eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

FACULTAD DE DERECHO

TESIS DOCTORAL

CIBERSEGURIDAD Y DERECHO PENAL

Presentada por

D. Christian CONAL

Dirigida por

Prof. Dr. iur. Dr. med. Dr. h. c. mult. Carlos María ROMEO CASABONA

2022

RESUMEN / ABSTRACT

El avance de la tecnología obliga a la creación de medidas de ciberseguridad innovadoras que protejan tanto el mundo físico como el virtual frente a nuevos desafíos. Esta investigación abarca desde el establecimiento de las bases conceptuales necesarias para su estudio, como la propia definición de ciberseguridad, hasta un análisis de las normas internacionales y comunitarias relacionadas con ella con objeto de valorar la adecuación del Derecho penal español a las mismas, así como un análisis de derecho comparado, cuyo objetivo es identificar los aspectos destacables de las normas jurídico-penales de los países más avanzados en la legislación de esta materia. Incluye también un análisis de distintos delitos del Código Penal español para determinar la posible existencia de un grupo de ellos que puedan considerarse delitos que afectan a la ciberseguridad, estudiando con especial profundidad el delito de acceso ilícito a un sistema de información, evaluando la conveniencia de reubicarlo en un nuevo título y de convertir la ciberseguridad en un bien jurídico autónomo protegido por el Derecho penal español. Continúa la investigación adoptando finalmente una perspectiva sanitaria continuamente insinuada, con un análisis de la manera en que nuevas tecnologías como la inteligencia artificial, la robótica, los drones, los hospitales inteligentes o el Internet de las cosas médicas afectan a la ciberseguridad y al Derecho penal, para concluir con una mirada al futuro de ambos en conjunto teniendo en cuenta el metaverso, los avances en ciberbioseguridad y computación cuántica, y nuestro deber de vigilar diligentemente la frontera digital.

Technological progress makes necessary the creation of innovative cybersecurity measures to protect both the physical and virtual world against new challenges. The scope of this research covers from the establishment of the conceptual bases necessary for its study such as the definition of cybersecurity itself, to an analysis of the international and EU regulations related to cybersecurity in order to assess how Spanish Criminal Law accommodates them; as well as an analysis of comparative law with the aim of identifying the noteworthy aspects of penal law regulations in leading countries regarding legislation on this matter. Furthermore, several criminal offences laid out in the Spanish Criminal Code are analysed to determine the potential existence of a group of criminal offences that could be considered that affect cybersecurity. In particular, the present paper delves into the study of the criminal offence of unlawful access to an information system, assessing the advisability of relocating it to a new Chapter and of making cybersecurity an autonomous legal interest protected by Spanish Criminal Law. Then, the present research focuses on a continuously insinuated health perspective, with an analysis of how new technologies such as Artificial Intelligence, robotics, drones, smart hospitals or the Internet of Medical Things (IoMT) affect cybersecurity and criminal law. Finally, it concludes with an outlook to the future of both in conjunction, taking into account the Metaverse, cyberbiosecurity and quantum computing breakthroughs, and our duty to remain vigilant on the digital frontier.

