



Universidad de Valladolid

Facultad de Derecho

Grado en Derecho

Delitos informáticos: situación actual, acceso ilícito y responsabilidad penal de las personas jurídicas

Presentado por:

Elisa Millán López

Tutelado por:

José Mateos Bustamante

Valladolid, 27 de Julio de 2023

INDICE

INTRODUCCIÓN.....	4
1.-DELITOS INFORMÁTICOS	6
1.1.-CONCEPTO DE DELITO INFORMÁTICO.....	7
1.1.1.- <i>El delito informático, categoría difusa</i>	7
1.1.3.- <i>Los bienes jurídicos protegidos y su posible carácter especial</i>	12
1.1.4.- <i>El bien jurídico protegido: La intimidad</i>	14
1.1.5.- <i>Conclusión</i>	16
1.2.- DELITO INFORMÁTICO EN EL CP ESPAÑOL	17
1.2.1.- <i>El acceso ilícito</i>	17
1.2.3.- <i>La posición del proveedor</i>	19
1.2.3.- <i>Conclusión</i>	20
2.-RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS	22
2.1.-ANTECEDENTES.....	22
2.1.1.- <i>Origen: La responsabilidad colectiva en la Antigüedad</i>	23
2.1.2.- <i>Universitas en la Edad Media</i>	24
2.1.3.- <i>Edad Moderna y responsabilidad corporativa</i>	26
2.1.4.- <i>Revoluciones francesa y norteamericana: El Derecho penal liberal y las corporaciones</i>	27
2.1.5.- <i>S.XIX y XX</i>	29
2.1.7.- <i>Conclusión</i>	30
2.2.-RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS EN EL DERECHO ACTUAL.....	31
2.2.1.- <i>El Código penal español y su modo de imputación de responsabilidad penal a las personas morales</i>	31
2.2.2.- <i>El sujeto activo: identificación y naturaleza de la persona jurídica penalmente responsable</i> ...	34
2.2.3.- <i>Cuestiones sobre la teoría del delito y las personas jurídicas</i>	38
2.2.4.- <i>Conclusión</i>	45
3.-RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS EN EL CIBERESPACIO: EL ACCESO ILÍCITO	46
3.1.-RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS EN EL MUNDO CIBERNÉTICO.....	47
3.1.1.- <i>Personas jurídicas acceso ilícito</i>	47
3.1.2.- <i>Compliance y protección de los sistemas informáticos</i>	49
3.1.4.- <i>El blockchain, la inteligencia artificial y otras dificultades</i>	52
3.1.5.- <i>Conclusión</i>	54
4.-CONCLUSIONES	56
5.-BIBLIOGRAFÍA	57

INDICE DE ABREVIATURAS Y SIGLAS

CE: Constitución española

CP: Código penal

DP: Derecho penal

DUE: Derecho de la Unión Europea

IA: Inteligencia artificial

LO: Ley orgánica

LSSI: Ley de servicios de la sociedad de la información y de comercio electrónico

RPPJ: Responsabilidad penal de las personas jurídicas

Owig: Ordnungswidrigkeitengesetz (ley sobre la infracción reglamentaria)

PJ: Persona jurídica

RDL: Real Decreto Ley

TC: Tribunal Constitucional

TIC: Tecnologías de la información y la comunicación

TS: Tribunal Supremo

STC: Sentencia del Tribunal Constitucional

STS: Sentencia del Tribunal Supremo

UE: Unión europea

Resumen

Desde la introducción del primer delito informático en 1995, hasta la reforma de la LO 1/2015 que modificaba de forma sustancial el régimen de responsabilidad penal de las personas jurídicas introducido en 2010, se ha dado una evolución enorme en el tratamiento de ambas figuras jurídico-penales.

La protección de los individuos frente ataques informáticos ha alcanzado el punto en el que se les defiende de las actuaciones provenientes de personas no sólo físicas, sino también jurídicas. Para entender cómo se articula tal será necesario analizar la esencia de la responsabilidad penal de los entes no naturales comprendidos como subsistemas autopoiéticos dentro del ordenamiento jurídico. Y para comprender cómo se configuran los delitos informáticos habrá que explorar los bienes jurídicos concretos por los que velan, resolviendo el debate acerca de la posible protección de nuevos bienes como la ciberseguridad.

Abstract

From the introduction of the first cybercrime in 1995, to the LO 1/2015 reform that substantially altered the corporate criminal liability system introduced in 2010, there has been a tremendous evolution in the way those two criminal figures are treated.

The protection of the individuals who are affected by cyberattacks has reached the point where they are defended not only from the actions emanated from natural people, but also from the legal ones. To understand how corporate liability is integrated, it will be needed to comprehend those entities as autopoietic subsystems integrated inside the legal system. And to grasp how cybercrimes are configured it is necessary to explore the legal assets that they guard, solving this debate about the possible protection of new legal assets such as cybersecurity.

Palabras clave

Acceso ilícito, intrusismo informático, intimidación, responsabilidad penal de las personas jurídicas, ciberespacio, privacidad, compliance, sistemas autopoiéticos, allanamiento informático, sistema informático.

INTRODUCCIÓN

La segunda vida desmaterializada que vivimos a través de la informática se desenvuelve en lo que conocemos como ciberespacio. Tal elemento entraña posibilidades y riesgos particulares, muchas veces, desconocidos por quienes lo utilizan. No es extraño encontrarse casos de uso de la informática con finalidades delictivas. Sin embargo, algo a tener muy presente es que quienes configuran y crean estos sistemas informáticos son personas jurídicas, no físicas. A raíz de ello, y de la cantidad de delitos e irregularidades que se han cometido en su seno, los organismos internacionales y sus Estados miembros han ido configurando medios para castigar tales comportamientos.

El elemento transnacional que impregna a estas comisiones delictivas ha obligado a los distintos Estados a crear instrumentos de persecución y cooperación internacionales. Y la UE no ha escapado a esa necesidad, por lo que cuenta con mandatos para sus Estados miembros relativos a la persecución de los delitos informáticos, de los cometidos por personas jurídicas, y de la combinación de ambos.

La existencia de estos instrumentos internacionales ha supuesto la introducción en España de la persecución del allanamiento informático cometido por personas no naturales. De ahí que se preste necesario analizar cómo se configurará tal responsabilidad en nuestro entorno, sus riesgos, aplicación y aspectos a criticar. Y todo ello se pretende explorar en este trabajo, que busca arrojar luz sobre un campo de imputación penal difuso tanto por el factor informático como por la difícil atribución de responsabilidad a personas inmateriales.

El análisis de esta cuestión se ha llevado a cabo en tres apartados diferenciados, que tratan al acceso ilícito, la responsabilidad penal de las personas jurídicas y la comisión del allanamiento informático por ellas de forma separada.

En la primera parte se pretenden exponer y dar por zanjados (en la medida de lo posible) los principales debates que se arremolinan alrededor del concepto de delito informático. Además, se analiza el delito de acceso ilícito informático, los bienes jurídicos que tutela y cuestiones relacionadas con él, como la figura del proveedor de servicios informáticos de la LSSI.

En el segundo apartado se plantea el estado de la cuestión de la responsabilidad penal de las personas jurídicas en el ordenamiento español, así como un análisis profundo de sus fundamentos y antecedentes. Con él se pretende crear una visión omnicompreensiva de cómo

operaba este tipo de responsabilidad (o más bien sus equivalentes), como opera y como podrá hacerlo.

El último tema que tratar es la comisión por parte de una persona jurídica del delito de acceso ilícito. Sobre todo, se exploran los mecanismos de exención de responsabilidad que podrían ser aplicables al caso, así como nuevos riesgos genéricos relacionados con la informática que deberían ser tenidos en cuenta.

El método que se ha utilizado para llevar a cabo este análisis ha sido la recopilación y estudio de doctrina nacional e internacional, la legislación nacional, los comentarios al respecto del propio legislador y la fiscalía, así como la revisión de la doctrina del TS y TC al respecto.

1.-DELITOS INFORMÁTICOS

La génesis del código y la computación es tan remota que indicar su origen requeriría un trabajo a parte. Sin embargo, sí son localizables hitos históricos que fueron allanando el terreno sobre el que se construirían los sistemas informáticos actuales. Estos utilizan el lenguaje binario en sus computaciones, cuyo origen lejano podría encontrarse en algunos jeroglíficos egipcios que datan del 2500 AC, o en textos como el «I Ching», elaborado alrededor del 1200 A.C en China. Y cuyo origen próximo sería el primer ordenador mecánico, creado por ADA LOVELACE y CHARLES BABBAGE, que data del año 1822¹.

La venida tanto del ciberespacio como de soportes asequibles desde los que cualquier particular pudiera ahondar en él; propició la elaboración, en los años 80 y 90 del siglo pasado, de trabajos relacionados con la criminalidad de ese entorno de manos de autores como ULRICH SIEBER, KLAUS TIEDEMANN, ROMERO CASABONA² o VICENZO MILITELLO entre otros.

De hecho, la primera ocasión en la que se habla con intenciones legislativas de criminalidad informática fue en 1976, cuando se dio la «12th Conference of Director of the Criminological Research Institutes: Criminological Aspects of Economic Crime» del Consejo de Europa³.

A ella le siguieron informes, creaciones de comités expertos y más instrumentos que culminaron con la creación de herramientas como el Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Este texto se ha utilizado como base para que los Estados armonizaran la lucha contra un tipo de criminalidad característicamente transnacional.

A este convenio le han seguido dos protocolos adicionales. El primero, de la criminalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas de ordenador de 2003. Y el segundo, relativo a la cooperación reforzada y la revelación de pruebas electrónicas, que la decisión 2023/436 del Consejo de la UE de 14 de febrero de 2023 autoriza a firmar a los estados miembros.

¹ LÓPEZ, J. C. (21 de diciembre de 2020). *El ADN de nuestros ordenadores tiene más de 4400 años: esta es la sorprendente historia del sistema binario*. Obtenido de xataka: <https://www.xataka.com/historia-tecnologica/adn-nuestros-ordenadores-tiene-4400-anos-esta-sorprendente-historia-sistema-binario>

² MERLO, M. N.-S. (21 de septiembre de 2020). Análisis de los delitos informáticos. Una propuesta de clasificación. *Revista Aranzadi de Derecho y Proceso Penal*(60).

³ SÁNCHEZ-ESCRIBANO, M. I. (2014). Panorama normativo supranacional del delito de acceso ilícito a un sistema informático. *Investigaciones en ciencias jurídicas*, 47.

Por último, habrá que tener en cuenta el contenido de otros documentos internacionales, como es la directiva (UE) 2022/2555, dedicada a establecer las obligaciones de ciberseguridad para los Estados miembros y medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación.

Dejando al margen las principales fuentes supranacionales al respecto. En este apartado se va a intentar establecer, de forma introductoria, el estado de la cuestión sobre los delitos informáticos y el de la legislación española.

1.1.-CONCEPTO DE DELITO INFORMÁTICO

Se ha procurado tratar, aunque de manera resumida, los problemas principales que adolece la existencia de estos tipos en el ordenamiento español. En concreto, como la doctrina ha intentado introducir criterios que posibiliten delimitar a los tipos genuinamente relacionados con la informática. Y, sobre todo, el profundo debate que se ha desarrollado sobre la posible vigencia de bienes jurídicos autónomos para esta clase de delitos.

1.1.1.-El delito informático, categoría difusa

Antes de entrar a analizar el acceso ilícito y su aplicación en el ámbito informático, sería conveniente introducir algunos conceptos del Derecho informático. En concreto, se va a procurar analizar, de forma breve, el estado de los delitos informáticos en la doctrina y el derecho positivo. Concretamente, se tratará su denominación, delimitación y clasificación.

1.1.1.1.-Denominación

Hay quien habla de «criminalidad informática» o de «cibercriminalidad»; mientras que algunos autores utilizan los términos «delitos informáticos» o «ciberdelitos»⁴.

La criminalidad tiene que ver con toda fenomenología criminal que esté impregnada de elementos informáticos, más que aquellas conductas ya tipificadas en este campo. Mientras que los delitos informáticos se refieren estrictamente a ello; a tipos vigentes que donde la informática está presente, o aquellos donde la protección del bien jurídico depende de su seguridad (esto es relativo, porque no existe definición que los acote).

⁴ ELOY VELASCO NÚÑEZ, CAROLINA SANCHIS CRESPO. (2019). *Delincuencia informática tipos delictivos e investigación con jurisprudencia tras la reforma procesal y penal de 2015*. Valencia: Tirant lo Blanch.

Por otra parte, hay quien considera más acertado hablar de ciberdelitos que de delitos informáticos, pues tal denominación pone el foco en el ciberespacio, más que en el uso de sistemas electrónicos. Actualmente, este espacio es lo que caracteriza a estos tipos, ya que es lo que permite que se cometan infracciones desde cualquier lugar físico y que afecten a diferentes bienes jurídicos, de forma simultánea⁵. Sin embargo, esta consideración, sólo se tendrá por cierta si se considera que lo característico de estas conductas es el ciberespacio, más que el uso de sistemas informáticos.

1.1.1.2.-Delimitación

Existen autores que, sin dudar de la existencia de un «Derecho informático», no consiguen concebir la de un Derecho informático penal. Todo porque el uso de tal categoría puede dar a entender que existe una rama común del ordenamiento penal a todos estos delitos, como la que comparten aquellos con un bien jurídico protegido común.

De hecho, hay quienes defienden que el delito informático es puramente referencial a «acciones y omisiones dolosas o imprudentes, penadas por la ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático»⁶. Pero que no existe (como delito autónomo) al no estar tipificado como tal en el CP, ni aparecer en ninguna legislación penal especial.

Desde esta perspectiva no se puede hablar de delito informático en sentido estricto. Pero sí cabe hablar de delincuencia o criminalidad informáticas. Concretamente en lo referido a esa unidad de hechos relacionados con los ordenadores y que tienen relevancia penal. Los topos cometidos a través de medios informáticos son una conducta con gran desvalor de acción porque tienen un carácter insidioso y clandestino. Es necesario que exista un bien jurídico relevante dañado y un especial desvalor de acción en la conducta.

Independientemente de su posible existencia como categoría autónoma, se pueden establecer diferencias entre delitos informáticos en sentido estricto y amplio. Los primeros serían aquellos que cuentan con elementos específicos en su tipificación; deben tener una especial referencia a las TIC, bien en la conducta, medios, modalidad, efectos o a algún otro elemento esencial o circunstancial del tipo (Ej. Acceso ilícito al sistema informático).

Del otro lado estarían los delitos informáticos en sentido amplio, o «delitos cibernéticos». Estos son aquellos donde la comisión se realiza o puede realizarse a través de

⁵ CASTAÑO, E. N. (Mayo de 2022). La relevancia penal de las nuevas tecnologías y su incidencia en los denominados ciberdelitos: especial referencia a los delitos contra la intimidad. *Revista General de Derecho Penal*(37).

⁶ RODRÍGUEZ, M. Á. (2020). *Manual de Derecho Informático*. Pamplona: Thomsom Aranzadi.

las TIC, pudiendo esta ser un elemento expreso del tipo o uno interpretativamente compatible con él (Ej. Incitación al odio, difusión de pornografía)⁷.

Sobre lo que es o deja de ser ciberdelito existen discrepancias en la doctrina, GALAN MUÑOZ propone como opción una definición amplia. En ella, se considera como tal a cualquier conducta típica que tenga como medio un sistema informático, que ataque a uno, o donde esté involucrado un software. Si se pretende poner énfasis en el ciberespacio como el lugar de comisión, se puede recurrir a la definición de MIRO LINARES, que los concibe como delitos que se dan en el ciberespacio, con sus particularidades criminológicas, victimológicas y su concreto riesgo penal⁸.

Acotar un concepto donde se aúnen todos los tipos de criminalidad que puedan estar relacionados con el uso de las TIC, y al mismo tiempo, no hacerla tan amplia que se quede vacía de contenido, es bastante complicado. Más aun teniendo en cuenta que los avances tecnológicos en este campo se dan con suma rapidez. Además, ni el CP ni el Convenio de Budapest de 2001 recogen uno.

Sin embargo, casi parecen más convincentes aquellos conceptos más estrictos del delito, pues si se considera que es informático cualquiera donde se tenga un mínimo contacto con las TIC en su comisión, absolutamente todos podrían serlo.

Por eso algunos autores tratan de crear una definición más estrecha. Y en ella, hay quienes terminan por incluir factores criminológicos; porque aluden a la frecuencia con la que los delitos se cometen a través de o contra la tecnología; independientemente de si el tipo contiene referencias literales a las TIC⁹.

⁷ Esta distinción, que enuncia PICOTTI, se encuentra equivalentemente presente en la mente de los autores españoles, quienes distinguen entre delitos informáticos donde las TIC son un elemento fundamental del tipo, y aquellos donde son un elemento secundario. Sin embargo, los criterios en virtud de los cuales se establece el carácter de amplio o estricto, difieren entre autores, aunque guardan una tónica común que es convenientemente superponible: algunos acotan el concepto estricto únicamente por las referencias que este haga en el tipo al uso de elementos informáticos; mientras que otros señalan que serán ciberdelitos en sentido estricto aquellos que sólo puedan cometerse a través de las TIC.

Para más información véase el artículo de MAURICIO MEJÍA-LOBO, SANDRA VICTORIA HURTADO-GIL, ANDRÉS MAURICIO GRISALES-AGUIRRE. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: estudio comparativo. *Revista de ciencias sociales*, 29(2), 356-372. Y el siguiente: PICOTTI, L. (s.f.). *Reati infomatici, riservatezza, identità digitale*. Obtenido de aidp.it: https://www.aidp.it/allegato_prodotti/115_001_Reati_informatici_e_contro_riservatezza_Picotti.pdf.

⁸ CASTAÑO, E. N. (Mayo de 2022). La relevancia penal de las nuevas tecnologías y su incidencia en los denominados ciberdelitos: especial referencia a los delitos contra la intimidad. *Revista General de Derecho Penal*(37).

⁹ Así lo hace GALAN MUÑOZ, que trata de encontrar una definición que genuinamente recoja a todos estos delitos. Para leer sobre la defensa de una definición amplia y criminológica del delito informático, ver: MUÑOZ, A. G. (2021). Compliance frente a delitos informáticos. En S. B.-B.-P. MIGUEL ABEL SOUTO, *Estudios penales en homenaje al profesor José Manuel Lorenzo Salgado* (págs. 553-572). Valencia: Tirant lo Blanch.

Sin embargo, cabe pensar que esta concepción sigue siendo demasiado amplia. No es que se quiera prescindir de todo aspecto criminológico, pero incluir a todo delito que «suela» ser cometido a través de sistemas informáticos crea una especie de limbo. No se especifica tampoco a partir de cuánta frecuencia adquieren el carácter de ciberdelito; ni se tiene en cuenta el hecho de que muchas actividades criminosas no son detectadas, ni por ende registradas, lo cual difumina más si cabe el criterio de la frecuencia. Además, si el legislador no incluyó referencia alguna a la informática en la redacción del tipo, debería procurar evitarse poner en su boca palabras que no son suyas. Más aún si no ha dado definición genérica de lo que es un delito informático, ni les ha separado sistemáticamente.

