo de la reforma se llevó a cabo gracias a los siguientes acontencimientos:

1. La Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 8 de abril de 2014 invalidó la Directiva 2006/24/CE, que obligaba a los Estados miembros a conservar determinados datos generados o tratados por proveedores de servicios de comunicaciones electrónicas. El TJUE consideró que esta directiva vulneraba los derechos fundamentales al no establecer límites suficientes respecto a la finalidad, el acceso y el tiempo de conservación de los datos. Esta decisión tuvo un impacto directo sobre el modelo de retención de datos en la legislación española, cuestionando su compatibilidad con los estándares europeos en materia de privacidad.

2. La Sentencia 145/2014 del TC español declaró inconstitucional la intervención de comunicaciones en el interior de una celda policial, incluso cuando existiera autorización judicial. El tribunal argumentó que, en ausencia de una ley que regulara de forma específica dicha medida, se infringía el derecho fundamental al secreto de las comunicaciones, reconocido en el artículo 18.3 de la CE. Esta sentencia dejó en evidencia la insuficiencia del marco legal existente y reforzó la necesidad de una regulación expresa que diera seguridad jurídica tanto a los investigadores como a los ciudadanos.

[24] QUEVEDO GONZÁLEZ, J. (2017). *Investigación y prueba del ciberdelito.* Sepin. Madrid, España. P, 61

Señalar también, la existencia de una figura operativa de gran utilidad en la lucha contra la delincuencia informática: la intervención bajo identidad encubierta en entornos cerrados de comunicación digital, tales como foros o servicios cifrados. Esta actuación debe ser previamente autorizada por un juez y se encuentra regulada en los apartados 6 y 7 del artículo 282 bis, en garantía de los derechos fundamentales de las personas investigadas, especialmente el derecho a la intimidad y al secreto de las comunicaciones [25].

En el marco del proceso penal español, el Ministerio Fiscal asume un papel destacado durante la fase de investigación, especialmente en lo que respecta a la criminalidad vinculada al uso de las TIC.

Aunque en la actualidad no existen órganos judiciales especializados exclusivamente en ciberdelincuencia, la Fiscalía ha adoptado una serie de medidas para dar una respuesta efectiva al creciente fenómeno delictivo en el entorno digital.

Una de las iniciativas más relevantes fue la aprobación de la Instrucción 2/2011 de la Fiscalía General del Estado, en la que se establece una primera clasificación de los delitos que pueden ser considerados como parte de la criminalidad informática.

Esta categoría abarca conductas ilícitas muy diversas, todas ellas relacionadas con el uso indebido de tecnologías digitales, en particular, de internet. La generalización del entorno digital en los ámbitos económico, social y cultural ha dado lugar a nuevas manifestaciones delictivas, con dinámicas y estructuras que hasta hace poco eran desconocidas.

[25] LEÓN CAMINO, A. (2022). *El agente encubierto virtual,* Tesis doctoral, Universidad Carlos III de Madrid. P, 38.

Para hacer frente a estos desafíos, se ha creado la figura del Fiscal de Sala Coordinador de Criminalidad Informática, quien ejerce sus competencias con ámbito nacional. Este fiscal especializado tiene la responsabilidad de dirigir, coordinar y supervisar todas las investigaciones relacionadas con delitos informáticos. Entre sus funciones principales se encuentran [26]:

- Impulsar diligencias de investigación orientadas a esclarecer hechos constitutivos de delitos informáticos, lo que incluye la práctica de actuaciones como la recopilación de evidencias digitales, toma de declaraciones o análisis de sistemas informáticos.

- Intervenir directamente en procedimientos de especial trascendencia, ya sea por la gravedad de los hechos o por el elevado número de personas afectadas, o bien mediante la emisión de instrucciones a otros fiscales con el objetivo de garantizar la eficacia de la investigación.

- Coordinar la actuación de las secciones especializadas en criminalidad informática existentes en las fiscalías provinciales o territoriales. Esta labor incluye la elaboración de criterios homogéneos de actuación, la propuesta de directrices y el seguimiento de las investigaciones abiertas.

- Requerir información actualizada a las secciones territoriales especializadas, con el fin de mantener una visión general del estado de las investigaciones y poder adoptar decisiones estratégicas bien fundamentadas.

- Elaborar, de forma anual, un informe detallado dirigido al Fiscal General del Estado, en el que se recogen los procedimientos desarrollados y las principales actuaciones llevadas a cabo en materia de ciberdelincuencia. Este documento se integra en la Memoria Anual de la Fiscalía General del Estado.

En definitiva, el Fiscal de Sala de Criminalidad Informática se configura como una figura clave dentro del sistema de persecución penal en el entorno digital. Su especialización técnica y capacidad de coordinación resultan esenciales para garantizar una respuesta eficaz frente a los delitos que afectan a la seguridad jurídica y a los derechos fundamentales de los ciudadanos en el ámbito digital.

[26] MINISTERIO FISCAL. (2025). Funciones: Criminalidad informática. [en línea] https://www.fiscal.es/-/criminalidad-informatica [Consulta: 4 julio 2025.]

3. EL CASO ALCASEC Y SUS IMPLICACIONES PROCESALES

3.1 Contexto del caso Alcasec, hechos relevantes del caso e impacto mediático y social

En este punto abordaremos uno de los casos más relevantes de ciberdelincuencia cometidos en España en los últimos años.

El caso, protagonizado por José Luis Huertas Rubio, conocido en el ámbito digital bajo el alias "Alcasec", alcanzó notoriedad pública debido a sus ciberataques dirigidos contra infraestructuras públicas y privadas de alta sensibilidad, así como por el hecho de que, en el momento de los hechos, tenía entre 17 y 19 años, lo que acentuó aún más el impacto mediático del caso.