Índice

ABREVIATURAS

AAP Auto de la Audiencia Provincial

ACSC Australian Cyber Security Centre

AEPD Agencia Española de Protección de Datos

art. Artículo

arts. Artículos

ATS Auto del Tribunal Supremo

BCSC Centro Vasco de Ciberseguridad del Gobierno Vasco

CCB Centre for Cyber Security Belgium

CCIPS Computer Crime and Intellectual Property Section

CCPP Códigos penales

CE Constitución española

CEPC Comité Europeo para los Problemas Criminales

CERT Equipo de Respuesta ante Emergencias Informáticas

CFCS Centre for Cyber Security de Dinamarca

CIA Central Intelligence Agency

CNCS Consejo Nacional de Ciberseguridad

coord. Coordinador

coords. Coordinadores

CP Código penal

CSIRT Equipo de Respuesta ante Incidencias de Seguridad Informáticas

CYCO Cybercrime Coordination Unit Switzerland

DDoS Ataque de denegación de servicio distribuido

dir. Director

dirs. Directores

DNS Sistema de nombres de dominio

DOJ United States Department of Justice

DOD United States Department of Defense

DoS Ataque de denegación de servicio

DUDH Declaración Universal de los Derechos Humanos

EC3 Centro Europeo contra la Ciberdelincuencia

ECS Especialista en Ciberseguridad Sanitaria

ed. Edición

edit. Editor

eds. Editores

Ed. Editorial

EE. UU. Estados Unidos

ENISA Agencia de la Unión Europea para la Ciberseguridad

Europol Agencia de la Unión Europea para la Cooperación Policial

FBI Federal Bureau of Investigation

FFCCSE Fuerzas y Cuerpos de Seguridad del Estado

FVEY Five Eyes

GDT Grupo de Delitos Telemáticos de la Guardia Civil

I+D Investigación y desarrollo

IA Inteligencia artificial

IBM International Business Machines Corporation

IC3 Internet Crime Complaint Center

IdC Internet de las Cosas

IdCM Internet de las Cosas Médicas

INCIBE Instituto Nacional de Ciberseguridad de España

IP (Dirección del) Protocolo de Internet

KGB Comité para la Seguridad del Estado de la Unión Soviética

LECrim Ley de Enjuiciamiento Criminal

LO Ley Orgánica

LOPD Ley Orgánica de Protección de Datos de Carácter Personal

LOPD-GDD Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales

LOPJ Ley Orgánica del Poder Judicial

MGN Medical-Grade Network

NCA National Crime Agency de Reino Unido

NCAZ Nationales Cyber-Abwehrzentrum de Alemania

NCSC National Cyber Security Centre de Reino Unido

no. Número

NSA Agencia de Seguridad Nacional del Gobierno de los Estados Unidos

OMS Organización Mundial de la Salud

ONU Organización de las Naciones Unidas

OSCE Organización para la Seguridad y la Cooperación en Europa

OTAN Organización del Tratado del Atlántico Norte

p. Página

pp. Páginas

RFID Identificación por radiofrecuencia

RGPD Reglamento General de Protección de Datos

§ Sección

SAN Sentencia de la Audiencia Nacional

SAP Sentencia de la Audiencia Provincial

SIM Módulo de identificación de abonado

STC Sentencia del Tribunal Constitucional

StGB Strafgesetzbuch o Código penal alemán

STJUE Sentencia del Tribunal de Justicia de la Unión Europea

STS Sentencia del Tribunal Supremo

SsTC Sentencias del Tribunal Constitucional

TAJM Tratado de asistencia jurídica mutua

TC Tribunal Constitucional

TFUE Tratado de Funcionamiento de la Unión Europea

TIC Tecnologías de la Información y la Comunicación

TJUE Tribunal de Justicia de la Unión Europea

TS Tribunal Supremo

UE Unión Europea

UIT Unión Internacional de Telecomunicaciones

UKUSA Tratado de seguridad entre el Reino Unido y los Estados Unidos

UNODC Oficina de las Naciones Unidas contra la Droga y el Delito

USC Code of Laws of the United States of America

vol. Volumen

INTRODUCCIÓN

CIBERSEGURIDAD Y DERECHO PENAL: CONCEPTUALIZACIÓN

El avance de la tecnología y el mundo digital e interconectado que ha nacido a consecuencia del mismo han provocado la obsolescencia de la definición clásica de seguridad[1]. Innovaciones como Internet, la inteligencia artificial, la robótica, los drones, o el IdCM, todas ellas susceptibles de ser utilizadas por los delincuentes en su actividad criminal, obligan a replantear esta definición alejándola de su planteamiento tradicional, que se sustentaba sobre los límites físicos de un Estado y sobre la pretensión de proteger un territorio específico sobre el que se ejerce la soberanía[2]. No obstante, no resultaría inteligente renunciar por completo a las valiosas aportaciones que la doctrina y la jurisprudencia han desarrollado a lo largo de los años, sino que es mucho más razonable, tras una selección de lo mejor de las mismas, concebir una nueva definición adaptada a un escenario en el que imperan la digitalización y la tecnología más vanguardista.

En la elaboración de esta definición hay que tener en cuenta, primero, que la seguridad es necesaria para alcanzar un objetivo, una tarea o una funcionalidad, y para defenderlos de quienes pretenden impedir que se consigan[3]; segundo, que los objetivos a proteger, así como los potenciales peligros y los medios para hacerles frente (ya sea mediante políticas, estrategias o estructuras de seguridad) se caracterizan por su enorme

---

[1] E. Hirsch Ballin, H. Dijstelbloem y P. De Goede, "The Extension of the Concept of Security", en E. Hirsch Ballin, H. Dijstelbloem y P. De Goede (eds.), *Security in an Interconnected World: A Strategic Vision for Defence Policy,* 1ª ed., Cham, Springer, 2020, pp. 13 - 26. Además de los avances tecnológicos, también han influido los profundos cambios geopolíticos que han tenido lugar a nivel mundial en las últimas décadas.