Entonces ¿Qué criterio se sigue para delimitar cuáles son y dejan de ser ciberdelitos? El Derecho positivo español ha optado, por lo que se deduce del CP, por una concepción amplia del asunto. De forma que se considerará delito informático a todo comportamiento típico donde las TIC jueguen un papel en su forma de comisión. Es decir, cualquier acción cometida en o a través del ciberespacio, con las connotaciones criminalísticas y victimológicas que eso conlleve. Así pues, los delitos contra la intimidad se considerarían ciberdelitos solamente bajo la concepción amplia de los mismos¹⁰.

Ahora bien, con respecto al criterio que debiera seguirse, la doctrina puede seguir debatiendo al respecto largo y tendido; pues no existen argumentos de inexpugnables en favor de una u otra visión. Aunque considerando que los efectos de la consideración de un delito como informático no escapan del ámbito descriptivo, seguir el criterio del legislador se presta adecuado.

1.1.1.3.-Clasificación

En la práctica los tipos son cuantiosos y muy heterogéneos, de ahí que muchos autores hayan intentado clasificarlos. Si nos aproximamos a SIEBER, veremos que este distingue cuatro categorías: manipulación de datos, destrucción de datos, obtención no autorizada de datos o formas de agresión al hardware¹¹.

¹⁰ CASTAÑO, E. N. (Mayo de 2022). La relevancia penal de las nuevas tecnologías y su incidencia en los denominados ciberdelitos: especial referencia a los delitos contra la intimidad. *Revista General de Derecho Penal*(37).

¹¹ El foco central de esta clasificación son los datos, la información. Cabría pensar si a esta consideración se le escapan algunas conductas, pues en ocasiones, a través de la informática se pueden obtener activos económicos, o violentar bienes jurídicos que poco tienen que ver con la tenencia de datos. Bien es cierto, que a algunos de estos bienes no se les podría dañar sin obtener primero información que se encuentra almacenada por sistemas informáticos (difícilmente voy a compartir un video sexual de alguien si no lo he podido interceptar). Sin embargo, existen otros tipos donde no es necesaria la obtención, modificación o manipulación de datos (apología del terrorismo, amenazas, injurias, lesiones al honor...).

Así pues, la manipulación o alteración de datos versa de ataques sobre el procesamiento de estos, y el momento del proceso en el que se dé es irrelevante. La conducta puede darse al inicio, alterando la base sobre la que se va a trabajar; o al final, siendo una mera alteración de los resultados. También está la destrucción de datos, aquí el medio y el momento también son irrelevantes. Seguidamente, SIEBER habla del espionaje informático, que consiste en la apropiación de datos almacenados informáticamente. Por último, estaría la agresión al hardware, que consistirá en un ataque físico al sistema informático en cuestión¹².

Por otra parte, existen más formas de realizar la clasificación. Lo cual tiene sentido ya que van apareciendo nuevas posibilidades a medida que evolucionan las TIC y, por ende, nuevas conductas susceptibles de dañar bienes jurídicos.

Genéricamente se puede dividir este tipo de delitos entre ciberintrusivos, cibereconómicos y los de ciberterrorismo. Así lo hacen ELOY VELASCO NÚÑEZ y CAROLINA SANCHIS CRESPO (entre otros). Estos autores definen a los cibereconómicos como aquellos donde el autor busca apoderarse del capital de terceros a través de un uso torticero de la tecnología. A los ciberintrusivos como aquellos donde el delincuente pretende apoderarse de información privada o íntima de terceros mediante el uso ilegítimo de la tecnología. Y al ciberterrorismo como la comisión de alguna de las conductas del Art. 573 CP a través de las TIC¹³.

Sin embargo, otros autores, como GONZALEZ RUS¹⁴ o ALFONSO GALÁN MUÑOZ¹⁵ deciden elaborar una división en función de los bienes jurídicos afectados. Esta clasificación originaría problemas en cuanto a la posible existencia de bienes jurídicos nuevos relacionados con el ámbito informático, o si en verdad sólo se defienden los tradicionales de nuevas amenazas. La mayoría de la doctrina dividirá los delitos entre aquellos que atentan contra la intimidad, y los que lo hacen contra el patrimonio económico¹⁶.

Cabría pues, preguntarse, si la clasificación está anticuada y no caben en ella conductas típicas más actuales; o si, por el contrario, en ella se pretende contener sólo a aquellas conductas donde el elemento informático sea fundamental (delitos informáticos en sentido estricto).

¹² MARTÍN, R. M. (2001). *Delincuencia informática y derecho penal*. Madrid: Edisofer, S.L.

¹³ ELOY VELASCO NÚÑEZ, CAROLINA SANCHIS CRESPO. (2019). *Delincuencia informática tipos delictivos e investigación con jurisprudencia tras la reforma procesal y penal de 2015*. Valencia: Tirant lo Blanch. Y NÚÑEZ, E. V. (2010). Planteamiento y punto de partida. *La ley*.

¹⁴ CASTAÑO, E. N. (Mayo de 2022). La relevancia penal de las nuevas tecnologías y su incidencia en los denominados ciberdelitos: especial referencia a los delitos contra la intimidad. *Revista General de Derecho Penal*(37).

¹⁵ MUÑOZ, A. G. (2019). *Los ciberdelitos en el ordenamiento español*. Barcelona: Editorial UOC.

¹⁶ MAURICIO MEJÍA-LOBO, SANDRA VICTORIA HURTADO-GIL, ANDRÉS MAURICIO GRISALES-AGUIRRE. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: estudio comparativo. *Revista de ciencias sociales*, 29(2), 356-372.

Por último, son interesantes posiciones alternativas, como la de MARIANA N. SOLARI MERLO; quien propone una clasificación teleológica, basada en la finalidad del uso de las TIC con las que se comete el delito. Esta consistiría en tres categorías superponibles: búsqueda y/o aproximación a la víctima, difusión de mensajes y/o contenidos y búsqueda de clientes o adquirentes. Contemplar si las conductas que entran en esta clasificación tienen una mayor lesividad por la introducción del elemento tecnológico es lo relevante, ya que en muchas de ellas el uso de la informática es alternativo al tipo común (Ej. Estafas, espionaje, amenazas, *stalking*...), y en otras, es exclusivamente informático (Ej. Estafa online, piratería)¹⁷.

Independientemente de la manera en la que se acoten estos delitos, el CP no cuenta con un apartado sistemáticamente independiente para ellos; sino que la doctrina ha hecho el esfuerzo de crear categorías que faciliten su identificación y estudio.

En realidad, la legislación de estos tipos se encuentra en diferentes apartados del Código, donde el legislador ha contemplado la necesidad de tipificar la comisión de conductas a través de la tecnología, por considerarla un elemento más fundamental que secundario de la conducta (por lo que parece prevalecer la distinción entre delitos informáticos en sentido estricto y amplio).

1.1.3.-Los bienes jurídicos protegidos y su posible carácter especial

En ese caso cabría preguntarse por qué los tipos con apartados referidos al elemento informático deben existir ¿No podrían perseguirse estas conductas con los habituales? Si el desvalor es el mismo si se realiza por el medio informático que materialmente ¿Por qué existe necesidad de crear tipos específicos para este fenómeno?

A la hora de iniciar este debate, se deben tener en cuenta varias cosas. La primera es que el DP tiene carácter de *ultima ratio*, y sólo se dedicará a proteger a los ciudadanos de aquellos ataques más graves a los bienes jurídicos que este se ha comprometido a proteger. Para que estos se vean en tela de juicio, deben cumplirse tanto el principio de subsidiariedad como el de fragmentariedad del Derecho¹⁸. Pero, además, se tiene que identificar la

¹⁷ MERLO, M. N.-S. (21 de septiembre de 2020). Análisis de los delitos informáticos. Una propuesta de clasificación. *Revista Aranzadi de Derecho y Proceso Penal*(60).

¹⁸ Es decir, sólo se podrá condenar la conducta lesiva de un bien jurídico que se haya considerado merecedor de protección penal, y cuando se hayan agotado el resto de los recursos que ofrezca el ordenamiento. Y, además,

intencionalidad que persigue el sujeto. El sorteo de sistemas de seguridad muchas veces es, para el autor, un reto intelectual; en otras, existe una motivación económica, política o social (sexual, venganza etc.)¹⁹. En definitiva, los bienes jurídicos son requisito indispensable para el ejercicio del *ius puniendi*, fundamentan el castigo y ayudan a delimitar la proporcionalidad de las penas.

Puede considerarse al ciberespacio como un reflejo del mundo material que cuenta con sus propias reglas y costumbres. La cuestión que plantea esto desde el ámbito del Derecho penal es si su existencia implica la necesidad de proteger bienes jurídicos nuevos.

El debate gira entorno a cómo de profundos han sido los cambios introducidos por las innovaciones tecnológicas. En caso de que hayan entrado de manera fundamental en nuestras vidas, podría considerarse factible el surgimiento de nuevos intereses a proteger. Tales como la seguridad informática, la intangibilidad o indemnidad de datos informáticos, la libertad o la intimidad informática²⁰.

La discusión se ha dado originariamente entre autores como SIEBER y MILITELLO. El primero defiende que en la sociedad conviven colectivos y bienes jurídicos. Mientras que el segundo observa que es fácil confundir el objeto material y el bien jurídico protegido en muchos tipos (Ej. Estafa). Para él, el bien jurídico se puede determinar de una u otra manera dependiendo del sistema de referencia que se utilice; en este caso la referencia es la informática, por lo que puede defenderse que existe un bien jurídico unitario y autónomo para todos los daños realizados a través de ella²¹.

MILITELLO habla de la intangibilidad informática. Este supuesto bien jurídico protegería a los ciudadanos del quebranto de su confianza en la informática como concepto abstracto. Lo que se defiende es que no se altere el lícito uso y funcionamiento del ciberespacio, que la información la manipulen solo aquellos sujetos que estén legitimados a ello, y que, por tanto, la concepción de la realidad de este mundo que tienen todos sus usuarios no se quebrante.

la protección de estos bienes jurídicos no será absoluta, sino que se le considerará en supuestos donde sea precisa una especial guarda del bien.

MARTÍN, R. M. (2001). *Delincuencia informática y derecho penal*. Madrid: Edisofer, S.L.

¹⁹ CASTAÑO, E. N. (Mayo de 2022). La relevancia penal de las nuevas tecnologías y su incidencia en los denominados cibercrimitos: especial referencia a los delitos contra la intimidad. *Revista General de Derecho Penal*(37).

²⁰ CASTAÑO, E. N. (Mayo de 2022). La relevancia penal de las nuevas tecnologías y su incidencia en los denominados cibercrimitos: especial referencia a los delitos contra la intimidad. *Revista General de Derecho Penal*(37).

²¹ MARTÍN, R. M. (2001). *Delincuencia informática y derecho penal*. Madrid: Edisofer, S.L.

Pero este no fue el único autor que defendió la tesis de los bienes jurídicos nuevos, sino que hubo más, que pretendieron tutelar tales como la seguridad o la libertad informática. En la defensa de estos bienes no se los protege de un daño material, sino del interés de los operadores y usuarios de que los sistemas funcionen y sean seguros.

Hay quien pensó entonces que sería necesario un nuevo bien jurídico, como la seguridad del sistema de información o la ciberseguridad. Porque una lesión del sistema puede tener consecuencias inmediatas al margen de la afcción a la intimidad de sus usuarios.

Este sería adecuado para funciones como garantizar las condiciones básicas necesarias para un correcto funcionamiento de las TIC en el entorno social. Y, seguidamente, la posibilidad de que mediante la protección de este bien jurídico supraindividual se adelante la protección de otros bienes jurídicos individuales, como la intimidad, o el patrimonio²².

Sin embargo, cuando nos atenemos al derecho positivo español, ninguno de estos bienes jurídicos diferenciados viene referenciado. Por otra parte, el propio Convenio de Budapest no hace referencia alguna a nuevos bienes tutelables. Sino que más bien alude a la protección de estos intereses difusos en orden a tutelar los bienes jurídicos preexistentes. Así pues, la defensa de la ciberseguridad no se daría más que a través de su relación con intereses o bienes jurídicos bien determinados. De lo contrario se estaría extralimitando el alcance del derecho penal, desvirtuando así su carácter de *ultima ratio*.

Los intereses defendidos por los bienes jurídicos que propone esta parte de la doctrina son demasiado difusos. No permiten definir la potencial lesividad de la conducta prohibida, y, por ende, no permiten delimitar ni el marco de necesaria protección penal, ni qué penas serían proporcionales al daño que causan.

1.1.4.-El bien jurídico protegido: La intimidad

Dejando de lado el debate sobre la existencia de bienes jurídicos particulares adscritos al elemento informático. Cabe añadir, que, aunque estos no cuenten con tipos autónomos y diferenciados, no es descabellado pensar que los bienes jurídicos clásicos se desarrollan de manera diferente según su ámbito.

Según la doctrina del TC el Art 18.1 CE reconoce un derecho al secreto, es decir, a que los demás no sepan lo que hacemos. Se da al ciudadano poder sobre la esfera de su vida

²² ROBERTO HERNÁNDEZ BERLINCHES y ALICIA GIL GIL. (2019). *Cibercriminalidad*. Madrid: Dykinson.

privada que es conocida por terceros. Lo que le otorga al individuo el derecho a la intimidad es un poder jurídico, en virtud del cual puede decidir qué se conoce sobre su vida y la de su familia y qué no²³.

Así pues, «la intimidad es, entre otras facetas, una reserva de conocimiento de un ámbito personal, que por eso denominamos privado y que administra su titular, tal administración y tal reserva se devalúan si el titular del ámbito de intimidad desconoce las dimensiones del mismo porque desconoce la efectiva intromisión ajena»²⁴.

Ahora bien, habrá que tener en cuenta qué es lo reservado, es decir, cuál es el mínimo de privacidad que debe ser protegido. Y es precisamente aquí donde empieza a difuminarse la cuestión, pues el ámbito de lo reservado está altamente condicionado por el recato, el pudor, la vergüenza y lo que comúnmente se entiende por tales.

Existirán pues distintas facetas de la intimidad en relación al ámbito en que se desarrollen. Por ejemplo, existe la intimidad corporal, referida a la entidad cultural sobre el recato corporal. Serán intromisiones a tal derecho las que violen, según un cabal juicio, el pudor o recato de la persona²⁵. Es decir, que sólo serán intromisiones a la intimidad corporal aquellas que culturalmente se consideren como tales²⁶.

Por tanto, en relación con el ciberespacio, habría que ver cuáles son los conceptos de pudor, recato y vergüenza que culturalmente percibe cualquier persona en atención a las reglas de la sana crítica. Y no se pretende defender con la identificación de tal la existencia de una intimidad informática; sino su afección a la ya constitucionalmente protegida.

Será importante remarcar que el titular del derecho a la intimidad tiende a actuar de manera diferente en el mundo material y el ciberespacio. Y esto es relevante, entre otras cosas, porque los soportes informáticos que suelen utilizarse para navegar en internet recogen información de sus usuarios constantemente; y sin su noticia o consciencia plenas.

Además, la concepción cultural del recato o lo reservado en internet puede verse alterada por la sensación de distancia e irrealidad que predomina en las redes sociales. Si bien, culturalmente no suele enseñarse a todo el mundo el interior del hogar de uno, sus comidas,

²³ STC 134/1999, de 15 de julio.

²⁴ STC 89/2006 de 27 de marzo.

²⁵ STC 196/2004 de 15 de noviembre.

²⁶ PORTILLA, F. J. (2018). Los derechos de la personalidad: la protección de la intimidad, el honor y la vida privada. En J. M. OTROS, *Derecho constitucional II* (págs. 533-576). Pamplona: Aranzadi.

vacaciones, cuerpos y experiencias en las relaciones sociales materiales. En internet es común compartir toda esa información con desconocidos.

Este factor será importante por dos motivos primordiales. El primero es que el titular está desprovisto de poder para controlar lo que se hace con aquello que sube a internet. Y, además, lo que allí se encuentra muchas veces ha sido recogido sin su permiso o consciencia²⁷. Segundo, que el software a través del que se navega ha sido creado y es actualizado por empresas que tienen capacidad para controlar qué se hace con lo que sus usuarios suben a la red.

Tratándose el trabajo de uno sobre el acceso ilícito, convendría, por último, diferenciar la concepción de intimidad y privacidad. La cuestión radica en el alcance, pues la intimidad se refiere al ámbito íntimo del titular. Mientras que la privacidad no es tan profunda, no se refiere a la esfera más reservada o personal.

1.1.5.-Conclusión

La mera existencia de una categoría de delitos informáticos suscita debate, y con buen motivo. Ya que esta se encontraría vinculada con la creación o consideración de nuevos bienes jurídicos a proteger, bienes, que serían supraindividuales. Esto no colinda con el carácter del Derecho Penal, y vulnera el principio de lesividad. Y lo hace porque tales bienes tienden a ser bastante difusos e indefinidos.

Por tanto, a la hora de hablar de los delitos de los Arts. 197 y ss. Se tendrá que hacer referencia o bien al bien jurídico individual y personal de la intimidad, o al de la privacidad, que se diferencian por su alcance.

Por otra parte, pretender acotar, definir y clasificar a los delitos informáticos es algo vacuo, ya que tales consideraciones no tendrán reflejo más allá del mundo de la doctrina. Serán caracteres útiles para la didáctica o descripción, pero no apelables en el derecho positivo.

²⁷ No resultan extraños los casos de espionaje (comercial y no comercial) realizado a través de los micrófonos, movimientos bancarios, webs visitadas y demás operaciones realizadas a través de los teléfonos móviles. Quienes han diseñado y controlan el estado de los softwares implicados pueden obtener enormes bases de datos con información privilegiada de todos sus usuarios: qué compran, dónde, cómo lo descubren, qué cantidad estimada de dinero gastan al mes, el patrimonio total que ostentan etc. La posibilidad de almacenar estos datos, organizarlos, y estudiarlos a través del big data puede suponerle cierto beneficio extra a quienes los adquieran. Y pueden llegar a tener consecuencias mayores, sobre todo si se tiene en cuenta el efecto de los metadatos en el análisis de estos datos (según como estén programados, pueden ser poco seguros, o pueden llevar a que se cree publicidad individualizada que perpetúe estereotipos tendentes a mantener o acentuar discriminaciones). Las consecuencias del mal uso de esta clase de datos son patentes en casos como el caso Roman Zakjarov v. Rusia, o el más conocido Cambridge Analytica.

1.2.- DELITO INFORMÁTICO EN EL CP ESPAÑOL

En primer lugar, se ha de hacer una sucinta referencia a las fuentes del derecho penal informático español. Existe un Código de Derecho de la Ciberseguridad, el cual contiene, de forma sistemática, aquellas normas con vinculación al ciberespacio. Así pues, hace referencia, entre otros, al CP y a todas las leyes especiales que puedan tener relación con la imputación por cibercrimes (ley de protección de datos, general de telecomunicaciones, de seguridad nacional...)

En cuanto a las fuentes internacionales, a parte del Convenio de Budapest, existen bastantes más. Ya bien entrados los 80 la OCDE (Organización de Cooperación y Desarrollo Económico) creó un comité de Expertos en Delincuencia Informática destinado a analizar las mejores propuestas de armonización en esta materia. Este emitió en 1986 un informe denominado «Computer-related crime-analysis of legal policy». En el cual se hacía referencia a la necesidad de armonizar la tipificación de ciertos actos como delitos informáticos, el quinto de ellos era el acceso ilícito²⁸.