Entre los hechos delictivos más graves que se le atribuyen destacan:

1. El acceso no autorizado a sistemas informáticos de organismos públicos como:

- El Consejo General del Poder Judicial (CGPJ): accedió al Punto Neutro Judicial, una plataforma restringida utilizada por jueces, fiscales y otras autoridades para intercambiar información sensible. Desde allí, logró extraer información personal de más de medio millón de ciudadanos, incluidos datos tributarios y judiciales.
- La Agencia Tributaria y el Ministerio de Justicia: obtuvo credenciales comprometidas de empleados públicos y las utilizó para ingresar a sus sistemas, accediendo a historiales fiscales y documentos oficiales.
- La Dirección General de Tráfico (DGT): accedió a bases de datos que contenían información sobre vehículos y conductores, lo que le permitió construir perfiles detallados de ciudadanos.

2. Robo, filtración y venta de datos personales:

Tras obtener los datos, los ofrecía en venta en foros ilegales de la dark web y a través de canales en plataformas como Telegram. Los datos incluían nombres completos, DNIs, direcciones, teléfonos, datos bancarios y antecedentes judiciales o fiscales.

3. Revelación de secretos y usurpación de identidad:

Alcasec utilizaba los datos obtenidos para crear identidades falsas o suplantar la identidad de ciudadanos reales, pudiendo así realizar otros delitos como fraudes bancarios o estafas por internet.

También se le acusa de haber facilitado a terceros el acceso a esos datos, fomentando la creación de redes de fraude.

4. Blanqueo de capitales:

El lucro obtenido a través de estas actividades hizo posible que el joven ostentase signos de riqueza inusuales para alguien de su edad, aparentando un estilo de vida alejado de su perfil como estudiante, lo cual contribuyó a su exposición mediática y su posterior identificación por las autoridades. Se detectó que parte de los ingresos obtenidos a través de la venta de datos o servicios informáticos ilícitos fue movilizada mediante criptomonedas, dificultando su trazabilidad.

5. Creación y distribución de herramientas delictivas:

Además de explotar vulnerabilidades, cabe destacar que Alcasec también habría fundado o participado activamente en grupos cibercriminales conocidos, como "Los Telecos", dedicados a la explotación de datos sustraídos y al desarrollo de herramientas para la comisión de delitos informáticos.

6. Reincidencia y libertad bajo medidas cautelares:

A pesar de ser detenido en varias ocasiones (la primera siendo menor de edad), fue puesto en libertad con medidas cautelares, pero continuó delinquiendo.

Su detención más relevante tuvo lugar en 2023, cuando la Policía Nacional, tras una larga investigación, logró intervenir sus dispositivos y acceder a pruebas clave que evidenciaban el alcance de sus operaciones.

El caso se encuentra aún en proceso judicial, y ha reabierto el debate sobre la capacidad de respuesta del ordenamiento jurídico ante delitos cometidos en el ciberespacio, especialmente cuando los autores son menores o jóvenes con conocimientos técnicos superiores a los medios de protección empleados por las instituciones públicas [27].

La ejecución de los delitos cibernéticos cometidos por el hacker español se basó en una combinación de técnicas propias del *hacking ético* aplicadas con fines delictivos. Su *modus operandi* reflejaba un conocimiento profundo de los sistemas de información utilizados por organismos públicos, así como de los fallos humanos y técnicos que podía explotar para obtener acceso no autorizado y extraer información de alto valor.

[27] Policía Nacional. (2023). Nota de prensa: Detenido un joven hacker por acceso ilícito a bases de datos oficiales. Ministerio del Interior.

Entre las técnicas más relevantes destaca, en primer lugar, el uso de ingeniería social para la obtención de credenciales de acceso. Esta metodología se basa en manipular a usuarios legítimos de un sistema, como empleados públicos o proveedores, para que revelen contraseñas, pinchen enlaces maliciosos o descarguen archivos infectados. En algunos casos, Alcasec habría accedido a correos electrónicos institucionales mediante técnicas de *phishing* (suplantación de identidad digital), lo que le permitió capturar credenciales y autenticarse como usuarios autorizados [28].

3.2 Análisis procesal del caso

3.2.1- Inicio de la investigación

El inicio de la investigación del caso *Alcasec* tuvo su origen en una serie de alertas procedentes de diversos organismos públicos que detectaron accesos anómalos a sistemas institucionales sensibles. La primera señal de alarma surgió en el año 2022, cuando el CGPJ denunció una intrusión en el sistema del Punto Neutro Judicial. La detección de accesos no autorizados, así como la sospecha de exfiltración de datos personales y confidenciales, motivó la apertura de diligencias por parte de la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional, en colaboración con la Fiscalía de Criminalidad Informática.

El proceso de investigación se enmarcó dentro de una operación de carácter reservado que, con el tiempo, fue denominada *Operación Borraska* [29].

Una pieza clave en el inicio de la investigación fue la filtración de una muestra de datos robados, publicada por el propio hacker en canales de mensajería cifrada. Este hecho permitió a los cuerpos de seguridad comprobar la veracidad y el origen institucional de la información sustraída, confirmando la gravedad del incidente. A partir de este momento, se intensificaron las labores de vigilancia digital, recurriendo a la monitorización de foros clandestinos y redes de comunicación en las que el sospechoso operaba bajo distintos seudónimos [30].

---

[28] RODRÍGUEZ-MAGARIÑOS, F. (2009). Nuevos delitos informáticos: phishing, pharming, hacking y cracking. Práctica Penal, 48 , 3-4.

[28] HUESCA, G. (2025). Alcasec hackeó datos de la DGT, la CNMC, el Registro Civil y Transportes y los derivó a Suiza [en línea]https://www.larazon.es/espana/alcasec-hackeo-datos-dgt-cnmc-registro-civil-transportes-derivo-suiza_202505316839b08d812a8f1e6a0af1f2.html[Consulta: 4 julio 2025.]

[30] Policía Nacional. (2023). Nota de prensa… op.cit.

3.2.2- Procedimientos policiales y judiciales

La respuesta judicial al caso, se desarrolló en distintas fases procesales marcadas por la complejidad técnica de los hechos y la especial condición del acusado, que era menor de edad cuando se produjeron las primeras actuaciones delictivas.