[2] L. Coles-Kemp, D. Ashenden y K. O´Hara, "Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen", *Politics and Governance,* vol. 6, no. 2, 2018, pp. 46 – 47. Para un Estado, su soberanía en el ciberespacio depende del reconocimiento externo de su autoridad por parte de otros Estados y de su capacidad para ejercer medidas de control sobre una determinada parte del mismo.

[3] F. Obrador Serra, "Análisis del concepto de seguridad", *Cuadernos de estrategia,* no. 49, 1992, p. 30.

variedad[4]; y, tercero, es fundamental tener en cuenta las nuevas tecnologías en sí mismas[5] y los riesgos emergentes[6], puesto que pueden adquirir nuevas dimensiones de peligrosidad, sobre todo en lo concerniente a infraestructuras críticas como, entre otras, las sanitarias.

Además de dichas ideas, relacionadas con el contenido de la seguridad, los elementos que estructuralmente componen la misma, son: su objeto referente (que ya no se limita a un único Estado, sino que obliga a implementar un modelo de seguridad cooperativo para hacer frente a desafíos de carácter transnacional), la naturaleza de los desafíos a los que se enfrenta, los valores a proteger y, por último, los mecanismos a través de los cuales se trata de garantizar la seguridad[7]. Esta idea de mecanismo o barrera resultará esencial en esta investigación, puesto que la ciberseguridad está íntimamente relacionada con la misma.

Por último, el factor de la intencionalidad es muy importante, puesto que en ausencia del mismo, la doctrina anglosajona utiliza el término *safety,* reservando *security* para aquellos actos intencionados que, venciendo los mecanismos establecidos para garantizar la seguridad, provocan una lesión

[4] D.A. Baldwin, "The concept of security", *Review of International* Studies, no. 23, 1997, pp. 24 – 25.

[5] J. Avilés Farré, "Por un concepto amplio de seguridad", en Ministerio de Defensa – Instituto Español de Estudios Estratégicos (eds.), *Revisión de la Defensa Nacional,* 1ª ed., Madrid, Ministerio de Defensa – Instituto Español de Estudios Estratégicos, 2002, pp. 34 – 35. Se menciona de manera específica el ciberespacio como nuevo entorno con inmensas posibilidades para la actividad delictiva en perjuicio tanto de las instituciones públicas como de las empresas privadas. Ya entonces, era indudable la necesidad de ampliar el concepto de seguridad atendiendo a los gravísimos daños que podría ocasionar un ciberataque contra los sistemas informáticos que regulan los sectores esenciales de un país, como la Defensa Nacional.

[6] M. Nieto Rodríguez, "El nuevo concepto de seguridad: amenazas y riesgos emergentes", en Ministerio de Defensa – Instituto Español de Estudios Estratégicos (eds.), *La cooperación Fuerzas de Seguridad – Fuerzas Armadas frente a los riesgos emergentes,* 1ª ed., Madrid, Ministerio de Defensa – Instituto Español de Estudios Estratégicos, 2001, p. 58. En las primeras aproximaciones doctrinales a la conceptualización de la seguridad se tenía ya en cuenta la importancia de la incipiente revolución tecnológica sobre la misma.

[7] G. Abad Quintanal, "El concepto de seguridad: su transformación", *Comillas Journal of International Relations,* no. 4, 2015, pp. 43 – 50. A efectos de esta investigación, los desafíos a los que se enfrenta la seguridad son los delitos, y los valores a proteger son, como es lógico, los bienes jurídicos protegidos.

en un valor a proteger. La actividad criminal en la que el sujeto activo quebranta intencionadamente las leyes establecidas para proteger determinados bienes jurídicos debe encuadrarse, por lo tanto, en el segundo de los términos.

En consecuencia, la seguridad puede definirse como la condición en la que la probabilidad de efectos negativos intencionados sobre los objetivos a proteger es baja[8].

Al estar dotada de un carácter multifuncional, es posible acompañar la noción de seguridad de un enorme número de adjetivos para hacer referencia a realidades distintas[9], como la ciberseguridad[10], seguridad informática o seguridad de la tecnología de la información, objeto de nuestro estudio, que es diferente de la seguridad de la información.

Para poder relacionar la ciberseguridad con el Derecho penal y desarrollar una definición unitaria que sea la base de esta investigación, es necesario definir primero lo que es la ciberseguridad, por sí misma. Solo de este modo será posible entender de qué se trata y encajarla en tipos delictivos específicos del Derecho penal que han sido analizados durante décadas por

---

[8] P.J. Blokland y G.L. Reniers, "The Concepts of Risk, Safety and Security: A Fundamental Exploration and Understanding of Similarities and Differences", en C. Bieder y K. Pettersen Gould (eds.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice,* 1ª ed., Cham, Springer, 2020, p. 14.