A mayores, existen más instrumentos internacionales que pueden ser de utilidad, sobre todo a la hora de velar por el derecho a la intimidad en el ciberespacio, a estos efectos, la directiva 95/46/CE es bastante relevante. En ella, además, vienen definidos bastantes términos ius-informáticos aplicables a estos delitos.

A raíz de ello, y de más mandatos internacionales²⁹, el CP (tras las reformas de 2010 y 2015, que añadieron delitos informáticos a un código que sólo contaba con la estafa) cuenta con una prolija regulación de tipos donde el elemento informático es determinante en su comisión, o directamente son cometidos a través de él. (delitos de abuso sexual, producción de pornografía, descubrimiento de secretos, acceso o facilitación para acceder a un sistema informático, revelación de tales secretos etc.)³⁰

1.2.1.-El acceso ilícito

La vertiente informática de este tipo fue introducida en 2010 y reformada en 2015. Se recoge en el artículo 197 bis 1 del CP. La conducta típica consistirá en acceder, mantenerse

²⁸ SÁNCHEZ-ESCRIBANO, M. I. (2014). Panorama normativo supranacional del delito de acceso ilícito a un sistema informático. *Investigaciones en ciencias jurídicas*, 47.

²⁹ Como la Directiva 2013/40/UE o la decisión marco que ha salido este año, la cual insta a los miembros de la UE a firmar el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas.

³⁰ MAURICIO MEJÍA-LOBO, SANDRA VICTORIA HURTADO-GIL, ANDRÉS MAURICIO GRISALES-AGUIRRE. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: estudio comparativo. *Revista de ciencias sociales*, 29(2), 356-372.

o facilitar el acceso de un tercero a un sistema de información contra la voluntad de quien tenga derecho a excluir tal intromisión (el titular del derecho a la privacidad).

Para entender el tipo, tendrá que definirse el concepto de sistema de información, al que ya se ha hecho referencia anteriormente. Esto es el hardware, al soporte físico de almacenamiento y tratamiento de datos³¹.

El delito de acceso ilícito se sitúa junto a aquellos que protegen al bien jurídico de la intimidad. Pero en ningún caso se pretenderá proteger (al menos en el ordenamiento español) un bien jurídico informático abstracto, distinto de la intimidad o privacidad, como el de la seguridad informática. Y sobre esto cabe una concreción, pues según la exposición de motivos de la reforma del 2015, el objeto de defensa de los delitos del 197 no es la intimidad personal, sino la privacidad³².

La cuestión es que el 197 bis no vela directamente por la intimidad, por el derecho al secreto. Sino que más bien adelanta la protección, ya que se posiciona como un delito de peligro abstracto, donde lo penado es el mero acceso, independientemente de si en el sistema informático se contienen datos personales de la víctima. Esta posición que sostiene parte de la doctrina conduce a pensar que lo que realmente se protege es la ciberseguridad antes mencionada, a la noción de que los sistemas informáticos son seguros contra estos ataques, se defiende el tráfico informático³³.

Sin embargo, tal perspectiva ya se ha dado por superada. No se vela realmente por la ciberseguridad. No tendría sentido la posición sistemática del artículo, y su protección sería demasiado difusa. Podría ponerse en tela de juicio el principio de lesividad (ya que no se dañaría un bien jurídico determinado)³⁴.

³¹ La Directiva 2013/40/UE da una definición más exhaustiva «todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento»

³² Esto se debe a las críticas que recibió la anterior reforma por la colocación del delito de intromisión informática. Ahora se pretendía dejar el 197 como delito de defensa de la intimidad personal, y el resto para la privacidad. COLLANTES, T. G. (enero de 2015). Los delitos contra la intimidad tras la reforma de 2015: luces y sombras. *Revista de Derecho penal y criminología*, 3(13), 51-84.

³³ Debe anotarse que la introducción de este artículo se debe a la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información, la interceptación de datos electrónicos cuando no se trata de una comunicación personal. En ella se recogían algunas exigencias y anotaciones que fueron tenidas en cuenta por el legislador en 2015. En ella se hace mención a la separación de datos que afectan directamente a la intimidad, y otros cuya revelación solo alcanza a la privacidad, lo cual influyó al legislador a la hora de realizar la separación del 197.

³⁴ CASTAÑO, E. N. (Mayo de 2022). La relevancia penal de las nuevas tecnologías y su incidencia en los denominados cibercrimes: especial referencia a los delitos contra la intimidad. *Revista General de Derecho Penal*(37).

Bien es cierto, por otra parte, que el Art. 197 bis no parece defender directamente la privacidad personal, pues supone más bien un derecho a la no intromisión en el sistema informático, independientemente de si contiene datos reservados o no. Más que defenderse la privacidad en sí misma, se ampara el derecho a la exclusión que se desprende de ella, una suerte de inviolabilidad informática³⁵.

Por último, atendiendo a lo expuesto en el apartado anterior, el tipo del 197 bis 1 será un ciberdelito en sentido estricto. Ya que la incidencia de las TIC es esencial, si se atiende al tenor del artículo, este no podría existir sin los elementos informáticos que lo componen³⁶.

1.2.3.-La posición del proveedor

Se ha hablado del acceso ilícito en abstracto, y referido a un supuesto sencillo en el que un individuo accede al sistema informático de otro sin mayor complejidad. Sin embargo, en la realidad, los datos personales pueden estar siendo tutelados por terceros. A estos se los conoce como intermediarios, proveedores de servicios o «providers»³⁷.

Incluso suponiendo que los providers son personas físicas, su atribución de responsabilidad es compleja. Y lo es, entre otras cosas, por su fuerte carácter transnacional, ya que los servidores que se utilizan para cometer un delito en España pueden encontrarse en distintos países. Por eso la colaboración internacional era necesaria, así la UE tomó una posición armonizadora en esta cuestión, creando la directiva 200/31/CE de 8 de junio del 2000.

Esta trataba aspectos jurídicos de los servicios del comercio electrónico en el mercado interior y el régimen de responsabilidad propio de estos providers. Es importante mencionarla porque será la principal fuente de inspiración para la Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y del correo electrónico (LSSI). Esta delimita la responsabilidad de los providers también en el ámbito penal.

³⁵ La protección de esta inviolabilidad posibilita el adecuado ejercicio de la intimidad personal, pues si no se impidiera o disuadiera del acceso a los sistemas informáticos particulares, todo dato personal quedaría al descubierto. Y estos deben ser protegidos, aunque no contengan elementos reservados, pues no se puede exigir al titular un especial deber de cuidado a la hora de ejercer un derecho que es tan fundamental como cotidiano. MUÑOZ, A. G. (2021). Compliance frente a delitos informáticos. En S. B.-B.-P. MIGUEL ABEL SOUTO, *Estudios penales en homenaje al profesor José Manuel Lorenzo Salgado* (págs. 553-572). Valencia: Tirant lo Blanch.

³⁶ CASTAÑO, E. N. (Mayo de 2022). La relevancia penal de las nuevas tecnologías y su incidencia en los denominados ciberdelitos: especial referencia a los delitos contra la intimidad. *Revista General de Derecho Penal*(37).

³⁷ MUÑOZ, A. G. (2019). *Los ciberdelitos en el ordenamiento español*. Barcelona: Editorial UOC

Es bastante común que el creador de contenido que se difunde, y quien lo hace accesible por tenerlo almacenado (host) sean personas diferentes. La tarea de proveer almacenamiento es bastante común, y a esta hace referencia la responsabilidad de los prestadores de servicios la LSSI en su capítulo II. El artículo 13 establece que las empresas o personas que presten servicios de la información son susceptibles de responsabilidad penal. Sin embargo, los artículos siguientes establecen un régimen de exenciones, considerando cuando estas habrán tratado los datos con el debido cuidado.

En nuestro caso, nos resulta interesante el Art 15, aunque su redacción no versa directamente sobre la responsabilidad del provider cuando se da un acceso ilícito sobre datos custodiados por estos. En concreto, este artículo habla de los prestadores de servicios que realizan copias temporales de los datos solicitados por los usuarios. Y se exime de responsabilidad a estos cuando permitan el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas al fin por el que crean la copia.

Esta es la única mención que puede relacionarse con el acceso ilícito en el capítulo, pues el resto de los artículos versan sobre la responsabilidad de los proveedores a la hora de manipular datos ilícitos.

Se puede deducir entonces que el legislador no ha pensado en establecer responsabilidad para los proveedores cuando un tercero acceda (online) a un sistema informático de un particular a través de sus servicios, o violando su seguridad (la cual puede ser más o menos pobre). O incluso en el caso en que los mismos providers transmitan esa información, siempre que no sea ilícita. Habrá que ver, más adelante, a qué sujetos en particular se refiere el 197 quinquies.

1.2.3.-Conclusión

La ingente cantidad de mandatos internacionales al respecto del derecho penal informático ha tenido sus frutos en España. Pues nuestro código penal ha introducido y modificado estos tipos ya en tres ocasiones.

La legislación no cuenta con un título particular para los delitos informáticos, sino que estos se encuentran redactados, de forma específica, junto a delitos preexistentes. Esto colinda con la perspectiva dominante en la doctrina, que entiende que no existen o no deben existir bienes jurídicos autónomos referidos a estas conductas. En concreto, el delito de acceso ilícito velará, según el derecho positivo, por la privacidad, más que por la intimidad

personal. Aunque esto queda discutido por gran parte de la doctrina. De un lado hay quienes siguen defendiendo la vigencia y defensa de la ciberseguridad como bien jurídico supraindividual. Y de otro, están quienes encauzan la cuestión a través de la inviolabilidad informática.

Sobre él cabe añadir, que se trata de un delito de peligro abstracto, y un delito informático en sentido estricto, siguiendo la clasificación anteriormente presentada. Y que la conducta típica requiere una manipulación de las medidas de seguridad propias del sistema informático al que se accede, pero no necesita que los datos que de tal se obtienen sean reservados.

2.-RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

Elaborar un análisis detallado de la responsabilidad penal de las personas jurídicas no es una tarea sencilla, por lo que siempre quedarán recovecos inexplorados al llevarla a cabo. Más aún cuando se la pretende comprimir en el menor espacio posible.

Sin embargo, se ha procurado tocar con la profundidad suficiente todos aquellos temas atinentes a la misma que permitan tener una visión clara de su funcionamiento. Pues de otra manera sería imposible incardinar esta responsabilidad con el añadido del delito informático.

2.1.-ANTECEDENTES

Iniciar un análisis de la responsabilidad penal de las personas jurídicas desconociendo su origen supondría obviar los cimientos sobre los que se erige la RPPJ y sus limitaciones. Cabe destacar que, por la naturaleza del asunto, el principio *societas delinquere non potest* y sus orígenes serán cardinales; pues su vigencia ha determinado un antes y un después en esta materia.

Que este postulado esté bien integrado (aunque ya se le haya negado en el CP) en la mente de cualquier jurista actual, contrasta con el hecho de que, durante la mayor parte de la historia del derecho, no estuvo vigente. Sino más bien todo lo contrario, la punibilidad de las personas morales es la norma desde el Derecho romano hasta la mitad del S.XIX

Al concepto de *societas delinquere non potest* se le atribuyen distintos orígenes, hay quienes argumentan que proviene del Derecho Romano, otros defienden que la acuñó Inocencio IV, hay teorías sitúan su origen en el S.XIX y, por último, algunos autores han postulado que su origen es desconocido. De entre todas estas hipótesis, destaca la de MARTINEZ PATÓN³⁸, que señala a FRANZ VON LISZT como posible autor de esta locución, pues no existen registros de su uso en textos anteriores a 1881, y a partir de entonces, estos apuntan al jurista alemán como su acuñador.

³⁸ VÍCTOR MARTÍNEZ PATÓN. “Análisis histórico de la responsabilidad penal corporativa”, Tesis doctoral Universidad Autónoma de Madrid. Madrid-París, 2016.

2.1.1.-Origen: La responsabilidad colectiva en la Antigüedad.

Se estima que la primera expresión de punibilidad colectiva se dio en el año 1750 a.C.; donde el código del rey Hammurabi de Babilonia recogía tanto responsabilidad para unidades familiares como territoriales (Ej. Ciudades)³⁹.

Los antiguos griegos y romanos también contaban con sistemas de responsabilidad penal solidaria. Los primeros (aun no contando con la palabra *ius* ni Derecho en su vocabulario⁴⁰) utilizaban experiencias jurídicas similares a las ya mencionadas: de responsabilidad familiar, nacional, local, etc. Mientras que, en el Derecho romano, aunque se desconocía el concepto de persona jurídica, sí existían agrupaciones a las que se le atribuían derechos y deberes colectivos⁴¹.

Lo más relevante, porque será la base sobre la que edificarán los autores medievales y modernos, es que el Derecho romano distinguía a los *singuli* de las *universitas*. Los primeros serán los miembros de las corporaciones. Mientras que los segundos eran la corporación misma.

Por último, pese a que sí se considerara a las *universitas* como entes con responsabilidad penal colectiva⁴², los romanos se limitaron a formular principios que expresaban las funciones mecánicas de las mismas⁴³, por lo que no se puede hablar de RPPJ sensu stricto en este periodo.

³⁹ El Código de Hammurabi. MARÍA PILAR RIVERO GARCÍA. Clío: History and History Teaching, N° 7, 1999. <<http://clio.rediris.es/fichas/hammurabi.htm>> [Consulta: 29 noviembre 2022]

⁴⁰ PANIAGUA, J. M. (1988). *Historia del pensamiento jurídico I, de Heráclito a la Revolución francesa* (sexta ed.). Madrid: Universidad complutense de Madrid.

⁴¹ Aunque en esta época existieron numerosas denominaciones de personas colectivas, pues existían las *societas* y las *societas publicanorum*. Estas *societas* servían para relativizar la responsabilidad de una empresa compartiéndola entre los socios, podrían asemejarse, salvando mucho las distancias, a los actuales patrimonios de afectación. Mientras que las *societas publicanorum* son una suerte de proto sociedad anónima.

PHILIP J. STERN. *The corporation, a critical, multi-disciplinary handbook*, Cambridge, Cambridge University Press, 2017, pp. 21 - 46

⁴² Los autores que defienden la tesis de que en la antigua Roma existió la responsabilidad penal corporativa lo hacen a través de dos ejemplos. En primer lugar, las destrucciones de derechos que se dieron en algunas ciudades a modo de castigo a razón de, por ejemplo, abandonar a Roma durante una guerra. En segundo lugar, existía una especie de responsabilidad penal solidaria en las legiones, a través del diezmo. Este era un castigo militar que consistía en la ejecución al azar de un hombre de cada diez dentro de una legión o cohorte. Antecedentes históricos de la responsabilidad penal de las personas jurídicas.

LUCAS GABRIEL MENÉNDEZ CONCA. *Revista Ratio Juris*. Vol. 16 N° 32, 2021, pp. 93-116.

⁴³BACIGALUPO SILVINA. “La responsabilidad penal de las personas jurídicas”, Capítulo I: Los fundamentos clásicos de la máxima *societas delinquere non potest*. Antecedentes históricos, Bosch, 1998, Pp. 19-29.

2.1.2.-Universitas en la Edad Media

Las sociedades medievales estaban políticamente en cuanto a que carecían de un estado articulado. No existía un poder omnicompreensivo que controlara y unificara las relaciones sociales de aquellos afectados por su *imperium*.

Este hueco de poder fue ocupado principalmente por las corporaciones. Estas adquirieron un gran poder político y económico.

Por otra parte, la irrupción de la iglesia como otro ente de poder fáctico fue harto relevante para el debate sobre la punibilidad de las corporaciones. Pues a partir de los S. XII y XIV los privilegios antes particulares de otros estamentos les fueron atribuidos a universidades, ordenes monacales y similares.

A razón de su creciente importancia son los canonistas los que empiezan a elaborar un concepto abstracto de la personalidad jurídica. Y lo hacen partiendo del principio de que los derechos no pertenecen a los fieles, sino a Dios⁴⁴.

Estos juristas utilizan como base las categorías de *universitas* y *singuli* romanas, por lo que distinguen a la persona humana de la real. Y es aquí donde se diferencian de forma clara y concisa los derechos de estas dos partes, se concibe a la *universitas* como una persona ficticia, viéndose aquí por vez primera la concepción moderna de persona jurídica.

De entre los canonistas nos resulta interesante INOCENCIO IV por sus escritos acerca de la punibilidad de las corporaciones. Algunos historiadores le atribuyen la creación del principio *societas delinquere non potest* ya que el papa defendió que la pena de la excomunión (entre otras) no podía recaer sobre las ciudades ya que estas «no tenían alma», y por ende tampoco capacidad delictiva.

Sin embargo, se discute que el autor considerara que las personas fictas no pudieran delinquir, ya que se refería al castigo de la excomunión (que es una pena con una naturaleza muy particular) y no al compendio de la punibilidad corporativa. Lo relevante es que Inocencio estableció la percepción de las *universitas* como personas ficticias fue tomada y desarrollada por sus sucesores.

Hubo autores, en concreto BARTOLO DE SASSOFERRATO⁴⁵, que definieron a la capacidad delictiva de las *universitas* como una ficción jurídica. Y todo porque si la propia

⁴⁴ BACIGALUPO SILVINA. “La responsabilidad penal de las personas jurídicas”, Capítulo I: Los fundamentos clásicos de la máxima *societas delinquere non potest*. Antecedentes históricos, Bosch, 1998, Pp. 19-29.

⁴⁵ Este jurista italiano vivió de 1313 a 1357 y es considerado por muchos como el máximo exponente de la tradición romanística europea durante el medievo. DÍEZ HERRERA, C (II) Y ARIZAGA, B (II). “Mundos medievales: espacios, sociedades y poder: homenaje al profesor José Ángel García de Cortázar y Ruiz de Aguirre”. Tomo II. Santander, Spain: Editorial de la

universitas sobrevive a sus miembros, también lo harán las acciones que emanan de ella. Además, Bartolo definió dos tipos de acciones que podrían emanar de estas personas jurídicas: la emitidas de forma propia y las de forma impropia.

Las propias se corresponden con los delitos omisivos que la persona lleva a cabo en el ejercicio de sus deberes particulares, mientras que los impropios serán aquellos que sólo puedan emanar de un *singuli* pero se cometan a través de otros, es decir, que no son delitos relacionados con las atribuciones propias de la personalidad jurídica. (una persona jurídica no podrá cometer homicidio por sí misma, necesita de uno de sus miembros-impropio-, pero sí podrá, por ejemplo, malversar fondos)

Pero para la comisión de delitos, se den de forma propia o impropia, se exigía que la acción fuera fruto de la voluntad ficticia de la persona jurídica, es decir, que no fuese un acto deliberado de alguien que se desmarcara.

Este antiguo jurista también trató sobre el castigo a las acciones cometidas por *universitas*, en concreto si estas debían repercutir sobre ellas o el compendio de sus miembros. Para él, esto dependerá de si se trata de delitos propios o impropios. Según Bartolo la corporación debería ser castigada por los delitos propios, siendo en este caso considerados como instigadores sus miembros. Y en el caso de los impropios, la *universitas* sería la instigadora y los culpables los *singuli*⁴⁶.