La intervención de la jurisdicción penal se inició tras la denuncia presentada por el CGPJ a raíz del acceso no autorizado al sistema del Punto Neutro Judicial, lo que motivó la apertura de diligencias penales por parte de la Fiscalía de Criminalidad Informática y la incoación de la correspondiente investigación en la Audiencia Nacional.

En marzo de 2023 se llevó a cabo la detención del investigado por parte de la Policía Nacional, tras meses de seguimiento y recopilación de pruebas digitales.

La detención se produjo en el domicilio familiar del joven, donde se incautaron dispositivos electrónicos, soportes de almacenamiento y material vinculado a las actividades ilícitas.

Durante el registro, se encontraron indicios suficientes que permitieron consolidar su implicación en una serie de delitos informáticos, entre ellos el acceso ilícito a sistemas públicos, descubrimiento y revelación de secretos, daños informáticos y comercialización de bases de datos personales.

Ante la gravedad de los hechos, y considerando el riesgo de reiteración delictiva, el Juzgado Central de Instrucción correspondiente decretó la prisión provisional comunicada y sin fianza, con fundamento en los artículos 502 y 503 de la LECrim.

La decisión se justificó en la concurrencia de varios presupuestos: indicios racionales de criminalidad, riesgo de destrucción de pruebas, y especialmente, el peligro de reincidencia, ya que el joven había sido detenido anteriormente por hechos similares y continuó su actividad incluso estando investigado [31].

Durante la fase de instrucción, se practicaron numerosas diligencias de investigación de carácter técnico, entre ellas periciales informáticas, informes forenses de los dispositivos intervenidos, y el análisis de las comunicaciones mantenidas a través de canales cifrados y redes anónimas.

[31] CABEZAS, A. (2024). La Fiscalía pide prisión provisional para Alcasec, el joven que hackeó el Punto Neutro Judicial. ABC. [en línea] https://www.abc.es/espana/fiscalia-pide-prision-provisional-alcasec-joven-hackeo-20240524173146-nt.html [Consulta: 4 julio 2025.]

Asimismo, se solicitó la cooperación de plataformas digitales y proveedores de servicios para obtener registros que permitieran confirmar la autoría de las acciones imputadas.

Esta fase evidenció la necesidad de una preparación especializada de los operadores jurídicos frente a delitos tecnológicos, dada la elevada sofisticación de los medios empleados por el acusado.

En cuanto al proceso judicial, si bien parte de las actuaciones fueron inicialmente llevadas por la jurisdicción de menores, la acumulación de conductas una vez alcanzada la mayoría de edad del investigado, hicieron que gran parte del procedimiento fuera asumido por la Audiencia Nacional en su vertiente penal ordinaria,. A lo largo del proceso, la defensa alegó, entre otros extremos, la supuesta finalidad "investigadora" de las acciones del joven, sin embargo, la instrucción puso de manifiesto el lucro obtenido mediante la venta de datos sustraídos y el contacto mantenido con redes criminales en línea.

3.2.3- Pruebas digitales: recolección, autenticidad y cadena de custodia

En los delitos informáticos, la obtención, conservación y presentación de la evidencia tecnológica adquiere una relevancia capital, tanto por la volatilidad de los datos como por la necesidad de preservar la integridad y fiabilidad de los mismos a efectos probatorios.

En este caso, las principales fuentes de prueba recabadas fueron de naturaleza electrónica: registros de accesos a sistemas informáticos, direcciones IP vinculadas a intrusiones no autorizadas, archivos sustraídos, comunicaciones en aplicaciones de mensajería cifrada, y contenidos almacenados en dispositivos incautados durante los registros domiciliarios.

La recolección de estas evidencias digitales se llevó a cabo mediante actuaciones dirigidas por la Brigada de Investigación Tecnológica de la Policía Nacional, en colaboración con peritos informáticos. El procedimiento incluyó registros judiciales, tanto físicos como remotos, y la clonación forense de discos duros, teléfonos móviles y otros soportes de almacenamiento.

Se respetaron en todo momento los principios establecidos por la jurisprudencia del TS sobre la validez de las pruebas digitales, como pueden ser, la Sentencia TS 173/2011, de 10 de marzo, en la que se establece que los archivos digitales y las pruebas tecnológicas (en ese caso grabaciones de conversaciones) tienen plena validez si se han obtenido respetando las garantías legales y los derechos fundamentales o laSentencia TS 300/2015, de 19 de mayo, sobre la validez

de correos electrónicos como prueba: intervención judicial previa, proporcionalidad, necesidad e idoneidad de la medida, así como el derecho a la defensa y la cadena de custodia de los elementos intervenidos.

En cuanto a la autenticidad de la prueba, esta fue garantizada mediante herramientas de hash criptográfico que permitieron comprobar que los datos analizados no habían sido alterados desde su incautación. La integridad de los archivos y comunicaciones se documentó a través de actas firmadas por los agentes actuantes y técnicos especializados, lo que dio plena validez a su incorporación en el procedimiento. Además, se practicaron periciales informáticas independientes para confirmar los resultados obtenidos, siguiendo los criterios del artículo 456 de la LECrim, en relación con los informes técnicos y la prueba pericial.

Respecto a la cadena de custodia, esta se documentó de forma rigurosa desde el momento de la incautación de los dispositivos hasta su análisis en dependencias policiales o judiciales. Se registraron cada uno de los traslados, accesos, manipulaciones autorizadas y actuaciones practicadas sobre las pruebas, con el fin de evitar cualquier sospecha de contaminación, pérdida de validez o vulneración de derechos fundamentales.

3.2.4- Estrategias de defensa y acusación

Tanto la acusación pública como la defensa articularon sus posiciones en torno a elementos jurídicos, técnicos y personales que condicionaron el desarrollo y la dirección del proceso.

Desde la posición acusadora, el Ministerio Fiscal configuró un relato fáctico centrado en la reiteración delictiva, la intencionalidad del sujeto y el perjuicio causado a organismos públicos de relevancia institucional.