[9] C. Milione, "La noción de seguridad en la doctrina del Tribunal Europeo de Derechos Humanos: referencias al derecho a la tutela judicial efectiva", *Revista de Derecho Político,* no. 107, 2020, pp. 244 – 245.

[10] El diccionario de la Real Academia Española no recoge la palabra *ciberseguridad*. Sí recoge, no obstante, el prefijo *ciber-* (que indica relación con redes informáticas) y el nombre común *seguridad* (cualidad de seguro). Así, a pesar de la ausencia de una entrada específica, se deduce que la palabra *ciberseguridad* define la cualidad de segura de una red informática. La primera matización que quiero introducir es que una red podrá considerarse segura cuando esté exenta de daño, incluso cuando no lo esté de peligro o riesgo, siendo estos dos últimos factores inevitables que solo cuando se concretan conllevan el primero. Será cuando la red sufra un daño cuando deje de ser segura, no así cuando esta se encuentre en un peligro o riesgo inherentes a su existencia. El Oxford English Dictionary, por su parte, sí define la palabra *cybersecurity*: "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this". La definición británica, mucho más amplia, introduce una doble categoría al referirse, por un lado, al estado en el cual se está protegido contra el uso criminal o no autorizado de datos electrónicos y, por otro, a las medidas adoptadas para conseguir este objetivo.

los académicos más distinguidos de dicho campo del saber, relacionando así ambas disciplinas. Gracias a esta definición podré acotar qué arts. del CP están relacionados con la ciberseguridad y cuáles no, analizando solo aquellos en los que, objetivamente, puede encuadrarse la misma. Si se pretende llegar a una definición verdadera y definitiva apartando todos los datos erróneos o innecesarios que se han ido añadiendo a medida que distintos expertos realizaban sus aportaciones, hay que empezar por distinguir entre lo que la ciberseguridad es y las medidas orientadas a garantizarla.

Y es que, en ausencia de esta distinción, no tiene sentido hablar de medidas de ciberseguridad o protocolos de ciberseguridad, toda vez que el propio término ya incluiría, en sí mismo, la referencia al medio para la consecución de este fin. Si distinguimos, en cambio, entre el medio (la medida adoptada para garantizarla) y el fin (la ciberseguridad), reservando el término para este último, la utilización de estas expresiones en las que se hace referencia al medio adquiere pleno sentido. Limitaré la definición, en consecuencia, al objetivo que se pretende obtener con la ciberseguridad, revelando así su verdadera esencia.

Hay que tener en cuenta que el mayor problema que existe para definir la ciberseguridad es que ya ha sido objeto de una interminable discusión académica que ha pretendido analizarla desde distintas perspectivas[11]. El término se utiliza, en la actualidad, de manera generalizada, y parecen existir tantas definiciones como autores, siendo, en muchos casos, subjetivas y de

[11] R.J. Deibert, "Toward a Human-Centric Approach to Cybersecurity", *Ethics & International Affairs,* vol. 32, no. 4, 2018, p. 411. Aunque existe un consenso en torno a la importancia de la ciberseguridad, sucede lo contrario con su definición, hasta el extremo de que, en una base de datos de Washington, D.C., pueden encontrarse hasta cuatrocientas definiciones distintas, la mayoría de ellas con un punto de vista relacionado con la seguridad nacional. Es decir, que la mayoría de las definiciones, aunque distintas entre sí, ponen al Estado como elemento principal a proteger, por tener que desenvolverse en un escenario de competencia en el que el objetivo es la supervivencia. Creo que, desde la perspectiva de la utilidad para el Derecho penal, conviene desarrollar una definición jurídica de ciberseguridad aplicable tanto a las instituciones públicas como a las empresas privadas de cada país, así como a sus ciudadanos, de manera que encaje en tipos delictivos muy distintos entre sí en lo concerniente a qué pretenden proteger y al sujeto pasivo.

escaso valor informativo[12]. Considero que lo más acertado es escoger las definiciones del ámbito jurídico más precisas e, igual que en el caso de los diccionarios, extraer lo útil rechazando lo erróneo o innecesario. Se trata, por tanto, de equilibrar dos intereses opuestos: por un lado, realizar una definición sucinta y exacta; por otro, que la misma contenga el mayor nivel de detalle posible sin disminuir su calidad.