Mención especial merecen algunas otras formas de solidaridad penal derivadas de la costumbre y pertenecientes a un derecho que no toma como base el romano. Destaca en concreto la catalogación de responsabilidad corporativa en la categoría de *frankpledge* o *frithborh*: el castigo de todos los miembros de un grupo cuando uno de ellos ha evitado ser enjuiciado por un crimen⁴⁷. Es una institución de origen inglés, en virtud de la cual, la responsabilidad por comisión de crímenes en 10 casas de un pueblo se les atribuía a sus diez

Universidad de Cantabria. Bartolo da Sassoferrato: introduzione a un giurista globale. Mario Ascheri. Università di Roma 3, 2014, Pp. 1029-1041

⁴⁶Antecedentes históricos de la responsabilidad penal de las personas jurídicas. LUCAS GABRIEL MENÉNDEZ CONCA. Revista Ratio Juris. Vol. 16 N° 32, 2021, pp. 93-116.

⁴⁷ Fue una institución introducida en tiempos de Canuto II el Grande, rey de Inglaterra entre 1016 y 1035. Este término se opone al de *deodand*, que implica el castigo de objetos o animales que hayan causado daño. La categorización de la responsabilidad punitiva de las colectivas encaja en mayor medida con el primer concepto. Aunque se critica que el modo de establecer la criminalidad de entes atiende a un fin de inducir un mayor control interno en las corporaciones en lugar de suponer un castigo criminal sensu stricto. ALSCHULER, A. (2009). *Two ways to Think about the Punishment of Corporations*. Recuperado el 29 de Noviembre de 2022, de Northwestern Pritzker School of Law Scholarly Commons: <https://scholarlycommons.law.northwestern.edu/facultyworkingpapers/192>

patriarcas, y si cualquier miembro escapaba tras cometer un hecho delictivo, el resto eran castigados con una multa⁴⁸.

2.1.3.-Edad Moderna y responsabilidad corporativa

Durante los periodos tendentes al absolutismo, las teorías referidas a las corporaciones de Bartolo Sassoferrato seguían siendo el mayor referente para los juristas de la época, que fueron desarrollando, a la par que se erigía un Estado institucionalizado, el estudio de la responsabilidad corporativa. La época no fue tan prolífica como la edad media en este respecto, mayormente encontramos a juristas que cuestionan y modernizan las perspectivas del autor italiano.

Por otro lado, en este periodo comienzan a tener mayor relevancia los escritores del *common law*⁴⁹. El que más interesa a los efectos de este escrito es BLACKSTONE (1765), este importante autor dedicó tiempo al estudio de las corporaciones, su responsabilidad civil y penal. Aquí es donde se puede ver la primera defensa tajante y elaborada de que las personas jurídicas no pueden delinquir. La obra y opinión de BLACKSTONE tuvo gran influencia en el derecho continental, sobre todo a través de Francia, donde sus obras fueron traducidas, publicadas y comentadas.

Consecuencia de ello será, además, que, a la doctrina francesa, que inspirará las ordenanzas promulgadas por los revolucionarios, se traslade el concepto de corporación inglés, distinto de la tradicional *universitas*.

Aunque algunos autores estuvieran cuestionando la responsabilidad corporativa; en aquella época se siguieron realizando castigos corporativos, estos cayeron mayormente sobre

⁴⁸ Esta institución evolucionó y fue también adoptada por los Normandos y otros pueblos del noroeste europeo, y supuso una buena solución a la ausencia de fuerzas del estado profesionales en tiempos anteriores a la llegada de estados absolutistas. Concretamente desapareció en el siglo XV por la aparición de las justicias de paz VÍCTOR MARTÍNEZ PATÓN. “Análisis histórico de la responsabilidad penal corporativa”, Edad moderna (I): Siglos XVI y XVII, Tesis doctoral Universidad Autónoma de Madrid. Madrid-París, 2016. Pp. 257-246

⁴⁹ De entre ellos, cabe destacar también a ROGER MANHOOD (1580); este jurista inglés siguió la tesis que INOCENCIO IV usó para defender que las ciudades no podían ser excomulgadas por no tener alma y se la aplicó a todo tipo de corporaciones. MANHOOD se limita a trasponer las teorías ya formuladas por los canonistas al derecho inglés.

Seguidamente tendrá interés su predecesor: EDWARD COKE, quien defenderá que existen acciones determinadas cuya punición necesitara que el sujeto activo tenga alma, es decir, que sea una persona con libre albedrío o voluntad. Lo que consigue este autor es que la perspectiva de MANHOOD tenga una mayor aceptación entre la doctrina y juristas ingleses de la época .

VÍCTOR MARTÍNEZ PATÓN. “Análisis histórico de la responsabilidad penal corporativa”, Edad moderna (I): Siglos XVI y XVII, Tesis doctoral Universidad Autónoma de Madrid. Madrid-París, 2016. Pp. 257-246

entes municipales. Por ejemplo, en 1548 sobre Burdeos, en 1567 sobre Beaufort, en 1607 sobre Donauwörth o en 1739 sobre Grosselfingen y Hausen⁵⁰.

Esta práctica se fue mitigando progresivamente hasta el Siglo XIX, donde la instauración del absolutismo había finiquitado la influencia y poder que tenían las corporaciones y señoríos de la época.

2.1.4.-Revoluciones francesa y norteamericana⁵¹: El Derecho penal liberal y las corporaciones

Durante este periodo se tomarán los principios elaborados por BLACKSTONE para abordar la cuestión de la responsabilidad solidaria desde nuevos prismas.

Durante el mismo, los revolucionarios, fundándose en postulados primero iusnaturalistas y después ilustrados, erigen un nuevo orden social y jurídico. Ahora se trata de construir un estado con monopolio de la violencia, donde el pueblo (o más bien sus ciudadanos más pudientes) sea soberano y donde no existan privilegios estamentales que nieguen de algún modo la libertad del individuo-ciudadano.

Siendo el individuo el centro del proceso penal, el debate sobre la idoneidad de la solidaridad penal quedó zanjado en favor de un principio que la excluyera. Además, la responsabilidad corporativa quedó ligada al AR, lo cual generaba más reticencias a aceptarla.

Existen dos hipótesis principales sobre el origen de la supresión de la responsabilidad corporativa: Puede que dejara de ser aceptable a causa de la vigencia de los derechos del hombre y del ciudadano. O cabe considerar que terminó por falta de necesidad al desaparecer las corporaciones medievales⁵².

De entre los distintos textos de derecho revolucionario que se dieron en este periodo destacan, sobre todo, la ley de Allarde y la ley de le Chapellier.

Los dos últimos textos estuvieron influidos por las ideas de pensadores como ROUSSEAU⁵³, entre otros; y su análisis puede apoyar la tesis de que las corporaciones fueron

⁵⁰ LUCAS GABRIEL MENÉNDEZ CONCA. “Antecedentes históricos de la responsabilidad penal de las personas jurídicas”, Revista ratio iuris, Vol. 16 N° 32, 2021, pp. 93-116.

⁵¹ Se prestará atención en exclusiva a la revolución francesa, pues de ella emanan todos los postulados que nos pueden resultar de interés en un apartado que se pretende sintético.

⁵²Antecedentes históricos de la responsabilidad penal de las personas jurídicas. LUCAS GABRIEL MENÉNDEZ CONCA. Revista Ratio Juris. Vol. 16 N° 32, 2021, pp. 93-116.

⁵³ Es importante recalcar la influencia de Rousseau en el debate acerca de la punibilidad de las corporaciones, pues es un buen punto de partida. A la hora de definir orden social que no está regido por el autoritarismo equivalente al de un padre sobre sus hijos o un pastor sobre su rebaño, Rousseau defiende que la sociedad abandona su estado salvaje plasmando su voluntad en un contrato social. Y, para que esa voluntad general, que

erradicadas en favor de la necesidad de eliminar sus privilegios en favor de la libertad de empresa.

Primero, la ley de Allarde suprime las corporaciones para defender el libre comercio, al mismo tiempo que elimina cualquier tipo de protección o privilegio que se heredada del antiguo régimen. Como esto condujo a diferentes revueltas de artesanos y obreros que quedaron desprotegidos salió la ley de Le Chapelier; que, en teoría, crearía nuevos mecanismos de protección para estos agentes⁵⁴.

La segunda tesis antes mencionada defendía que fue la vigencia de los derechos individuales y de un Derecho penal moderno la que condujo a que se erradicara la RPPJ.

En estos momentos tuvo una gran influencia el Tratado de los delitos y las penas (1764) de Beccaria. En él no se hace mención alguna al derecho penal corporativo, y, como quien calla otorga, cabe cuestionarse por qué.

Puede que el autor considerara tan trivial la impertinencia de esta responsabilidad en el derecho penal moderno que ni la mencionó. O puede que quisiera crear una obra dedicada sólo al derecho penal individual, sin que eso supusiera la necesidad de dejar fuera de ese ámbito a una posible responsabilidad colectiva.

Los defensores de esta tesis argumentan que el hecho de que se cree un derecho penal moderno, donde el individuo es el centro del proceso, choca de base con la responsabilidad penal de entes no humanos.

Independientemente de cuál se entienda por verdadera causa de la erradicación de la punibilidad corporativa. Lo cierto es que al desaparecer las corporaciones con la ley de Allarde, así lo hace su responsabilidad penal. Sin que eso afecte a la vigencia de penas

es soberana, no hierre, "*Importa (...) que no existan sociedades particulares en el Estado, y que cada ciudadano opine con arreglo a su manera de pensar*"

Es en el capítulo tercero del libro segundo del Contrato social donde el autor se cuestiona si la llamada voluntad general tiene capacidad de errar, y al hacerlo, llega a esa conclusión, de que lo hará en menor medida si no cuenta con intermediarios. (instituciones intermediarias, que vendrán a ser las corporaciones que conserven privilegios feudales). Aquí se defiende la erradicación de las corporaciones por contravenir la creación de un Estado donde el pueblo sea soberano.

ROBERTO CAÑAS QUIRÓS. "El contrato social de Rousseau: el problema de la natural enemistad entra la soberanía y el gobierno". Revista Estudios, Universidad de Costa Rica. No. 21, 2008, pp. 137-148. Citando a ROUSSEAU, loc. cit., pp. 56-59, en la edición de 1762

⁵⁴ En este respecto, cabe destacar una interpretación particular, y es la que se encuentra en el primer tomo del Capital de Karl Marx, donde se argumenta que la desaparición de las corporaciones en favor de la libertad de empresa por medio de prohibir toda sindicación obrera (cosa que hacía la ley de Le Chapelier), no era más que un medio de asegurar la dominancia de la clase burguesa.

Esta concepción llevaría a pensar que la erradicación de la responsabilidad penal de las personas jurídicas es algo cómplice, pues deja un amplio margen a las empresas (entre otras) para que actúen con libertad absoluta, incluso si esto supone menoscabar los derechos tanto de sus miembros como de la sociedad en general. VÍCTOR MARTÍNEZ PATÓN. "Análisis histórico de la responsabilidad penal corporativa", Edad moderna (II): El Siglo XVIII, Tesis doctoral Universidad Autónoma de Madrid. Madrid-París, 2016. Pp. 347-451

aplicables a otros tipos de personas fictas: las *universitates*, que podrán ser territoriales, sin ánimo de lucro, con ánimo de lucro, sociedades y compañías⁵⁵.

2.1.5.-S.XIX y XX

Lo que caracterizó al siglo XIX fue la pluralidad de tesis sobre el tema de la punibilidad corporativa. Se reabrió sin tapujos el debate que se había dado por sentado durante la legislación revolucionaria.

Durante este prolífico periodo encontramos a numerosos autores defendiendo la tesis de la no punibilidad corporativa.

Estos juristas defendieron esta postura esgrimiendo diversos razonamientos: Algunos se basaban en la teoría de la ficción para defender que un ente sin voluntad no tendría jamás capacidad delictiva. Otros afirman que la responsabilidad de la persona jurídica sería la de sus miembros; y que, consintiéndola, aquellos que no han hecho nada, incluso quienes se adhieran al ente en un futuro, sufrirían consecuencias sin ser culpables.

La lista de argumentos, como que las personas jurídicas no pueden comprender la aplicación de la pena, podría seguir hasta la infinitud. Sin embargo, se presta más práctico centrar la atención a tres autores en particular.

En primer lugar, está el autor a quienes algunos historiadores le atribuyen la acuñación del principio *societas delinquere non potest*, LIZST⁵⁶. Y lo interesante, más que el significado de este es el hecho de que la no responsabilidad penal se predique de las *societas* en lugar de las *universitas*, que eran el objeto de debate hasta el momento. El resultado sería limitar el debate de la responsabilidad penal corporativa a la societaria. Por otra parte, se ha interpretado en sentido amplio el brocado, pues la significación que se le da es la de la no RPPJ.

Por último, son importantes las teorías de la persona jurídica de SAVIGNY y OTTO VON GIERKE. Estos juristas confrontaron sus respectivas teorías de la ficción y orgánica para defender la tesis de la no responsabilidad penal de las personas jurídicas y su contraria.

⁵⁵ LUCAS GABRIEL MENÉNDEZ CONCA. “Antecedentes históricos de la responsabilidad penal de las personas jurídicas”, Revista ratio iuris, Vol. 16 N° 32, 2021, pp. 93-116.

⁵⁶ Este autor formaba parte de la doctrina que escribía en favor de la RPPJ, pero escribió este principio en su obra *Das Deutsche Reichsstrafrecht* (1881) a la hora de explicar cuál era la doctrina dominante de la época en esta materia.

VÍCTOR MARTÍNEZ PATÓN. “Análisis histórico de la responsabilidad penal corporativa”, El siglo XIX, Tesis doctoral Universidad Autónoma de Madrid. Madrid-París, 2016, Pp. 451-524.

Savigny defendía que sólo los individuos naturales tienen capacidad de derecho, al ser esta una limitación a la libertad proveniente de la moral. Sin embargo, el derecho positivo puede negar esa realidad a través (en este caso) de la ficción de que las personas artificiales tienen capacidad jurídica. Así pues, Savigny concluye que las personas jurídicas no obran como tales cuando cometen delitos, sino que estos siempre los realizan personas naturales que las componen.

Si la teoría de la ficción parte de que solo la persona natural tiene capacidad de derecho al tener un raciocinio moral que le permite limitar la libertad. La orgánica baja a la tierra y observa cuál es la realidad social.

Tanto individuos como personas jurídicas gozan de una voluntad que les permite operar en el mundo del derecho. Olvidar las consecuencias de las acciones tomadas por parte de una persona ficticia sería falsear la realidad, estas existen en el tráfico jurídico emanen de una voluntad colectiva o de una individual.

Gierke defendía que la persona jurídica era una persona viva, real, capaz de obrar a través de sus órganos como lo hacen los humanos naturales. Y como tal podrá cometer delitos y ser sometida a penas acorde con su naturaleza, desde las pecuniarias hasta la disolución.

El debate continuó a finales del XIX y a lo largo del XX, y la influencia de GIERKE fue crucial, pues aumentó el número de autores en favor de la responsabilidad penal de las personas jurídicas.

2.1.7.-Conclusión

El recurso a la atribución de penas a entes colectivos ha sido no sólo común, sino imperante a lo largo de la historia. Este se ha ido adaptando a la manera en que mutaban las personas colectivas en los distintos modelos estatales y preestatales.

En sociedades más primitivas se utilizaba la institución social de la familia para crear una responsabilidad común, con la aparición de las corporaciones como entes de derecho independientes (y su correspondiente consideración como personas jurídicas) se elaboraron métodos de castigo colectivo que podían afectar hasta a ciudades enteras. Y, por otra parte, con la instauración del estado moderno el uso de estos recursos fue desapareciendo.

Hay quienes defienden que el desuso de estas instituciones y su posterior negación por parte de la doctrina son cómplices de un sistema que pretende proteger a las *societas* (que a partir del s. XVIII adquirieron una gran relevancia). Sin embargo, la intención con la que

se eliminara esta institución es irrelevante, lo que nos interesan son sus efectos: las sociedades han quedado libres de ser penadas hasta hace bastante poco.

Por último, debe tenerse en cuenta que afirmar tajantemente que durante la mayor parte de la historia del derecho existió la RPPJ sería faltarle a la verdad. En cuanto a que antes de su elaboración por parte de los canonistas no existía un concepto estricto de persona jurídica. Y en cuanto a que hasta los primeros códigos penales no se tenía noción de un Derecho penal moderno. Precisamente por los principios que este último enuncia, la doctrina tradicional rechazaba la implantación de la RPPJ. Esta es de difícil encaje en un sistema penal donde imperan los principios de culpabilidad y de personalidad de las penas.

Lo verdaderamente importante es destacar que el principio *societas delinquere non potest* no es ningún axioma inamovible, ni inmediatamente deducible de los principios regidores de nuestro sistema penal. Es decir, no hay por qué darle por supuesto, cabe su cuestionamiento y quebranto.

2.2.-RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS EN EL DERECHO ACTUAL

En este apartado se trata de explorar no sólo cómo regula nuestro CP la responsabilidad de estos entes, sino cómo se configuran las bases mismas del modelo elegido por el legislador. Es decir, se ha primado ofrecer una visión genérica, pero clara, de cómo se incardina esta responsabilidad por el Derecho español desde sus bases más profundas.

La concreta aplicación del Art. 31 y sus consecuencias serán vistas de manera más exhaustiva en atención al delito en particular que nos ocupa: el acceso ilícito. Y esto será planteado en el apartado tercero del trabajo.

2.2.1.-El Código penal español y su modo de imputación de responsabilidad penal a las personas morales

Es en 2010 cuando por vez primera se derrumba en España al principio *societas delinquere non potest*. Pues desde 1983 se le proclamaba en el artículo 15 CP⁵⁷. En esta reforma (con raíces en otra de 2003 y después modificada en 2015) se introduce la responsabilidad directa de las personas jurídicas para un numerus clausus de conductas.

⁵⁷ Si bien en el código de 1995 se incluía un el artículo 262 una imposición a la empresa a pena de inhabilitación especial, este no fue tomado como una proclamación de la RPPJ en su momento. CUESTA ARZAMENDI, JOSÉ LUIS. NORBERTO J. DE LA MATA BARRANCO. (2013). *Responsabilidad Penal de las Personas Jurídicas*. Pamplona: Aranzadi, pág. 51.

En este apartado se pretende aclarar, de forma breve, cuál es el contenido y significado exacto de los artículos de 31 bis a 31 quinquies. Pues sin conocer las bases de la responsabilidad penal difícilmente se podrá acotar el significado y connotaciones del 197 quinquies.

En primer lugar, el artículo 31 Bis indica los supuestos en los que la persona moral es susceptible de ser penada. En el párrafo uno permite atribuirle a esta los hechos cometidos por quienes tengan potestad de actuar en su nombre u ostenten facultades de organización/control sobre ella.

Seguidamente, la parte b) de ese epígrafe introduce la responsabilidad por los hechos que podrían cometer los subordinados a los sujetos del apartado a) que pudieran cometer estos delitos por incumplimiento grave de los deberes de control que se les adscriben⁵⁸. A primera vista puede apreciarse que se acepta un sistema de heteroresponsabilidad⁵⁹ en el apartado primero y uno de autorresponsabilidad⁶⁰ en el segundo, parece así que el CP español sigue una suerte de sistema mixto⁶¹.