Se argumentó que las intrusiones a sistemas como el Punto Neutro Judicial, la Agencia Tributaria o la DGT no fueron meros actos de curiosidad tecnológica, sino ataques deliberados y técnicamente sofisticados dirigidos a comprometer datos sensibles. La Fiscalía sustentó la existencia de dolo directo, descartando cualquier motivación altruista o de “hacker ético”, y subrayó el ánimo de lucro como uno de los móviles fundamentales, ya que parte de la información sustraída fue posteriormente comercializada en redes clandestinas [32].

[32] HUESCA, G. (2025). Alcasec hackeó datos de la DGT… op.cit.

Además, la acusación enfatizó el riesgo de reiteración delictiva, especialmente tras constatar que el investigado había continuado con su actividad incluso después de ser objeto de una primera detención y sometido a medidas cautelares.

Esta reincidencia fue utilizada para justificar la solicitud de prisión provisional y para fundamentar la necesidad de imponer una respuesta penal proporcionada pero firme, que actuara como elemento de prevención general y especial [33].

Por otro lado, la defensa del acusado estructuró su estrategia en dos líneas principales. En primer lugar, trató de minimizar la gravedad de las acciones alegando la inmadurez del joven y su desconocimiento sobre la trascendencia real de sus actos. Se presentó al acusado como una persona autodidacta con gran capacidad técnica, pero carente de una conciencia plena sobre las implicaciones jurídicas de sus conductas. En segundo lugar, se intentó reconducir los hechos hacia una figura próxima al "hacker ético", argumentando que la motivación principal no fue causar daño ni enriquecerse, sino poner de manifiesto las vulnerabilidades de los sistemas públicos, lo que, en opinión de la defensa, podría haberse gestionado a través de medidas no punitivas, como programas de reeducación tecnológica o mediación penal.

Asimismo, la defensa alegó posibles irregularidades en la obtención y uso de determinadas pruebas digitales, cuestionando la validez de algunos elementos. Ambas partes también confrontaron sus posturas en torno al impacto mediático del caso. Mientras la acusación aludió a la alarma social generada como un factor agravante, la defensa lo utilizó para denunciar una posible estigmatización del joven, cuya identidad había sido ampliamente difundida pese a su edad.

3.3 Implicaciones legales y éticas

3.3.1- Protección de derechos fundamentales.

Uno de los aspectos más sensibles en la investigación de delitos informáticos, especialmente en casos de gran repercusión como el de *Alcasec*, es la garantía efectiva de los derechos fundamentales del investigado.

La investigación de los ciberdelitos puede afectar a varios derechos fundamentales dependiendo de la diligencia de investigación interesada.

[33] HUESCA, G. (2025). Alcasec hackeó datos de la DGT… op.cit.

Algunos ejemplos pueden ser: el acceso a la información contenida en los dispositivos electrónicos por parte del sistema penal puede afectar a la intimidad personal (art. 18.1 CE), al secreto de las comunicaciones (art. 18.3 CE) y a la protección de datos personales (art. 18.4 CE), o a lo que algún autor ha denominado el *derecho a la identidad virtual*. También puede verse afectado el derecho a la inviolabilidad domiciliaria (art. 18.2 CE) en aquellos supuestos en los que el dispositivo electrónico se halle en el curso de una entrada y registro en domicilio [34]. Es por ello, que la propia LECrim, en la redacción dada por la Ley Orgánica 13/2015, de 5 de octubre, regula diversas medidas de investigación en el Título VIII del Libro II, precisamente bajo la rúbrica *"De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución"*.

El preámbulo de la ley señala que la modificación de la LECrim responde a la necesidad urgente de establecer un marco normativo claro para las medidas de investigación tecnológica, con el fin de proteger adecuadamente derechos fundamentales como la intimidad, el secreto de las comunicaciones y la salvaguarda de los datos personales, tal y como recoge la Constitución.

Como regla general, toda actuación de investigación penal que pueda afectar a derechos fundamentales requiere, salvo en situaciones excepcionales, una autorización judicial previa que se acuerde en el marco de un procedimiento judicial. Además, la jurisprudencia de nuestros tribunales ha ido perfilando los requisitos que deben cumplirse en estas intervenciones para garantizar la protección de esos derechos, conformando así un sólido cuerpo doctrinal aplicable a los casos en los que se produce una intromisión en la esfera privada sin el consentimiento del afectado [35]. Este criterio quedó claramente definido en la Sentencia del TC 173/2011, de 7 de noviembre:

a) La existencia de un fin constitucionalmente legítimo.

b) Previsión legal de la medida limitativa del derecho.

c) Proporcionalidad de la medida definida a través del juicio de idoneidad, ecesidad y proporcionalidad en sentido estricto.

d) Autorización judicial motivada salvo en los supuestos de intervención policial por razones de urgencia y necesidad y siempre que, en este último caso, no exista reserva constitucional a favor de la autoridad judicial.

[34] DELGADO MARTIN, J. (29 de Nov. 2013)"Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos". *Diario La Ley nº 8202,* Sección Doctrina, pags 1-20.

[35] *Vid.* GONZÁLEZ-CUELLAR SERRANO, N (1990). *Proporcionalidad y derechos fundamentales en el proceso penal*, Colex, Madrid

De forma general, en el ámbito de la investigación de ciberdelitos y la aplicación de nuevas tecnologías, los derechos fundamentales que suelen verse más comprometidos son el derecho a la intimidad y el secreto de las comunicaciones, a los que se suma la protección de los datos personales y, en un plano más amplio, el derecho al propio entorno digital, entendido como un concepto integrador de todos los anteriores:

- El derecho a la intimidad (art. 18.1) y el derecho a la protección de datos (art. 18.4 CE) son de naturaleza material, de origen natural y modulable por el ciudadano que puede decidir sobre los límites de protección. Está regulado, además de por la L.O.1/1982, de 5 de mayo (en cuanto a la intimidad), por la Ley Orgánica 15/1999, de 13 de Diciembre, de protección de datos de carácter personal, que permite el acceso a los mismos por la policía.