Pero puede defenderse que ese no es el caso. El propio Art. 31 ter explicita que la *universitas* será imputada directamente, pues no es preciso si quiera haber individuado a la persona física sobre la que se erige el tipo (incluso se puede imputar a la persona moral con la física fallecida).

Esto abre la posibilidad a la autorresponsabilidad en nuestro ordenamiento, pues el artículo continúa indicando que no será preciso demostrar la culpabilidad de la persona física actuante; tal prescindibilidad muestra que sólo se precisa de ella un acto típico y antijurídico para fundar la imputación de la persona moral por la vía del 31 bis 1. Por lo que la persona no natural comete, por sí misma, el acto en cualquiera de los casos. De hecho, la responsabilidad corporativa será autónoma y acumulativa a la de la persona física⁶².

⁵⁸ ZÚÑIGA RODRÍGUEZ, LAURA. KLAUS TIEDEMANN. (2009). *Bases para un modelo de imputación de responsabilidad penal a las personas jurídicas*. Pamplona: Aranzadi.

⁵⁹ Es el modelo de la transferencia o la atribución. Aquí se da la imputación de la persona jurídica por hechos que ha cometido una persona natural miembro, se traslada la responsabilidad de un sujeto a otro. PÉREZ ARIAS, J. (2014). *Sistema de atribución de responsabilidad penal a las personas jurídicas*. Madrid: Dykinson.

⁶⁰ La persona jurídica responde de su propia conducta, sin fundar la imputación en actuaciones ajenas.

⁶¹ CUESTA ARZAMENDI, JOSÉ LUIS. NORBERTO J. DE LA MATA BARRANCO. (2013). *Responsabilidad Penal de las Personas Jurídicas*. Pamplona: Aranzadi

⁶² JOSÉ MARÍA LUZÓN CUESTA, ALEJANDRO LUZÓN CÁNOVAS, MARÍA LUZÓN CÁNOVAS. (2021). Tema 15. En A. L. JOSÉ MARÍA LUZÓN CUESTA, *Compendio de Derecho Penal* (págs. 213-228). Madrid: Dykinson, S.L.

Por otra parte, el Supremo sacó una importante sentencia que despeja dudas sobre la correcta interpretación del Art. 31 bis. La STS 154/2016 indica que «*la determinación del actuar de la persona jurídica, relevante a efectos de la afirmación de su responsabilidad penal (...), ha de establecerse a partir del análisis acerca de si el delito cometido por la persona física en el seno de aquella ha sido posible, o facilitado, por la ausencia de una cultura de respeto al Derecho*»⁶³

De esto puede concluirse que nos encontramos ante un sistema de autorresponsabilidad donde la persona moral es imputada por sus actos propios. Concretamente, la acción parece de corte omisivo: no contar y hacer respetar una «cultura de respeto al Derecho»⁶⁴ en su seno⁶⁵. Así pues, el fundamento de la culpabilidad de la persona jurídica será el «defecto de organización»⁶⁶.

El apartado dos del artículo 31 bis contiene supuestos de exención de responsabilidad por las conductas del epígrafe anterior. Lo que se hace aquí es establecer cómo debe desarrollarse esa cultura de respeto al Derecho, es decir, el régimen general de los *compliance programs*.

Dejando atrás los modos de imputación de responsabilidad, el 31 bis cuenta con mayores requisitos para que esta se dé. A mayores, el artículo indica que los actos realizados por las personas del apartado primero han de ser «en su beneficio directo o indirecto». Esto quiere decir que la empresa ha de tener un «provecho»⁶⁷, una ventaja o incluso (como defiende la STS 154/2016) una simple expectativa de tal.

¿Y qué comprende el concepto de beneficio en este caso? Puede tratarse de lucro, ventajas competitivas, mejora de la posición respecto de los competidores, un mantenimiento de la buena imagen ... Se presta como un concepto jurídico indeterminado, dependiente de la interpretación en el caso concreto. Uno que además relacione la existencia del delito con la obtención del provecho.

Por tanto, los delitos cometidos por las personas jurídicas se configuran como tipos de comisión por omisión. En este caso se imputa a la persona jurídica la situación delictiva

⁶³ Vd. Fundamento del derecho Octavo de la STS 154/2016, 29 de febrero de 2016.

⁶⁴ Esta concepción parte de la teoría constructivista, la cual se fundamenta en los sistemas autopoiéticos de LUHMANN. (AGÜERO, 2010) y (La responsabilidad penal de las personas jurídicas, 2018)

⁶⁵ Habrá que tener en mente el voto particular de la sentencia, donde indica que las actuaciones de las personas del art. 31 bis 1 a) son las que fundan la culpabilidad de la empresa en lugar de un concepto tan etéreo como es la cultura de respeto al derecho (por anular el principio de certeza).

⁶⁶ AGUILERA, A. T. (Mayo-Junio de 2015). *Laleydigital*. Obtenido de El libro primero del Código Penal tras la Ley Orgánica 1/2015.

⁶⁷ Expresión que el CP utilizaba antes de la reforma.

que cometen las personas señaladas por el Art. 31 bis, siempre que no se hubiera diseñado una estructura adecuada a los riesgos de la sociedad que pueden culminar en la comisión de un delito.

Por eso también se trataría de delitos de resultado. El cual debe ser evitado creándose una eficaz consideración de los riesgos por parte del ente y métodos acordes para evitar que el peligro devenga en daños a bienes jurídicos concretos⁶⁸.

2.2.2.-El sujeto activo: identificación y naturaleza de la persona jurídica penalmente responsable.

2.2.2.1.-Identificación

Cuando uno se introduce en la cuestión dogmática de la responsabilidad penal de las personas jurídicas, lo primero que se pregunta es cuáles son y cómo las concibe el legislador. Resulta algo chocante la falta de concreción a la hora de conceptuar a la «persona jurídica penalmente responsable». Cuestión que se presta aún más relevante cuando el tipo que se pretende explorar cuenta con el añadido del elemento informático.

Bien es cierto que el artículo 297 CP nos otorga una definición de *societas* (de nuevo no se alude a las *universitas*). Sin embargo, la mayoría de la doctrina ha hecho bien en entender que esta no se aplica al caso de la RPPJ, pues queda relegada a los delitos societarios.

Cuando se acude a las referencias que el legislador del 2010 utiliza en su exposición de motivos como justificación a la introducción de esta reforma; muchas sugieren que debe utilizarse la noción de persona jurídica que sea de uso común en el Derecho nacional (que vendrían recogidas en el artículo 35 CC).⁶⁹

Es interesante el hecho de que el legislador recoge como imputable a toda persona jurídica a excepción de algunas elegidas por el legislador. En concreto, el artículo 35 bis en su apartado quinto indica que no son aplicables a las entidades de Derecho público (y

⁶⁸ BERNARDO FEIJOO SÁNCHEZ, CARLOS GÓMEZ-JARA DÍEZ, CARLOS GRANADOS PÉREZ, ALEJANDRO LUZÓN, MANUEL MARCHENA Y OTROS. (2018). *La responsabilidad penal de las personas jurídicas*. Madrid: Fiscalía General del Estado.

⁶⁹ Esta exposición indica en su punto VII que «son numerosos los instrumentos jurídicos internacionales que demandan una respuesta penal clara para las personas jurídicas». De entre los cuales, el convenio relativo a la protección de los intereses financieros de las CEE indica en su artículo 1 que deben ser consideradas como tales «cualquier entidad que goce de tal régimen jurídico con arreglo al Derecho nacional aplicable, con excepción de los Estados o de otros organismos públicos en el ejercicio de su potestad pública y de las organizaciones internacionales públicas». Y es precisamente esta concepción la que parece usar la LO 5/2010. Ya que la lista de personas jurídicas excluidas de responsabilidad del número quinto del párrafo segundo del artículo 31 bis CP parece intentar dejar fuera a los entes que indica ese artículo primero del tratado.

Sin embargo, el legislador interpreta de forma algo extensiva este criterio, ya que excluye a varios tipos de entes que difícilmente entran en las categorías que menciona el artículo (Lapsus que se matizó con la eliminación de los partidos políticos y los sindicatos de las exclusiones en la reforma del año 2012)

PÉREZ ARIAS, J. (2014). *Sistema de atribución de responsabilidad penal a las personas jurídicas*. Madrid: Dykinson, pág. 44.

asimiladas) ni a las agencias estatales mercantiles. Normalmente estas excepciones se justifican indicando que el Estado tiene un papel en el ejercicio de las potestades públicas tan fundamental que su afección por la comisión delictiva tergiversaría en exceso el orden constitucional⁷⁰.

Por otra parte, tanto la doctrina como la propia Circular 1/2011 han cuestionado y matizado la presencia de algunas de estas exclusiones. En primer lugar, el artículo exime de este tipo de responsabilidad a las Cámaras de comercio y los colegios.

Muchos no entienden la especial trascendencia constitucional de las actividades llevadas a cabo por estos entes que los llevaría a quedar exentos. Por otra parte, la *Circular 1/2011* matiza que su exención deberá interpretarse de manera restrictiva la exclusión de las organizaciones que ejerzan potestades públicas; siendo esta solo aplicable cuando ejecuten políticas directamente ejecutivas de tales potestades⁷¹.

2.2.2.2.-Naturaleza

Sin una norma o mención del legislador a por qué⁷² y de qué forma se le otorga primero personalidad y después responsabilidad a la persona jurídica; un buen recurso consiste en acudir a su régimen en el orden privado. Lo cierto es que el Código Civil (en sus artículos 35-39 CC) no deja claro si se adscribe a la teoría de la ficción de SAVIGNY, la de la realidad de GIERKE⁷³ o alguna otra.

En este terreno, el uso de una u otra teoría es más inocuo, pero en el ámbito penal tiene mayores consecuencias. No será igualmente considerada la culpabilidad de un ente cuya capacidad volitiva es independiente, que la de uno donde es considerada una mera ficción, una suma de voluntades.

En el Derecho privado la persona física y la jurídica son coexistentes. Pero esta distinción no les impide operar en el tráfico equitativamente. Ambos son reconocidos como

⁷⁰ Aunque no es extraño encontrarse con violaciones de derechos fundamentales que bien podrían ser delictivas cometidas por entidades de Derecho público, como las que se presentan en las conclusiones del abogado general GIOVANNI PITRUZZELLA, de 27 de enero de 2022 (Asunto C-817/19).

⁷¹ CUESTA ARZAMENDI, JOSÉ LUIS. NORBERTO J. DE LA MATA BARRANCO. (2013). *Responsabilidad Penal de las Personas Jurídicas*. Pamplona: Aranzadi, pág. 80.

⁷² La exposición de motivos de la reforma de 2015 alude siempre a la necesidad que suscitan los distintos convenios anticorrupción y contra la criminalidad organizada de introducir esta reforma. Sin embargo, estos solo buscan que se establezcan sistemas para paliarla que bien podrían ser administrativos. Por otra parte, se alude a la estadística de la cantidad de criminalidad que se lleva a cabo por parte de las universidades para justificar la introducción de su responsabilidad penal. En resumidas cuentas, son motivos propios de la política criminal (que debería ir de la mano de la dogmática, no sustituirla).

Vd. *Circular 1/2011*, de 1 de junio, relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 5/2010.

⁷³ *iberley*. (2 de Julio de 2016). Obtenido de Concepto y regulación de las personas jurídicas: <https://www.iberley.es/temas/concepto-regulacion-personas-juridicas-59410>

sujetos con plena capacidad de obrar en el tráfico jurídico. La distinción no falta a la verdad, pues son de naturaleza dispar, existen derechos personalísimos que una persona moral jamás podría ejercer (como el voto, por ejemplo).

Sin embargo, el Derecho civil reconoce que «*quien es capaz de tener derechos tiene personalidad, o lo que es lo mismo, se le atribuye personalidad a quien es apto para ser sujeto de derechos y obligaciones*». ⁷⁴ Esto radica de la autonomía de la voluntad y capacidad de autodeterminación propias de toda persona. Y, aunque parezca que se asume la teoría de GIERKE, nada nos lo asegura, pues en el orden civil existen tanto personas físicas como morales. Además, se dan instituciones, como la del levantamiento del velo, que sugieren una interpretación ficticia de la persona.

Podría leerse que la persona jurídica es considerada tan real en el tráfico jurídico (con sus limitaciones) como la física, siendo esta simplemente de naturaleza diversa.

¿Sería esta asunción transponible al derecho penal? No es algo que pueda afirmarse a la ligera, y nada (salvo la remisión del legislador de 2010 al derecho internacional) nos dice que los criterios privados deban ser aplicados aquí. En este ámbito sólo contamos con lo tipificado, y esto es que las personas morales son susceptibles de cometer delitos ⁷⁵ y ser penadas.

Lo que realmente será coherente con la razón del Derecho penal es un sistema donde, de imputársele penas a la persona moral, sea por sus hechos propios. Más que por los ejecutados por sus miembros, pues lo contrario supondría admitir la responsabilidad penal por el hecho ajeno. ⁷⁶

Volviendo a la concepción que sería menos conflictiva con los principios rectores del DP, cabría pensar que esta es la acuñada por GIERKE ⁷⁷. Sin embargo, esa ha sido superada.

⁷⁴ VILAR, S. B. (Octubre de 2022). Persona, algoritmización y posthumanismo, una ecuación hacia la «persona maquina» y su responsabilidad. *Actualidad Civil, Sección Persona y Derechos*(10).

⁷⁵ Podría decirse que antes no se consideraba que estos entes tuvieran capacidad de cometer delitos, pues sólo se les atribuía consecuencias accesorias en lugar de penas.

⁷⁶ CUESTA ARZAMENDI, JOSÉ LUIS. NORBERTO J. DE LA MATA BARRANCO. (2013). *Responsabilidad Penal de las Personas Jurídicas*. Pamplona: Aranzadi, págs. 69-70.

⁷⁷ Pues sería algo contradictorio atribuirle la responsabilidad penal a un ente incapaz de actuar por sí mismo, con acciones que son ficticias, las propias de una persona física miembro, o la suma de las de sus componentes. Además, la culpabilidad de un ente ficticio sería meramente formal, propia de una persona con capacidad de infracción, pero carente de «*elemento volitivo en sentido estricto*» como así lo afirma la STC 246/1991. Vd. Fundamento jurídico segundo de la STC 246/1991, de 19 de diciembre.

Si lo importante es que la persona cometa un hecho propio, no es absolutamente necesario corporeizarla para llegar a ello. El concepto de personalidad a estos efectos que más acogida ha tenido en el Supremo es la de la teoría de las organizaciones autopoieticas⁷⁸.

En concreto, nos interesa la doctrina de GUNTHER TEUBNER⁷⁹. Aunque esta no es strictu sensu una conceptualización de la persona jurídica, sino una visión aplicable a su funcionamiento⁸⁰. En síntesis, esta teoría crea una analogía entre la autopoiesis celular y el derecho positivo.

El concepto de autopoiesis deriva de la homeostasis, esta explica el mantenimiento de la estabilidad de sistemas naturales complejos (la célula) a través de la información y control (el ADN). La teoría que nos ocupa va más allá, porque habla del mantenimiento de la estabilidad a través de la «auto regeneración». Así pues, una organización autopoietica consistirá en una red cuyos elementos podrán producirse a sí mismos de manera recursiva y en un mismo espacio. Es decir, que la célula tiene la capacidad de «crearse» a sí misma constantemente. Esta se encuentra en un estado de permanente cambio ordenado gracias a sus sistemas de control (leyes naturales inscritas en sus cromosomas)⁸¹.

¿Cómo se trasvasa esto a la teoría del derecho? Un sistema legal autopoietico (según TEUBNER) será un sistema de comunicaciones, cerrado e indeterminado⁸². Y aplicado a las personas jurídicas en cuanto a organizaciones que obran en él, estas nacen como subsistemas cuando sus componentes se vinculan «hipercíclicamente». Podría decirse que estas personas nacen al desarrollar un ADN, cuando se autodeterminan como entes organizativos distintos de sus componentes.

Entonces cabe cuestionarse si GIERKE está rotundamente superado, pues se concibe a las personas morales como conformantes autorreferenciales de un sistema que se

⁷⁸ BERNARDO FEIJOO SÁNCHEZ, CARLOS GÓMEZ-JARA DÍEZ, CARLOS GRANADOS PÉREZ, ALEJANDRO LUZÓN, MANUEL MARCHENA Y OTROS. (2018). *La responsabilidad penal de las personas jurídicas*. Madrid: Fiscalía General del Estado.

⁷⁹ Esta doctrina se fundará en anteriores contribuciones de autores como LUHMAN.

⁸⁰ Ya que nace de una teoría de la comunicación, que a su vez parte de una explicación biológica del proceso circular de reproducción de los seres vivos. AGÜERO, J. O. (2010). Nicklas Luhmann y los sistemas autopoieticos. *VI Jornadas de Sociología de la UNLP*. La Plata: Universidad Nacional de La Plata.

⁸¹ BECK, A. (1994). Is Law an Autopoietic System? *Oxford Journal of Legal Studies*, 14(3), 401-418

⁸² La especialidad de la visión de TEUBNER proviene precisamente de que concibe al sistema legal como uno cerrado e indeterminado (Ya era concebido como un sistema de comunicaciones abierto por sus predecesores). Que sea cerrado implica que es: auto-constituyente, autorreferencial y autodescriptivo. Se constituye a sí mismo a través del actuar de los jueces, se autorreferencia porque los jueces utilizan los criterios y decisiones de otros jueces de manera recursiva, y se autodescribe porque es el discurso legal (que se da en los juicios) el que dice qué es la ley (el propio sistema, en su evolución, crea su *Rule of Reason*). Cabe pensar que esta concepción de la Ley está bastante influenciada por los sistemas anglosajones, donde existe una ley formal del precedente. BECK, A. (1994). Is Law an Autopoietic System? *Oxford Journal of Legal Studies*, 14(3), 401-418

considera a sí mismo un sujeto (la ley piensa y tiene vida propia, la Ley es la célula). Por otro lado, tampoco sería fidedigno considerar a los componentes de un ser vivo como seres en sí mismos. Lo que se presta más vecino a la realidad, podría ser considerarlos como meros órganos del mismo (cosa que hace el ordenamiento alemán).

A modo de conclusión podría decirse que clarificar la naturaleza y concepto de la persona jurídica se va prestando cada vez más necesario. Y lo hace por dos motivos principales: uno es el incremento de interconexiones casuales que caracteriza una sociedad postindustrial, donde tiende a imperar lo que SCHÜNEMAN denomina «criminalidad de la empresa». El otro es la cada vez más inminente irrupción de «personas maquínicas» e «híbridas» cuya responsabilidad y naturaleza convendría dejar delimitadas⁸³.

2.2.3.-Cuestiones sobre la teoría del delito y las personas jurídicas.

Primero debe tenerse en cuenta que la teoría del delito actual está diseñada a medida de las personas físicas; por lo que sus categorías se prestan, en ocasiones, algo difíciles de trasponer el ámbito de las morales. Sin embargo, se han ido proponiendo soluciones y maneras de contemplar los distintos elementos del delito.

En primer lugar, habría que explorar cómo se concebirá a la acción. El concepto del que se parte es el del CP: acciones y omisiones⁸⁴. Y yendo más allá, podría defenderse que, dado el marcado carácter de política criminal que caracteriza a la cuestión de la

⁸³ Primero, las sociedades tienen capacidad real de dominio sobre la vida social, la inmensa mayoría de la población pasa gran parte de su tiempo en ellas; lo cual explica por qué existe la criminalidad en la empresa. Pero la criminalidad de empresa nace de este dominio sobre la posición de sus empleados y la situación de especial peligrosidad a la que se ven sometidos en ese entorno.

Segundo, están irrumpiendo dos tipos de entes a tener en cuenta por todo el Derecho aplicable a la «persona». Los aumentos y modificaciones anatómicas cada vez son más sofisticados y llegará el momento en el que su uso deje de ser anecdótico. La persona a la que se le implanten no tendría que ver desvirtuada su concepción si estos no alteran su capacidad volitiva. Sin embargo, algunos de estas modificaciones afectan a la capacidad de discernimiento de la persona; es en este caso en el que habría que plantearse el carácter de su personalidad y su posible imputabilidad en caso de que cometieran actos delictivos. Sucede tres cuartos de lo mismo en el caso de los robots. Cuando alguno de estos dos entes comete un delito ¿es responsable quien programe al robot/modificación, lo es la persona híbrida, o tiene algo que ver la empresa fabricante? Cuanto más nítida sea la regulación de la persona penal, más fácil será responder a estas preguntas.

Vd. SCÜNEMANN, B. (1988). Cuestiones básicas de dogmáticas jurídicas-penal y de política criminal acerca de la criminalidad de la empresa. *Anuario de Derecho penal y ciencias penales*, 529-558 y ZÚNIGA RODRÍGUEZ, LAURA. KLAUS TIEDEMANN. (2009). *Bases para un modelo de imputación de responsabilidad penal a las personas jurídicas*. Pamplona: Aranzadi para obtener más información acerca de la criminalidad de empresa.

Y véase VILAR, S. B. (Octubre de 2022). Persona, algoritmización y posthumanismo, una ecuación hacia la «persona maquínica» y su responsabilidad. *Actualidad Civil, Sección Persona y Derechos*(10) para mayor profundidad sobre las personas «maquínicas» e híbridas.

⁸⁴ Esta sería una consideración simplificada, pues existen más formas que el CP usa para referirse a la acción penal, las cuales no llegan a una perfecta uniformidad.

responsabilidad penal de las personas morales, podríamos acercarnos a teorías como la funcionalista⁸⁵ para definirla.

Esto es así, porque la reforma, como ya se ha señalado, se funda en gran medida en criterios de política criminal. El motivo principal por el que se introduce esta responsabilidad es, según la exposición de motivos de la LO 5/2010, la lucha contra ciertos tipos de delitos que son predominantemente cometidos por estos entes (como la corrupción o ciertos tipos transnacionales).

Por tanto, tiene sentido que se conciba la acción bajo los mismos prismas que autores como ROXIN, SCHÜNEMANN o JAKOBS⁸⁶. Como punto de partida se puede utilizar a ROXIN⁸⁷. Quien conjuga la dogmática penal y la política criminal (disolviendo la separación de LISZT). El presupuesto del que se parte en la teoría racional-final es un finalismo⁸⁸ influenciado por la política criminal.

⁸⁵ Se trata de una corriente donde el sistema dogmático se elige en función de las necesidades o expectativas del sistema social, como su propio nombre indica, es un sistema funcional, bastante ajustado al modo en que se ha legislado sobre este asunto en España. CUESTA ARZAMENDI, JOSÉ LUIS. NORBERTO J. DE LA MATA BARRANCO. (2013). *Responsabilidad Penal de las Personas Jurídicas*. Pamplona: Aranzadi.

⁸⁶ ROXIN verá la cuestión desde la perspectiva de la escuela del funcionalismo moderado, mientras que JAKOBS lo hará desde el racionalismo radical. Sin embargo, se suele clasificar a los dos primeros autores (ROXIN y SCHÜNEMANN) dentro de las teorías racional-finales, mientras que a JAKOBS se le considera de las teorías de los sistemas. Lo cierto es que SCHÜNEMANN basa parte de sus postulados en los sistemas autopoieticos antes vistos, por lo que la escisión entre las escuelas a las que pertenezcan los autores no es tan radical.

CUESTA, J. M. (2021). *Compendio de Derecho Penal Parte General*. Madrid: Dykinson, S.L.

⁸⁷ Debemos tener en cuenta que todos estos autores son alemanes, país donde el principio *societas delinquere non potest* sigue (relativamente) vigente. El régimen alemán reconoce las sanciones a las personas jurídicas y asociaciones desde los años 20, las cuales se recogen en el actual *Verdandgeldbusse*. Lo que se hace en los delitos cometidos por sociedades es utilizar la figura del actuar en nombre del otro. Pero en general la doctrina considera que tanto personas jurídicas como asociaciones actúan a través de sus órganos, por lo que realizan ellas mismas la acción a través de estos (noción coherente con el pensamiento de GIERKE). El uso de la institución de la actuación en nombre de otro culmina con lo que se llama responsabilidad hacia abajo (el castigo de empresas y quienes actúan en su nombre propia del Derecho alemán). Por otra parte, también se utiliza en Alemania la responsabilidad hacia arriba, concretamente el 130 OwiG (*Gesetz über Ordnungswidrigkeiten*) contempla infracciones de un cierto deber de vigilancia para el titular de la empresa que se aplican de aplica en los delitos de resultado. Por lo que, aunque rija el *societas delinquere non potest*, lo hace de manera relativa, pues la OwiG establece multas asociaciones y un injusto concreto por incumplir el deber de vigilancia.

ZUÑIGA RODRÍGUEZ, LAURA. KLAUS TIEDEMANN. (2009). *Bases para un modelo de imputación de responsabilidad penal a las personas jurídicas*. Pamplona: Aranzadi.

⁸⁸ El finalismo, cuya acuñación le corresponde a WEZEL, nace a partir de los años 30. En él, la acción queda dividida en dos partes, una mental y otra fáctica. Es decir, el autor primero elige su meta, después los medios necesarios para alcanzarla, y posteriormente realiza la actividad que culminará con ella. CUESTA ARZAMENDI, JOSÉ LUIS. NORBERTO J. DE LA MATA BARRANCO. (2013). *Responsabilidad Penal de las Personas Jurídicas*. Pamplona: Aranzadi.

Si escuchamos a SCHÜNEMAN, este hablará de la «irresponsabilidad organizada»⁸⁹ de las entidades comisoras de delitos. Este autor critica la posible punibilidad de la persona física actuante en el caso de que se condene a la jurídica bajo la que lo hace.

El concepto nace de la consideración de que el poder de dominio inicial sobre la acción que ostentan los directivos empresariales muta en un «poder de intermediación». Por lo que el dominio de acción no será tal, sino una «función de coordinación»⁹⁰.

Lo que se viene a decir es que la acción está desfragmentada en los esquemas societarios. En ellos, una persona tiene el conocimiento, otra da la orden, una tercera puede delegar en un subordinado... y así hasta que se llega al autor material. La acción realmente ha sido cometida por quien controla (o deja de hacerlo) este sistema de división del trabajo, pero queda diluida dentro de este.

Cabe, por otra parte, la posibilidad de que, a resultas de un amplio sistema de distribución del trabajo, ninguna persona termine siendo responsable, que no se la pueda individualizar. Esto es lo que se conoce como «irresponsabilidad desorganizada»⁹¹.

Por otro lado, si escuchamos a JAKOBS, este definirá a la acción como «objetivación de la falta de reconocimiento de la vigencia de la norma»⁹². De esto se puede leer que la acción penal es la comunicación por parte del autor de no reconocer a la normativa penal. Lo que hace a fin de cuentas es defraudar las expectativas de esta regla. Adecuar esta teoría al campo de las interrelaciones empresariales complejas no es sencillo.

Si las normas tienen la función de comunicar cómo debe organizarse la sociedad (qué comportamientos u omisiones son reprochables y dañinas, y cuales inocuos), esta funciona gracias a la expectativa de que el resto no las violará. Traspuesto a un entramado empresarial, esto deviene en una maraña de «expectativas de expectativas».

Dentro de este sistema de expectativas corporativas, cada eslabón confía en que el siguiente cumplirá con ellas y que el anterior también lo ha hecho; por lo que no cuestionará cuan legítimas son sus acciones. Así, no hay injusto si el sujeto no se desvía de su rol dolosa o imprudentemente. Y la sociedad tiene cierto control sobre ese entramado de expectativas, pues en caso de que la comunicación entre eslabones falle y alguien desencaje, esta deberá

⁸⁹ SCHÜNEMANN, B. (2002). Responsabilidad penal en el marco de la empresa. Dificultades relativas a la individualización de la imputación. *Anuario de Derecho penal y ciencias penales.*, 9-38.

⁹⁰ SCHÜNEMANN, B. (2002). Responsabilidad penal en el marco de la empresa. Dificultades relativas a la individualización de la imputación. *Anuario de Derecho penal y ciencias penales.*, 9-38.

⁹¹ MARTÍNEZ, M. G. (1 de abril de 2021). Criminalidad corporativa en la era del compliance: una aproximación penal y criminológica a la ciberdelincuencia. *LA LEY compliance penal*(5).

⁹² SIERRA, P. G. (2012). *La responsabilidad penal de las personas jurídicas*. Granada: Editorial de la Universidad de Granada.

actuar para evitar el delito. El castigo con el que se amoneste el no cumplimiento de la expectativa no hará sino reafirmar la organización social y sus normas. Lo que se concebirá como injusto en este caso será la comunicación defectuosa, de ahí deducimos que lo que se pretende es mantener el orden social⁹³.

Lo cierto es que la acción penal española es lo suficientemente amplia como para que todas estas concepciones quepan en ella.

Si hemos afirmado que el Art. 31 bis introduce la autorresponsabilidad de la persona jurídica, y el TS matiza que se da cuando la sociedad no ha impuesto una cultura de respeto al derecho ¿qué concepto de la acción se puede deducir de aquello? Existiendo tal distancia entre acción y responsabilidad, es difícil de dilucidar. Aunque tampoco es estrictamente necesaria una definición excluyente y omnicomprensiva de la acción penal para que el Derecho positivo actúe.

Seguidamente se tiene que analizar la atribución de un hecho peligroso para los bienes jurídicos defendidos por el orden penal. La noción de tipicidad del Código español la concibe como un elemento relacionado con la antijuridicidad (Art. 4 CP), por lo que parece aplicable una teoría como la de los elementos negativos del tipo⁹⁴; así que convendría explorar cómo se aplican las causas de justificación al caso.

En concreto, para que se dé la tipicidad en la actuación de una persona jurídica tienen que cumplirse dos elementos. Primero, una acción de una o más personas físicas que funde lo que se denomina «hecho de conexión». Y, seguidamente, que este hecho sea llevado a cabo en nombre, por cuenta y en beneficio directo o indirecto de la *universitas*⁹⁵.

Como se ha indicado, la acción se diluye en una estructura societaria descentralizada, por lo que podría considerarse que ya no es dominable por el autor. Sin este hecho de conexión será difícil determinar la responsabilidad de la persona jurídica.

⁹³ Bajo esta perspectiva, lo protegido, más allá de los bienes jurídicos concretos, es el sistema jurídico en sí mismo considerado, el mantenimiento de las expectativas que este implica y que mantienen el orden social. SIERRA, P. G. (2012). *La responsabilidad penal de las personas jurídicas*. Granada: Editorial de la Universidad de Granada.

⁹⁴ Bajo esta perspectiva la constatación de la tipicidad se comprueba con la existencia o ausencia de una causa de justificación. CUESTA, J. M. (2021). *Compendio de Derecho Penal Parte General*. Madrid: Dykinson, S.L.

⁹⁵ TOMILLO, M. G. (Septiembre de 2011). Imputación objetiva y culpabilidad en el derecho penal de las personas jurídicas. Especial referencia al sistema español. *Revista jurídica de Castilla y León*(25), 43-84.

En el Derecho Positivo español, se enuncia la exigencia de esta conexión en el Art. 31 bis. Es la persona física la que realiza el hecho; siempre que sea un representante legal, administrador de hecho⁹⁶ o de derecho, los trabajadores sólo lo cometerán cuando estén sometidos a autoridad de esas personas.

Sin embargo, como se ha visto, el artículo indica que existirá responsabilidad penal de la persona jurídica aunque no se pueda individualizar al autor material del hecho. Por lo que la tarea de comprobar la existencia de causa de justificación se complica, si se considera que es en este sujeto donde debe operar. Porque ahí está la cuestión, el Art. 31 ter no precisa ni individualización, ni proceso, ni culpabilidad del autor material del hecho. Este puede estar hasta muerto y la persona jurídica seguirá habiendo cometido el delito.

Por tanto, podría concluirse que el hecho de conexión no precisa del autor material más que el injusto. Lo que sí se precisa, a mayores de que el autor material pertenezca a las categorías del Art. 31 bis, es que se el hecho se lleve a cabo en nombre o por cuenta de la persona moral, y en su beneficio⁹⁷.

Por lo que respecta a las causas de justificación, nada dice el CP sobre cómo actúan las que puedan darse en el autor material en relación con la persona jurídica. Sin embargo, bien se ha dicho que el hecho de conexión exige el injusto del autor material, por lo que puede deducirse que en ausencia de este (por estar presente una causa de justificación) no habrá hecho de conexión y por ende la persona jurídica no será responsable⁹⁸.

Cosa distinta sucede en el ámbito de la culpabilidad, el propio Código indica que la del autor material no es necesaria para imputar a la persona jurídica. Lo cual es coherente con el uso del hecho de conexión. Así pues, la persona moral será culpable por el hecho

⁹⁶ Siendo el administrador de hecho una figura acuñada por el Tribunal Supremo federal alemán, el cual la concibe como quien «mediante un abuso de poder económico y de una posibilidad de configuración establecida jurídicamente se sirvió de un testaferro como miembro del Consejo de Administración (y), como verdadero administrador de la sociedad, ocasionó las infracciones de la Ley». SCHÜNEMANN, B. (2002). Responsabilidad penal en el marco de la empresa. Dificultades relativas a la individualización de la imputación. *Anuario de Derecho penal y ciencias penales.*, 9-38.

⁹⁷ En este caso tendría sentido retornar a la STS 154/2016, anteriormente se ha explicado cómo esta fundamentaba la responsabilidad de la persona moral cuando existe ausencia de cultura de respeto al Derecho. De tal fallo pudiere entenderse que la tipicidad subjetiva deriva de la falta de un modelo adecuado de previsión de riesgos, y en que el control para evitar la comisión de los delitos fue defectuoso.

⁹⁸ Esta interpretación queda acreditada por el hecho de que sí existe en el Art. 31 actual una referencia a que no se transmita la culpabilidad del autor material a la persona jurídica. Pero no existe referencia alguna a que no se trasvasen aspectos relativos a la tipicidad-antijuridicidad del hecho, y en concreto, de las causas de justificación. De hecho, en el Proyecto de Ley de 2007 esta prohibición de transmisibilidad afectaba a todas las circunstancias relativas al autor material, y se acotaron estas a las relativas a la culpabilidad. SIERRA, P. G. (2012). *La responsabilidad penal de las personas jurídicas*. Granada: Editorial de la Universidad de Granada. Pág 342.

propio. Y habrá que determinar qué definición de la culpabilidad es capaz de representar la capacidad volitiva de una persona jurídica.

Autores como FEIJOO o PÉREZ ARIAS⁹⁹ defienden que la persona moral carece de capacidad de culpabilidad. Otros, como MIR PUIG y GIMBERNAT, entienden que sería mejor sustituirla por «atribuibilidad» o «responsabilidad». Por otra parte, quienes siguen las teorías de los sistemas autopoieticos defenderán que el clásico libre albedrío que se da en las personas físicas, se presenta (salvando las distancias) en las jurídicas como «la libertad para autoorganizarse»¹⁰⁰.

La segunda posición parece la más coherente con nuestro ordenamiento. En primer lugar, porque este sigue un sistema de autorresponsabilidad sin tapujos. Seguidamente, porque estas posiciones contravienen el derecho de defensa de la persona jurídica. Y esto es así porque esta se vería obligada a defender la inocencia de la persona física en la que se encauza su responsabilidad. Además, el derecho a la presunción de inocencia de la persona jurídica también se vería condicionado por la situación del presunto autor material.

De entre los defensores de esta concepción destaca MAZA MARTÍN. Este autor reconoce que, al igual que ocurre con las personas físicas, no todas las jurídicas tendrán capacidad de ser culpables. Por eso mismo introduce el elemento del «actor corporativo», sólo este tiene la capacidad de autorreflexión suficiente como para ser considerado penalmente responsable. Por eso se dice que «sólo el actor corporativo podrá cometer un delito corporativo»¹⁰¹.

Para explicar qué es exactamente este actor es preciso que retornar a TEUBNER. Quien lo concibe un sistema comunicativo *sui generis*. Y ello porque tiene la capacidad de elaborar una comunicación reflexiva acerca de su propia existencia y capacidad de acción. Es una realidad diferente de la organización a la que pertenece, ya que en esencia es un aparato semántico de la misma que puede encauzarse en acciones reales. Por lo que aquellas corporaciones que carezcan de la suficiente complejidad no lo tendrán; pues sólo cuando

⁹⁹ Este último defiende que la persona jurídica es ficticia, y su culpabilidad también lo es. La culpabilidad de un ente ficticio sería meramente formal, propia de una persona con capacidad de infracción, pero carente de «elemento volitivo en sentido estricto» como así lo afirma la STC 246/1991. PÉREZ ARIAS, J. (2014). *Sistema de atribución de responsabilidad penal a las personas jurídicas*. Madrid: Dykinson.

¹⁰⁰ BERNARDO FEIJOO SÁNCHEZ, CARLOS GÓMEZ-JARA DÍEZ, CARLOS GRANADOS PÉREZ, ALEJANDRO LUZÓN, MANUEL MARCHENA Y OTROS. (2018). *La responsabilidad penal de las personas jurídicas*. Madrid: Fiscalía General del Estado.

¹⁰¹ BERNARDO FEIJOO SÁNCHEZ, CARLOS GÓMEZ-JARA DÍEZ, CARLOS GRANADOS PÉREZ, ALEJANDRO LUZÓN, MANUEL MARCHENA Y OTROS. (2018). *La responsabilidad penal de las personas jurídicas*. Madrid: Fiscalía General del Estado.

esta existe es preciso recurrir a un sistema que ordene las interrelaciones recursivas que se dan entre los miembros del ente.

Para simplificar este concepto podría decirse que una persona jurídica cuenta con un actor corporativo cuando «adquiere un cerebro», es decir, cuando desarrolla consciencia de sí misma. Con ella puede desarrollar una semántica propia con la que ordenarse a sí misma y a sus componentes de manera consciente. Adquiere no sólo voluntad sino capacidad de manifestarla; es decir, adquiere una cultura. Su consciencia se materializa en esta capacidad autodescriptiva, que guía el obrar de sus miembros.