- El derecho al secreto de las comunicaciones (art. 18.3 CE) es de naturaleza formal, de configuración legal y protegible sin modulaciones. Se encuentra regulado por la Ley 25/2007, de 18 de Octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Durante mucho tiempo, nuestras normas procesales han adolecido de una regulación detallada respecto a las investigaciones que suponen restricciones de derechos fundamentales. Esta carencia ha dado lugar a diversas resoluciones del Tribunal Europeo de Derechos Humanos (TEDH), que han instado a España a abordar dicha necesidad normativa. Sin embargo, esta ausencia de previsión legal ha sido compensada por la jurisprudencia, que, a través de sus fallos, ha conformado un cuerpo doctrinal propio en nuestro ordenamiento, recogiendo y aplicando los criterios fijados por el TEDH para suplir esa laguna legislativa.

La incorporación a la LECrim de la regulación de las medidas de investigación tecnológica, mediante la Ley Orgánica 13/2015, de 5 de octubre, puso fin a la ausencia de un marco normativo claro en esta materia. Sin embargo, esto no ha supuesto en modo alguno que deje de aplicarse la abundante doctrina jurisprudencial existente. De hecho, la nueva normativa se inspira en los principios ya establecidos por el Tribunal Europeo de Derechos Humanos (TEDH), de modo que se mantiene la misma línea interpretativa desarrollada hasta ahora por nuestros tribunales.

Por tanto, la interpretación que venían realizando los órganos judiciales españoles sobre la doctrina del TEDH continúa siendo plenamente válida para entender y aplicar esta nueva regulación.

3.3.2- Ciberseguridad y protección de infraestructuras críticas

La irrupción del caso *Alcasec* puso en evidencia una realidad cada vez más preocupante: la vulnerabilidad de determinadas instituciones públicas frente a amenazas cibernéticas. En particular, el acceso no autorizado a plataformas como el Punto Neutro Judicial, que canaliza información sensible entre órganos judiciales, fiscales y administrativos, constituye un ataque a lo que se considera una infraestructura crítica, en los términos definidos por la Ley 8/2011, de 28 de abril, de medidas para la protección de las infraestructuras críticas.

Este concepto abarca aquellas instalaciones, redes, sistemas o equipos físicos y tecnológicos cuya interrupción o destrucción afectaría gravemente la seguridad nacional, el orden público o el bienestar social. En consecuencia, los sistemas que gestionan datos judiciales, fiscales, sanitarios o de identidad ciudadana deben contar con los más altos estándares de seguridad informática, y estar sujetos a revisiones, auditorías y protocolos de respuesta ante incidentes [36].

La penetración de estos sistemas por parte de un individuo actuando en solitario, como ocurrió en este caso, revela deficiencias en los mecanismos de prevención, detección y contención de amenazas, especialmente en entornos institucionales.

Desde el punto de vista legal, estos ataques están tipificados en el CP español, particularmente en los artículos 264 y 264 bis, que sancionan con penas de prisión a quienes dañen, obstaculicen o interfieran en sistemas informáticos, especialmente cuando afecten a servicios públicos esenciales o infraestructuras críticas. La agravación penal no responde únicamente al daño directo causado, sino al riesgo sistémico que representa para el funcionamiento del Estado.

El caso analizado también suscita interrogantes éticos. ¿Cómo es posible que un joven, actuando sin una estructura criminal organizada detrás, haya logrado acceder a plataformas de alta sensibilidad?

Esta situación obliga a repensar el modo en que se gestionan los recursos de ciberseguridad en las administraciones públicas. A menudo, las inversiones en tecnología no van acompañadas de una cultura institucional adecuada: falta formación especializada, protocolos de respuesta rápida, simulacros periódicos y, en algunos casos, actualización de los sistemas operativos básicos.

[36] LISA INSTITUTE. (s.f). Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación [en línea] https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas?srsltid=AfmBOorrqHD9qXI9R8QUP-QhaZ2wLRcQgEXK7zKkuBySNAksGvUIBLGD[Consulta: 4 julio 2025.]

La ciberresiliencia institucional debe construirse no solo sobre herramientas tecnológicas, sino también sobre la concienciación del personal y la colaboración constante entre los niveles técnico, jurídico y político.

El caso *Alcasec* ilustra la necesidad de adoptar un enfoque preventivo y coordinado en la defensa del ciberespacio público. En línea con lo establecido por la Estrategia Nacional de Ciberseguridad y las directrices de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), resulta imprescindible reforzar la cooperación entre cuerpos de seguridad, autoridades judiciales, organismos públicos y sector privado. Esta cooperación debe orientarse a detectar vulnerabilidades antes de que se produzca un ataque, y a responder de forma ágil cuando se detecta una intrusión.

Por último, debe valorarse el impacto reputacional que estos ataques generan en la ciudadanía. Cuando la información confidencial de miles de ciudadanos es expuesta o comprometida, se resquebraja la confianza en las instituciones. Y la confianza, como bien jurídico intangible, es esencial para el funcionamiento del Estado de Derecho.

3.3.3- Responsabilidad penal de los menores en delitos informáticos

La participación de menores en delitos informáticos, como ha ocurrido en el caso de *Alcasec*, plantea retos específicos para el Derecho penal contemporáneo. El ordenamiento jurídico español, en línea con los principios internacionales de protección del menor, establece un sistema de justicia juvenil que difiere sustancialmente del régimen aplicable a los adultos. No obstante, cuando un menor demuestra una capacidad técnica excepcional y comete delitos de alta complejidad, como intrusiones en sistemas públicos o difusión de datos personales masivos, se genera una tensión entre la finalidad reeducativa del sistema y la necesidad de protección efectiva del interés general.

En España, las medidas dirigidas a menores infractores se encuentran recogidas en el artículo 7 de la Ley Orgánica 5/2000, de 12 de enero, de responsabilidad penal de los menores (LORPM). Este precepto, que abre el Título II de la norma bajo el título “De las medidas”, establece un amplio abanico de respuestas posibles que van desde la simple amonestación por parte del juez hasta el internamiento en un centro en régimen cerrado.