Este aparato semántico se utiliza como punto de referencia para imputarle las acciones de sus miembros a las personas jurídicas. Esto se hace a través de lo que TEUBNER llama «conjunción cíclica» entre la acción y la persona jurídica. (una conjunción entre la identidad autorreferencial y los elementos del sistema)¹⁰². Por desgracia, este autor no trató el tema de la responsabilidad corporativa en base a este elemento; pero la doctrina ha hecho el esfuerzo de habilitarlo, como así lo demuestra la STS de 29 de febrero de 2016. En ella, se entiende que las sociedades pantalla son inimputables por no ser más que una ficción carente de cultura propia e independiente.

Parece pues que en este campo se está consolidando el uso de las teorías de los sistemas para fundamentar la autorresponsabilidad. Sin embargo, existen autores que critican el uso de este modelo y otros que proponen soluciones alternativas.

En primer lugar, autores como PETTIT y LIST plantean una alternativa a la teoría de los sistemas. Estos critican a LUHMANN por las asunciones metafísicas y ontológicas del concepto de sistema (las cuales provienen de su origen biológico). En su teoría utilizan también los sistemas, pero de manera diferente. Estos serán sistemas de creencias que actuarán en pos de satisfacer las motivaciones que sus individuos racionalmente esperan. Aquí las corporaciones agrupan a individuos que pretenden garantizar esas esperanzas, y desviarse de los comportamientos que se interpongan en esa motivación, de manera racional. Una corporación se distinguirá entonces de una conjunción de individuos en cuanto sus miembros sean un agente único que encauce una única acción (no una suma de ellas).

Este sistema se asemeja a las «expectativas de expectativas» de JAKOBS, pues concibe a la corporación como la agrupación de voluntades en una sola para conseguir un

¹⁰² GÜNTHER, K. (2015). "Nulla poena sine culpa" and corporate personhood. *Nomos*, 360-376.

objetivo, y que no se desmenuza gracias a la confianza de los miembros entre ellos y para con el sistema¹⁰³.

Por otra parte, hay quienes critican las concepciones de LUHMANN y TEUBNER por considerarlas poco fieles a la realidad¹⁰⁴. Sin embargo, a si analizamos la manera en que se utilizan estos postulados, no parece que pretendan adecuarse a una suerte de realidad empírica de las organizaciones, sino que observan su realidad jurídica.

En definitiva, las maneras de concebir y encauzar esta responsabilidad están en proceso de consolidarse. La teoría de los sistemas parece predominar, y ya desde el 2015 impera la autorresponsabilidad como única forma de imputación a la persona jurídica. Varias de las concepciones expuestas serían aplicables al asunto, pero la de TEUBNER se ha prestado especialmente acomodable a nuestro sistema; por lo que quizás convendría perfeccionarla, más que deponerla.

2.2.4.-Conclusión

La regulación de la responsabilidad penal de las personas jurídicas en el Código Penal español sugiere un sistema de autorresponsabilidad, el cual se presta como la manera de introducir esta responsabilidad más acorde con el carácter del Derecho Penal.

Con respecto a la naturaleza de la persona penalmente responsable cabe decir que esta no ha sido especialmente delimitada ni por doctrina ni por legislador, pero ha sido algo acotada por la doctrina y la jurisprudencia del TS. A este respecto cabe destacar que la concepción tanto del sistema legal como de las personas que lo componen imperante es la de un sistema autopoietico cerrado e indeterminado.

Orientar la imputación de una persona jurídica en base a estos postulados no es una tarea sencilla, pero la STS 154/2016 terminó por llevarla a cabo. Así pues, la acción penal será propia de la persona jurídica por irresponsabilidad organizada (o desorganizada en caso de las ilícitas) al carecer de cultura de respeto al derecho. La tipicidad y antijuridicidad se encauzarán a través del hecho de conexión con el autor material. Y la culpabilidad se dará sólo *universitas* con actor corporativo, es decir, capaces de desarrollar una cultura autónoma.

¹⁰³ GÜNTHER, K. (2015). "Nulla poena sine culpa" and corporate personhood. *Nomos*, 360-376.

¹⁰⁴ SIERRA, P. G. (2012). *La responsabilidad penal de las personas jurídicas*. Granada: Editorial de la Universidad de Granada.

3.-RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS EN EL CIBERESPACIO: EL ACCESO ILÍCITO

El ciberespacio suele comprenderse como una reproducción desmaterializada de nuestra vida analógica. Y como tal, en ella existen peligros y amenazas tan susceptibles de lesionar los bienes jurídicos tutelados por el ordenamiento como las físicas. Por ello será necesario, y más aun considerando los avances que se van a ir dando, tratar de acotar la responsabilidad de quienes programan y mantienen los soportes físicos e inmateriales donde se desarrolla esta segunda vida: las sociedades del ámbito tecnológico.

Si se pretende acudir a la utilización en la práctica de los tipos que atribuyen responsabilidad a los entes, las sentencias condenatorias brillan por su escasez. Y sin medios para comprobar cómo se desenvuelven los tipos del 197 bis, 197 quinquies y 31 bis y ss. Es complicado analizar su incidencia y posible evolución en un futuro próximo.

Cuando uno acude al portal de estadística de cibercriminalidad del ministerio del interior, este no cuenta con la posibilidad de escindir los tipos en función del tipo de personalidad del autor. Cuestión que se debe al escaso recurso en la práctica de la herramienta de la RPPJ. Por tales motivos, es difícil concretar el uso práctico del artículo 197 quinquies, el cual recoge la responsabilidad penal de las personas jurídicas por el acceso ilícito.

Sin embargo, puede verse que los delitos de acceso ilícito son bastante comunes, habiéndose dado 2.637 hechos conocidos de infracciones por este tipo en 2021. Se trata de un tipo relativamente habitual, aunque no tanto como la estafa (en sus diferentes vertientes) o las amenazas. Por tanto, no resultaría extraño pensar que la posibilidad de que se den comisiones no conocidas o denunciadas de estos hechos cometidos a través de personas jurídicas.

Pese a todo lo anterior, los artículos que castigan estas conductas existen, y la posibilidad de su uso debe ser explorada; bien a través del análisis de las fuentes, los pocos casos prácticos donde se aprecia la posible comisión del delito y el derecho comparado.

3.1.-RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS EN EL MUNDO CIBERNÉTICO

La responsabilidad penal de las personas jurídicas en este ámbito se encauzará a través de los artículos concretos que delimiten un delito informático en sentido estricto y las disposiciones del 31 y bis y ss. Esto no suscita mayor complicación, pero sí lo hace el hecho de que esta responsabilidad pueda quedar atenuada o reducida si se cuenta con los adecuados programas de compliance que promuevan en ella una arraigada cultura de respeto al Derecho. Tales se verán influenciados por la presencia de elementos informáticos, y deberán estar adaptados a la presencia y riesgos particulares de la custodia de datos de clientes y trabajadores en sistemas informáticos.

3.1.1.-Personas jurídicas acceso ilícito

Para que un delito informático pueda ser cometido por una persona jurídica, basta con que exista un artículo que así lo estipule expresamente. En el caso del acceso ilícito se trata del 197 quinquies, cuya introducción vino determinada por la directiva 2013/40/UE.

Esta directiva, relativa a los ataques contra los sistemas de información define a las personas jurídicas como «toda entidad a la cual el derecho vigente reconoce este estatuto, salvo los Estados y otros organismos públicos que ejercen prerrogativas públicas y las organizaciones internacionales de carácter público». Por lo que, como se ha visto antes, esta noción no choca con la recogida 31bis CP.

Además, esta trata, en sus artículos 10 y 11, la RPPJ. El primero indica que los Estados deberán penar las conductas de acceso e interferencia a los sistemas de información (entra otras) cometidos por personas jurídicas. Bien a través de sus directivos, por falta de supervisión o control, y de manera independiente al autor material. El siguiente artículo habla de las penas a imponérseles a estas personas jurídicas responsables.

Para cumplir con esta necesidad de armonización (y la derivada de la Decisión Marco 1005/222/JAI), fue introducido el artículo 197 quinquies. Este imputa pena de seis meses a dos años a las personas jurídicas responsables (en virtud del Art. 31 bis) por los delitos de los artículos 197, 197 bis y 197 ter.

Como también se ha indicado antes, la existencia de este artículo es necesaria, pues no se le podría imputar responsabilidad penal a una persona jurídica por una conducta que no ha sido calificada como susceptible de hacerlo.

Además, el artículo referencia al 66 bis, en la medida en que podrán ser aplicadas las penas de b) a g) del artículo 33.7. Es decir, penas de: disolución, suspensión de actividades, clausura de locales y establecimientos, prohibición de ejercer actividades relacionadas con el tipo, inhabilitación para obtener subvenciones y ayudas e intervención judicial para proteger a acreedores y trabajadores. Precisamente por la gravedad de muchas de estas penas fue criticada la introducción de este artículo en la reforma de 2015¹⁰⁵.

Las entidades pueden manejar los datos de sus empleados/clientes/administrados dentro del marco legal (atendiendo a las disposiciones sobre protección de datos). La cuestión del acceso ilícito se plantea de manera clara cuando un tercero accede a esos datos, y cabría preguntarse cuál sería la responsabilidad de las entidades cuando uno de sus trabajadores accede a tales informaciones.

El tipo del 197 bis exige, para la conducta delictiva, que se manipule la seguridad del sistema informático en cuestión. Entonces, cabe cuestionarse en qué situaciones podrá ser responsable una empresa por la conducta de las figuras que contempla el 31 bis. Estos atribuyen a la entidad los hechos cometidos por representantes, directivos con poder de control y quienes estén sometidos a su autoridad; siempre y cuando actúen en beneficio de la sociedad. A esto habrá que añadirle la ausencia de una cultura de respeto al derecho en la sociedad.

Por ende, para analizar cuándo un ente puede cometer esta clase de delitos, habrá que atenerse al lenguaje interno de la empresa, a su cultura, a sus programas y comportamientos para evitar que tanto trabajadores como terceros puedan cometer estas infracciones.

Es en este momento en el que cobran mayor protagonismo los programas de compliance. Y en relación con la protección del derecho a la privacidad, lo hacen mecanismos concretos de protección: como el establecimiento de canales de denuncias internos o los medios de control en el acceso por parte de los empleados.

¹⁰⁵ COLLANTES, T. G. (enero de 2015). Los delitos contra la intimidad tras la reforma de 2015: luces y sombras. *Revista de Derecho penal y criminología*, 3(13), 51-84.

Será imprescindible que existan normas internas que controlen quienes y de qué forma pueden acceder a determinados datos.

3.1.2.-Compliance y protección de los sistemas informáticos

Habrá que considerar qué cultura del Derecho debe tener una sociedad para protegerse de los ataques a sus sistemas informáticos donde se almacenen datos personales. Y para evitar que quienes, por su pertenencia a la empresa puedan violar con mayor facilidad las barreras de seguridad de sistemas informáticos, lo hagan.

Sin embargo, es importante diferenciar el derecho a la protección de datos del de privacidad e intimidad. Los dos últimos solo se distinguen por su alcance, pero el primero, a pesar de contar con la misma raíz, tiene un contenido y expresiones distintos¹⁰⁶. Cabe destacar, además, que existen bastantes códigos de buena conducta y protocolos preestablecidos en relación con el derecho a la protección de datos; pero es no tan sencillo encontrar reglas acerca de la protección de la privacidad en relación con el acceso ilícito¹⁰⁷.

Si nos atenemos a la evolución de los sistemas de compliance desde la introducción en 2010 de la RPPJ, se han ido creando cada vez más y más normas técnicas a las que estos entes pudieren atenerse. De entre ellas destaca la Certificación UNE 19601: 2017 de Sistemas de gestión de compliance penal, la Certificación ISO 37001 de Sistemas de gestión de compliance y la Directiva de protección al denunciante. Por otra parte, la irrupción de la RPPJ ha generado reformas legislativas interesantes en diversos campos, como el administrativo¹⁰⁸ o el bancario¹⁰⁹; pero ninguna específicamente referida a la protección de la privacidad en el ámbito penal (al margen del CP)¹¹⁰.

Por otra parte, existen formas de compliance comunes que pueden ser aplicables al caso de la protección de la privacidad (o, si se acepta tal tesis, de la inviolabilidad informática) de clientes y trabajadores. Entre ellas destaca la posibilidad de establecer canales de denuncia anónimos, programas de seguridad, mapas de riesgos, contraseñas, dificultades de acceso a determinados sistemas en función del rango, contar con software y firewall de protección al

¹⁰⁶ STC 282/2000, de 30 de noviembre

¹⁰⁷ Existen elementos de compliance como la figura del delegado de protección de datos, o la propia Ley especial dedicada a la protección de datos. CASTRO, E. V. (2022). La doble faceta de la protección de datos personales en los sistemas de compliance. (A. SAU, Ed.) *Revista Aranzadi de Derecho y nuevas tecnologías*(59).

¹⁰⁸ Art. 71 de la Ley de Contratos del Sector público.

¹⁰⁹ RDL 11/2018 de transposición de directivas en materia de prevención de blanqueo de capitales y financiación de terrorismo.

¹¹⁰ MIRÓ, A. N. (2022). Evolución en el diseño de Sistemas de Compliance. *La ley, compliance penal*(9).

hackeo o copia por parte de empleados y/o terceros... Pero sobre todo destaca la figura del *compliance officer* u órgano específico de cumplimiento.

El estatuto de estos órganos no se encuentra nítidamente definido, lo cual pone en tela de juicio su independencia, ya que se encuentra en una posición intermedia entre la alta dirección y el resto de los trabajadores¹¹¹.

Anteriormente se ha comprendido como condición de exención de la responsabilidad penal de los entes (entre otras) a la existencia de una cultura de respeto al Derecho. Tal se concibe como un lenguaje o ADN particular de la sociedad en virtud de la teoría de los sistemas autopoieticos. Por tanto, este órgano, que se diseña como mecanismo de prevención penal (y también como una forma de adecuar la estructura empresarial a las exigencias de mercados donde la cultura del compliance está más arraigada), debe ser particular a la entidad en cuestión.

Existe debate acerca de la posibilidad de exportar o copiar los modelos de compliance de otras personas jurídicas. Y tal se resuelve indicando que no se deberían copiar los sistemas de compliance de otras entidades, aunque sea una práctica común para abaratar costes. Lo que sí puede hacerse es externalizar las actividades de la función de compliance siempre y cuando el encargado de realizarlas sea un profesional de reconocido prestigio y con amplia experiencia¹¹².

Las exenciones de responsabilidad a causa de un eficaz mecanismo de compliance se regulan en el Art. 31 bis, en sus párrafo segundo y cuarto. Tales se pueden clasificar, para una comprensión más transparente, entre las aplicables a delitos cometidos por directivos contra las cometidas por empleados.

Si el delito ha sido cometido por uno de los sujetos del 31 bis 1 a), es decir, directivos con poder de control; existen cuatro conductas eximentes: la adopción y ejecución de modelos de organización con medidas de vigilancia y control idóneas, la supervisión del cumplimiento del modelo de prevención implantado por parte del compliance officer (u órgano equivalente), que los autores individuales evadan fraudulentamente dichos modelos de prevención y que no se haya dado ninguna omisión o ejercicio insuficiente de la supervisión y vigilancia.

¹¹¹ MARTÍNEZ, M. D. (2021). El órgano de cumplimiento o compliance officer: figura clave en la organización empresarial. *REvista de DErecho Bancario y Bursátil*(164).

¹¹² MARTÍNEZ, M. D. (2021). El órgano de cumplimiento o compliance officer: figura clave en la organización empresarial. *REvista de DErecho Bancario y Bursátil*(164).

Si el delito ha sido cometido por un subordinado a la autoridad de tales directivos, la persona jurídica quedará exenta sólo si antes de la comisión del delito tuviera un sistema de prevención adecuado y este fuere ejecutado con eficacia.

Para que un programa corporativo de compliance y la actuación de su órgano puedan ser utilizados como eximentes de responsabilidad, no solo es necesario que estén planteados debidamente a las necesidades y riesgos particulares de la sociedad, sino que deben tener cierto arraigo. El alcance de la oponibilidad de estos frente a una denuncia depende del alcance de la extensión de su cumplimiento. Por ello es importante un órgano de refuerzo como el compliance officer. Porque, como indica el Art. 31 bis 2, estas eximentes podrán ser moduladas como atenuantes si no se acreditan totalmente.

También cabría cuestionarse cuál es, en sentido estricto, el concepto de acceso ilícito, más aún en lo que respecta a la responsabilidad de las personas jurídicas. Normalmente se piensa en un hackeo, pero en una empresa puede darse el caso de un acceso a un sistema por parte de un trabajador que no debiera conocer su contenido. En este caso, la sociedad debería contar con mecanismos que prevengan tales situaciones.

Por otra parte, el uso o difusión por parte de un trabajador de datos a los que sí tiene acceso por razón de su profesión no sería un allanamiento ilegal. Por eso, a la hora de contemplar si el mapa de riesgos elaborado por la entidad cuenta con medidas de protección para ambos casos.

Por último, cabe destacar que la proporción de las medidas que se deberían tomar y la posibilidad de imputar a una persona jurídica en base a ellas depende, tanto del tamaño de la empresa, como de la gravedad que supondría el acceso a sus datos. Es importante que el Derecho penal se plantee la lesividad que causaría el hackeo de datos custodiados por entidades bancarias, sistemas de salud, o registros mercantiles.

El acceso por parte de una empresa a los datos de contabilidad presentados por sus competidores en tiempo real, por ejemplo, podría suponerles millones de euros de pérdidas. Por eso es importante que las entidades que custodian esta clase de datos cuenten con sistemas de seguridad reforzados. De ahí que registros públicos como el mercantil cuenten con sofisticados softwares de almacenaje, donde se realizan copias y depuraciones periódicas, y donde se ha elaborado una encriptación adecuada de aquellos datos que sean sensibles.

Sin embargo, plantear la posibilidad de penar a un ente por no contar con las barreras de seguridad suficientes no es lo que viene a recoger el Art. 197 bis. Este artículo condena el ataque a estos sistemas informáticos, no el hecho de recibirlos; por muchos bienes jurídicos individuales que se vean afectados. Los únicos que podrían cometer el delito del 197 quinquies son los propios participantes de la empresa, y ese no suele ser el caso habitual.

Si se quisiera disuadir a los grandes entes para que custodien sus datos con mayor entereza sería preciso crear un tipo a mayores, o, mejor, utilizar medios que no impliquen el ejercicio del *ius puniendi*.

Un caso de actuación pública para fomentar la protección frente a estos ataques sería el de la Autoridad Catalana de la Competencia, que ha instado la concesión de subvenciones para la implantación de programas de compliance¹¹³. Convendría plantear medidas similares para el ámbito de la protección de la privacidad, o incluso de la difusa ciberseguridad (que sí podrá protegerse sin complejos a través de este tipo de políticas).

3.1.4.-El blockchain, la inteligencia artificial y otras dificultades

Los avances tecnológicos se dan de manera vertiginosa en nuestros tiempos, y a los ordenamientos jurídicos cada vez les cuesta más seguir el ritmo de dichos avances. Por eso es interesante tocar alguno de los temas que pueden causar mayores quebraderos de cabeza en un futuro próximo, aunque no estén íntimamente relacionados con el delito del acceso ilícito.

Las empresas de gran tamaño o incluso entes públicos gestionan una cantidad masiva de datos, algunos de ellos, parte de la esfera reservada de sus usuarios. En este tipo de custodia existen dos cuestiones interesantes a tratar: primero, que los mecanismos que estas utilizan pueden suponer un peligro en sí mismos. Y segundo, que la mayoría de grandes empresas tecnológicas son hackeadas comúnmente y ni siquiera informan a sus usuarios al respecto.

En primer lugar, la gestión de cantidades ingentes de datos siempre conlleva el uso de sistemas de big data, los cuales utilizan algoritmos para clasificarlos y encriptarlos de forma adecuada. Tales mecanismos necesitan ser programados a través de algoritmos muy sofisticados, los cuales pueden perpetuar los sesgos que en ellos hayan introducido sus creadores.

¹¹³ MIRÓ, A. N. (2022). Evolución en el diseño de Sistemas de Compliance. *La ley, compliance penal*.(9).

En lo que respecta a la protección de la privacidad a través del compliance, los métodos que se utilicen para salvaguardar los sistemas donde se almacenan estos datos serán la clave. Será importante que el compliance officer cuente con la posibilidad de un hackeo o intromisión física en ellos, y deberá reforzar tanto las buenas prácticas en el tratamiento de estos datos, como comprobar que las encriptaciones que los guardan son proporcionales al tamaño de la empresa y la sensibilidad de los datos. Una seguridad excesivamente laxa a la hora de proteger estos sistemas, junto con nulas indicaciones de no allanarla, incrementan el nivel de peligro sobre la privacidad de los usuarios.

Otro riesgo a tener en cuenta en este respecto es el uso de inteligencias artificiales a la hora de cotejar y administrar datos. Tales instrumentos pueden ser bastante útiles, pero dependiendo de la forma en que sean programados pueden constituir un riesgo.

Un ejemplo de dichos riesgos sería la discriminación sistemática a la que podría llegar, por ejemplo, una inteligencia artificial diseñada para elegir al mejor candidato de los que pugnan por un puesto en la sociedad. Es bastante común que las IAs cuenten con sesgos en función del sexo, raza, religión, nacionalidad y viceversa. Por eso será importante que los programas de compliance elaborados en empresas que vayan a hacer uso de estas, cuenten con medidas para comprobar si tales sesgos existen, para después erradicarlos.

Las inteligencias artificiales entrañan un riesgo penal aun mayor en los casos de aquellas que pueden ser utilizadas para fabricar o modificar imágenes y videos. Pues estas pueden utilizarse para crear fotografías difamatorias o pornográficas de personas que no han dado su consentimiento para aquello. O incluso han llegado a ser utilizadas para generar pornografía infantil utilizando el rostro e imagen de personas que habían subido fotografías de sí mismos en la infancia o sus hijos a la red.

Existen dificultades añadidas a la hora de determinar la responsabilidad en ciertos tipos de agrupaciones que, aun careciendo de responsabilidad jurídica, operan en el ciberespacio como figuras de hecho. Se trata de aquellos activos, conjuntos de ellos o almacenajes de datos creados a través del blockchain. Estos generan problemas a la hora de ejecutar sentencias que requieren la eliminación de datos cuya custodia y difusión en sí misma se considera ilícita (como la pornografía infantil).

Los ataques que se realizan a través de estos medios bien pueden afectar a la intimidad y honor de las víctimas. Pero en lo referido a este trabajo, es más interesante explorar si existe

alguna responsabilidad por parte de los fabricantes o providers en estos casos. Quizás serían convenientes medidas que protejan la ciberseguridad en este caso, no penales al no ser posible tal construcción, pero sí desde otros ámbitos.

Debería explorarse la exigencia a estos proveedores un mínimo de seguridad en los productos que distribuyen al público general, y es posible otorgarla, simplemente supondría una mayor inversión. Sería necesario mejorar sus algoritmos para que identifiquen cuando se está tratando de crear un video o imagen de una persona física, y se debería contar con personas humanas que controlen aquellas creaciones donde salte la alarma de actividad delictiva.

Por otra parte, también cabría solicitar mayores medidas de seguridad a los proveedores que controlan las redes, como la imposibilidad de capturar o descargar el contenido personal de quienes las utilizan; y mayor transparencia y seguridad en los casos de hackeo masivo.

3.1.5.-Conclusión

La introducción del 197 quinquies fue criticada por gran parte de la doctrina, entre otras cosas, por la especial gravedad de las penas que entrañaba. Este artículo, de poca vigencia práctica, es una respuesta a las exigencias del DUE, que requerían que existiera un tipo que castigara el acceso ilícito cometido por personas jurídicas.

Sin embargo, en la práctica no se han elaborado reformas legislativas ni leyes especiales al respecto de la protección de la privacidad de ataques cometidos por allanamiento informático en el seno de una persona jurídica. Y los códigos de soft law españoles e internacionales dan mayor relevancia a temas como la protección de datos, frente a sobornos o blanqueos de capital. Sin embargo, los sistemas y métodos que se utilizan para proteger a la sociedad de este tipo de responsabilidad por tales delitos, también son transponibles y adaptables a la prevención del allanamiento. Y aunque sea un delito de menor vigencia práctica en las sociedades que otros ciberdelitos, este deberá ser tenido en cuenta por los compliance officers en la elaboración de los mapas de riesgos de cada entidad.

A mayores, los riesgos de los avances de las nuevas tecnologías pueden incitar a que se quieran proteger bienes supraindividuales como la ciberseguridad desde el ámbito penal. Pero existen otras formas de promover las buenas conductas que eviten dichos riesgos. El Derecho Penal no puede absorberlo todo ni salirse de castigar aquellas acciones que más

pongan en peligro o dañen bienes jurídicos individuales previamente considerados de interés por el ordenamiento jurídico.

4.-CONCLUSIONES

Los delitos informáticos no existen como categoría sistemática diferenciada y autónoma dentro del CP, y no lo hacen porque no tutelan nuevos bienes jurídicos. Sin embargo, existe parte de la doctrina que considera que su existencia vela por intereses jurídicos supraindividuales como la ciberseguridad. En el caso concreto del acceso ilícito informático hay quienes cuestionan la decisión del legislador de considerarlo un tipo protector de la privacidad, y apuntan a una defensa de la intimidad o incluso de una especie de inviolabilidad informática. Sin embargo, el Derecho positivo concibe el intrusismo informático como un delito de peligro abstracto; cuya conducta comprende la entrada o mantenimiento en un sistema informático ajeno, siempre que se haga sorteando los sistemas de seguridad con que cuente. Y todo ello con independencia de la sensibilidad de los datos que este contenga (es este último matiz el que apunta a que se defiende la inviolabilidad informática más que la privacidad).

La responsabilidad penal de las personas jurídicas está cobrando una forma bien definida en nuestro ordenamiento. La opción del legislador por un sistema de autorresponsabilidad es la más coherente con los principios del derecho penal que rigen en nuestro ordenamiento jurídico, y es la adecuada si se pretende introducir este tipo de responsabilidad. Por otra parte, convendría explorar en mayor medida la naturaleza de las personas jurídicas penalmente imputables en nuestro sistema, ya que la vigencia de entidades de hecho (como las que operan a través de blockchain) o personas híbridas o maquínicas crearán dificultades para la imputación de estas en un futuro.

De otro lado, la interpretación de las personas jurídicas como subsistemas autopoiéticos en la que se fundan las resoluciones del TS. Si bien no es sociológicamente correcta, es útil a la hora de justificar *la cultura de respeto al Derecho* como criterio para decidir sobre los atenuantes y eximentes aplicables a la persona jurídica comisora de un delito. De tal posición, junto con la regulación de los arts. 31 bis y ss. ha nacido cierta cultura nacional del uso del compliance para evitar ser penado a través de este cauce.

Cabe anotar que los mecanismos de control y supervisión que se han creado hasta ahora prestan más atención a la protección de datos, a evitar los sobornos o blanqueo de capitales. Las referencias a la protección de la privacidad a través de medidas de control al acceso lícito son menores, pero deben estar vigentes en cuanto el Art. 197 quinquies introduce la RPPJ a raíz de esta conducta.

5.-BIBLIOGRAFÍA

- AGÜERO, J. O. (2010). Nicklas Luhmann y los sistemas autopoieticos. *VI Jornadas de Sociología de la UNLP*. La Plata: Universidad Nacional de La Plata.
- AGUILERA, A. T. (Mayo-Junio de 2015). *Laleydigital*. Obtenido de El libro primero del Código Penal tras la Ley Orgánica 1/2015.
- ALMIRÓN, F. J. (2017). La responsabilidad penal de las personas jurídicas a raíz de la jurisprudencia reciente del Tribunal Supremo. *Revista Aranzadi Doctrinal*.
- ALSCHULER, A. (2009). *Two ways to Think about the Punishment of Corporations*. Recuperado el 29 de Noviembre de 2022, de Northwestern Pritzker School of Law Scholarly Commons:
<https://scholarlycommons.law.northwestern.edu/facultyworkingpapers/192>
- ARANZADI. (12 de Enero de 2023). Obtenido de PENAL: Responsabilidad penal de las personas jurídicas.
- BACIGALUPO SAGGESE, S. (1998). Los fundamentos clásicos de la máxima societas delinquere non potest. En B. SILVINA, *La responsabilidad penal de las personas jurídicas* (págs. 19-95). Madrid: Bosch.
- BALLESTEROS, M. C. (2019). Cuestiones controvertidas sobre la responsabilidad de las personas jurídicas en el proceso penal y la eficacia de los programas de cumplimiento. *Foro, nueva época*, 233-246.
- BECK, A. (1994). Is Law an Autopoietic System? *Oxford Journal of Legal Studies* , 14(3), 401-418.
- BERNARDO FEIJOO SÁNCHEZ, CARLOS GÓMEZ-JARA DÍEZ, CARLOS GRANADOS PÉREZ, ALEJANDRO LUZÓN , MANUEL MARCHENA Y OTROS . (2018). *La responsabilidad penal de las personas jurídicas*. Madrid: Fiscalía General del Estado.
- CABEZAS, D. J. (2013). El hecho de conexión del art. 31 bis 1 CP. En V. D. LEAL, *El derecho y sus razones: aportaciones de jóvenes investigadores* (págs. 169-177). León: bubok editorial.
- CASTAÑO, E. N. (Mayo de 2022). La relevancia penal de las nuevas tecnologías y su incidencia en los denominados ciberdelitos: especial referencia a los delitos contra la intimidad. *Revista Genera de Derecho Penal*(37).
- CASTRO, E. V. (2022). La doble faceta de la protección de datos personales en los sistemas de compliance. (A. SAU, Ed.) *Revista Aranzadi de Derecho y nuevas tecnologías*(59).

- COLLANTES, T. G. (enero de 2015). Los delitos contra la intimidad tras la reforma de 2015: luces y sombras. *Revista de Derecho penal y criminología*, 3(13), 51-84.
- CONCA, L. G. (2021). Antecedentes históricos de la responsabilidad penal de las personas jurídicas. *Revista ratio iuris*, 16(32), 93-116.
- CUESTA ARZAMENDI, JOSÉ LUIS. NORBERTO J. DE LA MATA BARRANCO. (2013). *Responsabilidad Penal de las Personas Jurídicas*. Pamplona: Aranzadi.
- CUESTA, J. M. (2021). *Compendio de Derecho Penal Parte General*. Madrid: Dykinson, S.L.
- DÍEZ HERRERA, C. ARIZAGA, B. (2014). Bartolo da Sassoferrato: introduzione a un giurista globale. En M. Ascheri, *Mundos medievales: espacios, sociedades y poder: homenaje al profesor José Ángel García de Cortázar y Ruiz de Aguirre* (págs. 1029-1041). Roma: Università di Roma 3.
- ELOY VELASCO NÚÑEZ, CAROLINA SANCHIS CRESPO. (2019). *Delincuencia informática tipos delictivos e investigación con jurisprudencia tras la reforma procesal y penal de 2015*. Valencia: Tirant lo Blanch.
- GARCÍA, M. P. (1999). *El código de Hammurabi*. Recuperado el 29 de Noviembre de 2022, de Clío: History and History Teaching: <http://clio.rediris.es/fichas/hammurabi.htm>
- GROSSI, P. (2007). *Europa y el Derecho*. Barcelona: Critica, S.L.
- GÜNTHER, K. (2015). "Nulla poena sine culpa" and corporate personhood. *Nomos*, 360-376.
- iberley*. (2 de Julio de 2016). Recuperado el 22 de Marzo de 2023, de Concepto y regulación de las personas jurídicas: <https://www.iberley.es/temas/concepto-regulacion-personas-juridicas-59410>
- LIDÓN, J. M. (2007). Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales pornográficos, ciberterrorismo). (U. d. Deusto, Ed.) *Cuadernos penales José María Lidón*(4), 129-173.
- LÓPEZ, J. C. (21 de diciembre de 2020). *El ADN de nuestros ordenadores tiene más de 4400 años: esta es la sorprendente historia del sistema binario*. Obtenido de xataka: <https://www.xataka.com/historia-tecnologica/adn-nuestros-ordenadores-tiene-4400-anos-esta-sorprendente-historia-sistema-binario>
- LUX, L. M. (2017). El bien jurídico protegido en los delitos informáticos. *Revista chilena de Derecho*, 235-260.
- MARTÍN, R. M. (2001). *Delincuencia informática y derecho penal*. Madrid: Edisofer, S.L.
- MARTÍNEZ, M. D. (2021). El órgano de cumplimiento o compliance officer: figura clave en la organización empresarial. *REvista de DErecho Bancario y Bursátil*(164).

- MARTÍNEZ, M. G. (1 de abril de 2021). Criminalidad corporativa en la era del compliance: una aproximación penal y criminológica a la ciberdelincuencia. *LA LEY compliance penal*(5).
- MAURICIO MEJÍA-LOBO, SANDRA VICTORIA HURTADO-GIL, ANDRÉS MAURICIO GRISALES-AGUIRRE. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: estudio comparativo. *Revista de ciencias sociales*, 29(2), 356-372.
- MERLO, M. N.-S. (21 de septiembre de 2020). Análisis de los delitos informáticos. Una propuesta de clasificación. *Revista Aranzadi de Derecho y Proceso Penal*(60).
- MIRÓ, A. N. (2022). Evolución en el diseño de Sistemas de Compliance. *La ley, compliance penal*(9).
- MUÑOZ, A. G. (2019). *Los ciberdelitos en el ordenamiento español*. Barcelona: Editorial UOC.
- MUÑOZ, A. G. (2021). Compliance frente a delitos informáticos. En S. B.-B.-P. MIGUEL ABEL SOUTO, *Estudios penales en homenaje al profesor José Manuel Lorenzo Salgado* (págs. 553-572). Valencia: Tirant lo Blanch.
- NÚÑEZ, E. V. (2010). Planteamiento y punto de partida. *La ley*.
- ONTIVEIROS, A. (2022). *La Responsabilidad Penal de las Personas jurídicas*. Ciudad de México: Tirant lo Blanch.
- PANIAGUA, J. M. (1988). *Historia del pensamiento jurídico I, de Heráclito a la Revolución francesa* (sexta ed.). Madrid: Universidad complutense de Madrid.
- PATÓN, V. M. (2016). Edad Moderna (I). En V. M. PATÓN, *Análisis histórico de la responsabilidad penal corporativa* (págs. 257-246). Madrid-París: Tesis doctoral. Universidad Autónoma de Madrid.
- PATÓN, V. M. (2016). Edad moderna (II): El Siglo XVIII. En V. M. PATÓN, *Análisis histórico de la responsabilidad penal corporativa* (págs. 347-451). Madrid-París: Universidad Autónoma de Madrid.
- PATÓN, V. M. (2016). El siglo XIX. En V. M. PATÓN, *Análisis histórico de la responsabilidad penal corporativa* (págs. 451-524). Madrid-París: Universidad Autónoma de Madrid.
- PÉREZ ARIAS, J. (2014). *Sistema de atribución de responsabilidad penal a las personas jurídicas*. Madrid: Dykinson.
- PICOTTI, L. (s.f.). *Reati infotmatici, riservatezza, identità digitale*. Obtenido de aidp.it: https://www.aidp.it/allegato_prodotti/115_001_Reati_informatici_e_contro_riservatezza_Picotti.pdf

- PORTILLA, F. J. (2018). Los derechos de la personalidad: la protección de la intimidad, el honor y la vida privada. En J. M. OTROS, *Derecho constitucional II* (págs. 533-576). Pamplona: Aranzadi.
- QUIRÓS, R. C. (2008). El contrato social de Rousseau: el problema de la natural enemistad entre la soberanía y el gobierno. (U. d. Rica, Ed.) *Revista Estudios*(21), 137-148.
- ROBERTO HERNÁNDEZ BERLINCHES y ALICIA GIL GIL. (2019). *Cibercriminalidad*. Madrid: Dykinson.
- RODRÍGUEZ, M. Á. (2020). *Manual de Derecho Informático*. Pamplona: Thomson Aranzadi.
- SÁNCHEZ-ESCRIBANO, M. I. (2014). Panorama normativo supranacional del delito de acceso ilícito a un sistema informático. *Investigaciones en ciencias jurídicas*, 47.
- SCHÜNEMANN, B. (2002). Responsabilidad penal en el marco de la empresa. Dificultades relativas a la individualización de la imputación. *Anuario de Derecho penal y ciencias penales.*, 9-38.
- SCÜNEMANN, B. (1988). Cuestiones básicas de dogmáticas jurídicas-penal y de política criminal acerca de la criminalidad de la empresa. *Anuario de Derecho penal y ciencias penales* , 529-558.
- SIERRA, P. G. (2012). *La responsabilidad penal de las personas jurídicas*. Granada: Editorial de la Universidad de Granada.
- STERN, P. J. (2017). The corporation, a critical, multi-disciplinary handbook. *Cambridge University Press*, 21-26.
- TEUBNER, G. (1984). Autopoiesis in Law and Society: A Rejoinder to Blankenburg. *Law & Society Review*, 18(2), 291-301.
- TEUBNER, G. (2018). El Derecho como Sistema Autopoiético de la Sociedad Global. (C. G.-J. Manuel Cancio Meliá, Ed.) *Teoría de Sistemas y Sistema Jurídico*.
- TOMILLO, M. G. (Septiembre de 2011). Imputación objetiva y culpabilidad en el derecho penal de las personas jurídicas. Especial referencia al sistema español. *Revista jurídica de Castilla y León*(25), 43-84.
- TOMILLO, M. G. (2016). La responsabilidad penal de las personas jurídicas: Comentario a la STS 154/2016 de 29 de febrero, ponente José Manuel Maza Martín. *Diario La Ley*.
- VILAR, S. B. (Octubre de 2022). Persona, algoritmización y posthumanismo, una ecuación hacia la «persona maquina» y su responsabilidad. *Actualidad Civil, Sección Persona y Derechos*(10).
- WALL, D. (2004/5). What are Cybercrimes. *The centre for crime and justice studies*, 20-21.

ZÚÑIGA RODRÍGUEZ, L. (2009). *Bases para un modelo de imputación de responsabilidad penal a las personas jurídicas*. Pamplona: Aranzadi.