Estas medidas, como la libertad vigilada, el internamiento en centros especializados o las tareas socioeducativas, tienen como propósito principal promover la resocialización y reeducación del menor, mediante un proyecto educativo adaptado a la gravedad del hecho cometido, así como a la edad y al entorno social y familiar del menor[37].

Se trata, por tanto, de un sistema con un marcado carácter sancionador, pero fundamentalmente educativo, de acuerdo con el espíritu de la ley [37].

El caso de *Alcasec*, quien fue inicialmente detenido siendo menor de edad, generó un amplio debate público y jurídico respecto a la idoneidad de estas medidas. Aunque la ley contempla la posibilidad de aplicar medidas más severas en casos de especial gravedad (artículo 10 LORPM), sigue existiendo un límite legal y ético que impide imponer penas equivalentes a las del sistema de adultos, incluso cuando el delito presenta un alto grado de sofisticación y repercusión social. Esto plantea un dilema: ¿cómo actuar cuando un menor dispone de medios técnicos similares a los de una organización criminal y pone en jaque la seguridad pública?

En el contexto digital se introducen elementos nuevos en la valoración de la imputabilidad. En muchos casos, los menores acceden a recursos y conocimientos técnicos sin una formación ética o jurídica suficiente. La accesibilidad a herramientas de hacking, la normalización de prácticas de suplantación o la trivialización de la privacidad en redes sociales pueden generar una falsa percepción de impunidad. De ahí la necesidad de prevenir antes que sancionar, integrando en el sistema educativo contenidos sobre ciberética, protección de datos y legalidad digital[38].

[37] MARTINEZ MOLARES, P. (2023). Análisis de las medidas impuestas a menores infractores por delitos informáticos en España y Portugal. En ARANGÜENA FANEGO, C., DE HOYOS SANCHO, M., PILLADO GONZÁLEZ, E. (Dirs.), FREITAS, P. M. (Coord.), & JIMÉNEZ-VILLAREJO FERNÁNDEZ, F. (Pr.), (Eds.), *El proceso penal ante una nueva realidad tecnológica europea* (cap. 19). Thomson Reuters Aranzadi.

[38]AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). El uso de internet por los menores de edad. Enséñales a ser legales en internet. [en línea] https://www.aepd.es/guias/ensenales-ser-legales-en-internet.pdf [Consulta: 4 julio 2025.]

4. PROPUESTAS DE MEJORA EN LA LUCHA CONTRA LA CIBERDELINCUENCIA.

4.1- Reformas legales para el tratamiento de delitos informáticos

El ordenamiento penal español ha experimentado avances importantes en la tipificación de delitos informáticos, especialmente con la introducción del Título XIII bis del CP y la transposición de instrumentos internacionales como el Convenio de Budapest. Sin embargo, los hechos protagonizados por *Alcasec* demuestran que persisten vacíos normativos y zonas grises que dificultan una respuesta clara y proporcional. En este sentido, se propone una revisión técnica del catálogo penal que permita afinar conceptos como la "intromisión ilegítima", el "uso no autorizado de datos" o la "venta de información sustraída", con el fin de evitar solapamientos o lagunas.

Asimismo, podría valorarse la introducción de penas específicas para delitos informáticos cometidos por menores de alta capacidad tecnológica, que combinen medidas educativas con restricciones proporcionales a su nivel de peligrosidad digital. También sería oportuno establecer protocolos legales específicos para la intervención remota de dispositivos electrónicos en fase de instrucción, con garantías claras para la preservación de los derechos fundamentales, especialmente la intimidad y el secreto de las comunicaciones.

No obstante, en este punto hay que tener en cuenta que en agosto de 2026 será de aplicación el conocido como "paquete e-evidence", constituido por el Reglamento (UE) 2023/1543, del Parlamento Europeo y del Consejo, de 12 de julio de 2023 sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad y la Directiva de la misma fecha que le acompaña -la Directiva (UE) 1544/2023, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en los procesos penales [39].

Este paquete legislativo va a permitir a las autoridades judiciales de los Estados miembros el acceso a datos electrónicos (de abonados, de tráfico o de contenido) que se encuentren no sólo fuera de la jurisdicción que los reclama, sino incluso fuera de la propia Unión Europea, siempre y cuando el proveedor de servicios que los tenga almacenados disponga de oficina abierta en el territorio de la UE o, en su defecto, haya designado en dicho territorio un representante legal. Para ello el

[39] DE HOYOS SANCHO, M.(2024) *La nueva regulación en la Unión Europea sobre obtención transfronteriza de información electrónica en procesos penales. Análisis y valoración del e-evidence package*, Aranzadi, Cizur Menor.

Reglamento crea las órdenes europeas de producción y conservación de pruebas electrónicas, llamadas a convertirse en instrumentos ágiles dotados de una extraordinaria celeridad para hacer frente, a la volatilidad propia del objeto a que se refieren –los datos electrónicos almacenados- y evitar así que la prueba acabe desapareciendo [40].

4.2- Necesidades de formación en ciberseguridad para operadores jurídicos

Una de las principales lecciones de este caso es que el conocimiento jurídico, por sí solo, resulta insuficiente para afrontar con eficacia la complejidad de los delitos informáticos. Tanto jueces, como fiscales, abogados y miembros de las fuerzas de seguridad requieren una formación continua en ciberseguridad, análisis forense digital, técnicas de rastreo en redes anónimas y comprensión del funcionamiento de entornos cifrados y sistemas informáticos.

Por lo que desde mi punto de vista, me parece conveniente la creación de planes de formación obligatoria y especializada, integrados en la oferta de las Escuelas Judiciales, Centros de Estudios Jurídicos y academias policiales.

Esta capacitación debería permitir no solo entender las pruebas digitales y valorar su validez, sino también anticipar patrones delictivos y colaborar eficazmente con peritos técnicos y organismos especializados. Convirtiendose asi la interdisciplinariedad en una herramienta esencial para mantener la eficacia de la justicia penal en el ámbito digital.

4.3- Estrategias para prevenir y mitigar el hacking

Más allá del plano normativo y procesal, es necesario abordar la cuestión desde una perspectiva preventiva. El fenómeno del hacking, especialmente cuando es protagonizado por menores o jóvenes con talento tecnológico, plantea un dilema entre represión y canalización de habilidades. En lugar de responder únicamente con sanciones, sería conveniente desarrollar programas de detección temprana y reconducción del talento informático, orientados a integrar a estos perfiles en entornos legales y éticos, como la ciberseguridad profesional o la investigación académica.

[40] ARANGÜENA FANEGO, C. (2025), "El Reglamento e-evidence y las órdenes europeas de protección y conservación a efectos de prueba electrónica en procesos penales", en Pillado González, E. (directora), *Derecho Procesal y ciudadanía: Retos socioeconómicos y políticos de la justicia,* Atelier, Barcelona, pp.377-402.

Asimismo, las administraciones públicas deberían reforzar su infraestructura digital mediante auditorías de ciberseguridad periódicas, simulacros de intrusión controlada (pentesting) y colaboración continua con expertos del sector privado. En el plano educativo, convendría incorporar a los currículos escolares nociones básicas sobre legalidad digital, ética informática y consecuencias penales del uso indebido de la tecnología.

Y finalmente tambien sugeriría potenciar campañas institucionales de concienciación social sobre los riesgos del uso inadecuado de internet y la protección de datos personales, con especial énfasis en los jóvenes y usuarios más vulnerables. La prevención de la ciberdelincuencia no puede recaer únicamente en la respuesta penal; debe abordarse como un esfuerzo coordinado entre instituciones, sistema educativo, sector tecnológico y ciudadanía.

5. CONCLUSIONES

El tratamiento procesal de la ciberdelincuencia constituye, en la actualidad, uno de los retos más relevantes para el sistema de justicia penal. No se trata simplemente de castigar nuevas conductas delictivas, sino de adaptar los instrumentos jurídicos y procesales a una realidad digital que evoluciona con rapidez y complejidad. A diferencia de la delincuencia tradicional, los delitos cometidos en el entorno cibernético presentan una serie de características particulares que tensionan las estructuras clásicas del proceso penal: la deslocalización territorial, la anonimización del autor, la volatilidad de las pruebas digitales y la sofisticación técnica de los medios empleados.

En este contexto, el proceso penal se ve obligado a responder a múltiples exigencias: garantizar la eficacia en la investigación, asegurar la integridad y autenticidad de la prueba electrónica, preservar los derechos fundamentales del investigado y garantizar la tutela judicial efectiva de las víctimas. La normativa procesal española ha incorporado avances importantes en esta dirección, especialmente con la reforma operada por la Ley 13/2015, que introdujo un nuevo régimen de medidas de investigación tecnológica (arts. 588 bis y ss. LECrim). Sin embargo, aún existen lagunas normativas, vacíos interpretativos y limitaciones técnicas que impiden una respuesta plenamente satisfactoria frente a la ciberdelincuencia.

En el plano práctico, los órganos judiciales y los cuerpos y fuerzas de seguridad del Estado deben enfrentarse a la necesidad de intervenir dispositivos, acceder a comunicaciones cifradas, operar con jurisdicción transnacional y mantener la cadena de custodia de pruebas digitales en

condiciones de alta exigencia técnica. Esto requiere no solo una actualización permanente de las capacidades técnicas de los operadores jurídicos, sino también una colaboración eficaz con expertos en ciberseguridad, peritos informáticos, organismos internacionales y empresas del sector.

El caso *Alcasec* ha puesto en evidencia la fragilidad de algunas infraestructuras públicas ante ataques cibernéticos y ha demostrado las dificultades procesales que entraña la persecución de este tipo de conductas. Desde la perspectiva procedimental, se han planteado cuestiones como la obtención y validación de pruebas digitales, la proporcionalidad de las medidas de investigación, la adecuada protección del derecho a la intimidad y la necesidad de preservar la presunción de inocencia en entornos de fuerte exposición mediática. Además, el hecho de que el autor fuese menor en el momento de la comisión de parte de los delitos ha añadido una dimensión adicional: el desafío de compatibilizar el régimen de responsabilidad penal de los menores con la gravedad y sofisticación de los delitos informáticos.

Frente a esta realidad, el Derecho procesal penal debe asumir un papel proactivo y flexible. Es preciso avanzar hacia un modelo procesal más ágil y especializado, capaz de actuar eficazmente sin comprometer las garantías del Estado de Derecho. Para ello, sería conveniente promover reformas normativas que refuercen la cooperación internacional, mejoren la regulación sobre evidencia electrónica, y articulen mecanismos judiciales rápidos y seguros para la intervención de contenidos en línea y redes digitales. También es esencial la creación de unidades judiciales y fiscales especializadas en ciberdelincuencia, con formación técnica suficiente y herramientas legales actualizadas.

A este respecto, el tratamiento procesal de la ciberdelincuencia requiere una visión sistémica que combine prevención, represión, protección de derechos fundamentales y adaptación institucional. Solo desde un enfoque interdisciplinar y tecnológicamente competente será posible garantizar una respuesta penal eficaz, proporcionada y legítima ante los delitos del siglo XXI.

6. REFERENCIAS BIBLIOGRÁFICAS

Libros y capítulos de libro.

BUSTOS RUBIO, M. (2017). *Delitos acumulativos y delitos de peligro abstracto: el paradigma de la acumulación en el derecho penal*. ADPCP. Universidad de La Rioja, La Rioja.

DE HOYOS SANCHO, M.(2024) *La nueva regulación en la Unión Europea sobre obtención transfronteriza de información electrónica en procesos penales. Análisis y valoración del e-evidence package*, Aranzadi, Cizur Menor.

GÓMEZ TOMILLO, M. (1998). *Libertad de información y teoría de la codelincuencia. La autoría y la participación en los delitos cometidos a través de los medios de comunicación de masas.* Comares, Granada.

GONZÁLEZ-CUELLAR SERRANO, N (1990). *Proporcionalidad y derechos fundamentales en el proceso penal*, Colex, Madrid

LEÓN CAMINO, A. (2022). *El agente encubierto virtual.* Tesis doctoral, Universidad Carlos III de Madrid. P, 38.

MARTINEZ MORALES, P. (2023). Análisis de las medidas impuestas a menores infractores por delitos informáticos en España y Portugal. En ARANGÜENA FANEGO, C., DE HOYOS SANCHO, M., PILLADO GONZÁLEZ, E. (Dirs.), FREITAS, P. M. (Coord.), & JIMÉNEZ-VILLAREJO FERNÁNDEZ, F. (Pr.), (Eds.), *El proceso penal ante una nueva realidad tecnológica europea* (cap. 19). Thomson Reuters Aranzadi.

MIRANDA, J. J. C. (2020). *Factor Humano: La Teoría de las Actividades Cotidianas en la Ciberseguridad.*

MUÑOZ MACHADO, S. (2000). *La regulación de la red. Poder y Derecho en Internet.* Taurus, Madrid.

ORTIZ PRADILLO, J.C. (2013). *Problemas procesales de la Ciberdelincuencia.* Cólex.

QUEVEDO GONZÁLEZ, J. (2017). *Investigación y prueba del ciberdelito.* Sepin, Madrid

TÁVORA SERRA, M. J. (2022). *Vigilancia e investigación policial en el ciberespacio: aspectos procesales del ciberpatrullaje.*

VELASCO NÚÑEZ, E. (2010). *Delitos cometidos a través de Internet. Cuestiones procesales.* La Ley, Madrid.

VELASCO NÚÑEZ, E. (2021). *Delitos tecnológicos. Cuestiones penales y procesales.* Wolters Kluwer España S.A, Madrid.

Artículos de revista

ARANGÜENA FANEGO, C. (2025), "El Reglamento e-evidence y las órdenes europeas de protección y conservación a efectos de prueba electrónica en procesos penales", en Pillado González, E. (directora), *Derecho Procesal y ciudadanía: Retos socioeconómicos y políticos de la justicia,* Atelier, Barcelona.

BALLESTEROS, M. C. R., & HERNÁNDEZ, J. A. G. (2014). "Cibercrimen: particularidades en su investigación y enjuiciamiento". *Anuario Jurídico y Económico Escurialense,* (47).

DELGADO MARTIN, J. (29 de Nov. 2013) "Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos". *Diario La Ley nº 8202, Sección Doctrina,* pags 1-20.

HURTADO, M. P. R. (2013). "El Proceso Común, Vía Emblemática del Código Procesal Penal del 2004 (CPP) y su Primera Etapa: la Investigación Preparatoria". *Foro jurídico*, (12).

PRADA, I. F. (2015). "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia". *Revista Electrónica de Ciencia Penal y Criminología*,

RODRÍGUEZ-MAGARIÑOS, F. (2009). Nuevos delitos informáticos: phishing, pharming, hacking y cracking. *Práctica Penal,* 48 , 3-4.

ROSSO PEREZ, M. E. (2020). "Delitos informáticos o a través de medios telemáticos (I)". *LegalToday,* entrada del 10 de febrero.

SAINZ CANTERO, J. A. (1971). "El delito masa". *Anuario de Derecho Penal y Ciencias Penales.*

VERA, M. D. B. (2023). "El Ciberdelito, desafíos para la ley penal y civil. Marco jurídico nacional y comparado". *Revista Jurídica*, 7(1).

Recursos web

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). El uso de internet por los menores de edad. Enséñales a ser legales en internet. [en línea] https://www.aepd.es/guias/ensenales-ser-legales-en-internet.pdf [Consulta: 4 julio 2025.]

CABEZAS, A. (2024). La Fiscalía pide prisión provisional para Alcasec, el joven que hackeó el Punto Neutro Judicial. ABC. [en línea] https://www.abc.es/espana/fiscalia-pide-prision-provisional-alcasec-joven-hackeo-20240524173146-nt.html [Consulta: 4 julio 2025.]

DÍAZ GÓMEZ, A. (2010) El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest, REDUR 8. [En línea]. <http://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf > [Consulta: 7 julio 2025].

HUESCA, G. (2025). Alcasec hackeó datos de la DGT, la CNMC, el Registro Civil y Transportes y los derivó a Suiza [en línea]https://www.larazon.es/espana/alcasec-hackeo-datos-dgt-cnmc-registro-civil-transportes-derivo-suiza_202505316839b08d812a8f1e6a0af1f2.html[Consulta: 4 julio 2025.]

LISA INSTITUTE. (s.f). Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación [en línea] https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas?srsltid=AfmBOorrqHD9qXI9R8QUP-QhaZ2wLRcQgEXK7zKkuBySNAksGvUIBLGD[Consulta: 4 julio 2025.]

MINISTERIO FISCAL. (2025). Funciones: Criminalidad informática. [en línea] https://www.fiscal.es/-/criminalidad-informatica [Consulta: 4 julio 2025.]

MINISTERIO DEL INTERIOR. (2022). Balance de criminalidad: Informe anual sobre delitos informáticos. Gobierno de España. [en línea] https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2022/Balance-de-Criminalidad-Cuarto-Trimestre-2022.pdf [Consulta: 21 junio 2025.]

MINISTERIO DEL INTERIOR. (2023). Informe sobre la cibercriminalidad en España 2023. [en línea] https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf [Consulta: 21 junio 2025.]

POLICIA NACIONAL. (2023). Nota de prensa: Detenido un joven hacker por acceso ilícito a bases de datos oficiales. Ministerio del Interior. [en línea] https://www.interior.gob.es/opencms/en/detail-pages/article/Detenido-un-peligroso-hacker-responsable-de-mas-de-40-ciberataques-a-organismos-estrategicos/ [Consulta: 18 junio 2025.]

7. REFERENCIAS JURISPRUDENCIALES

STJUE de 8 de abril de 2014, C-238/14

STC 145/2014, FJ3º, (ECLI:ES:TC:2014:145)

STC 173/2011 de 7 de noviembre, (ECLI:ES:TC:2011:173)

STS 173/2011, de 10 de marzo.

STS 300/2015, de 19 de mayo.