La mera suma de definiciones existentes es incompatible con este objetivo[13], así como las definiciones demasiado extensas[14] [15]. Por otra parte, una exposición de todas ellas, con un análisis pormenorizado de sus elementos útiles, inservibles o equivocados solo conduciría a esta construcción teórica a la confusión[16]. Para poder definir la ciberseguridad, es

[12] D. Craigen, N. Diakun – Thibault y R. Purse, "Defining Cybersecurity", *Technology Innovation Management Review,* vol. 4, no. 10, 2014, p. 13. Es necesario ir más allá de las definiciones de ámbitos como la informática, la ingeniería eléctrica y las matemáticas para completar una definición jurídico-penal.

[13] J. Kosseff, "Defining Cybersecurity Law", *Iowa Law Review,* vol. 103, no. 3, 2018, p. 1010.

[14] R. Von Solms y J. Van Niekerk, "From information security to cyber security", *Computers & Security,* no. 38, 2013, p. 101. No puede definirse la ciberseguridad como la protección de todo el ciberespacio, puesto que dicha definición supondría una pretensión de abarcar demasiado, máxime cuando pretendo utilizarla como base para un posterior análisis jurídico-penal centrado en la protección de ciertos bienes jurídicos.

[15] D. Schatz, R. Bashroush y J. Wall, "Towards a more representative definition of cyber security", *The Journal of Digital Forensics, Security and Law,* vol. 12, no. 2, 2017, p. 66. Aunque la definición propuesta recoge, en efecto, los elementos más relevantes y habituales de las definiciones analizadas, el resultado es, como reconocen los propios autores, poco relevante. Es interesante, no obstante, que hagan referencia a la manera en que la definición sufrirá cambios con el tiempo de manera paralela al progreso tecnológico.

[16] Sirva como ejemplo la definición de C. Briera Dalmau, "La ciberseguridad: consideraciones y apuntes sobre el régimen jurídico aplicable a la seguridad de las redes y sistemas de la información", en J. Velázquez (coord.), *Cuadernos de Derecho para ingenieros: ciberseguridad,* Las Rozas, Madrid, Wolters Kluwer, 2017, pp. 272 – 274. Cuando se utilizan como base definiciones procedentes de distintas fuentes y se intenta integrarlas todas, el resultado es confuso y, sobre todo, poco útil en la práctica. Es lo lógico cuando, en las mismas, se parte de perspectivas completamente alejadas. Así, no queda claro, ni siquiera, si la ciberseguridad es una acción, una medida, o, en el caso de la definición de la UIT, un conjunto de herramientas, políticas, conceptos y salvaguardas relacionados con la seguridad, directrices, alternativas de gestión de riesgos, acciones, formación, mejores prácticas, garantías y tecnologías, todo ello con un determinado fin. Esto, por supuesto, constituye un *totum revolutum* de dudoso valor académico y sin ninguna utilidad práctica, y solo lo he incluido para justificar la manera en la que construyo mi definición, extrayendo solo lo útil y valioso de cada una de las fuentes citadas y rechazando los elementos inservibles.

necesario conocer primero cuál es su esencia, a la cual solo se puede llegar a través de la suma de sus atributos. Si bien hay que encuadrar la ciberseguridad, como término, en los primeros años de la década de 1990[17], los atributos que la caracterizan tardaron más de dos décadas en asentarse doctrinalmente[18]. Atendiendo a los mismos, se puede definir la ciberseguridad como la seguridad física y lógica de las redes y sistemas informáticos[19]. A través de las medidas de ciberseguridad se pretenden proteger, en primer lugar, las redes informáticas (conjunto de equipos conectados mediante cables, señales, ondas o cualquier otro medio de transporte de datos que comparten información, recursos y servicios), que se componen de elementos materiales (*hardware*) y de programas, instrucciones y reglas necesarios para ejecutar ciertas tareas (*software*); y, en segundo lugar, los sistemas informáticos, que hacen posible el almacenamiento y procesamiento de información y se componen de un conjunto de partes interrelacionadas (*hardware*, asociado al subsistema físico, como en el caso de la CPU; y *software*, asociado al subsistema lógico, como en el caso del sistema operativo). Aunque garantizar la ausencia total de peligro resulta imposible, unas medidas de ciberseguridad adecuadas deben ofrecer un elevado nivel de protección a los principales activos de una organización (es decir, a aquellos recursos del sistema necesarios para que se alcancen los objetivos propuestos): el *hardware*, el *software*, y, por supuesto, los datos. Cierto sector de la doctrina incluye entre estos activos, incluso, al personal de la organización que utiliza la estructura tecnológica y de comunicación.

Añadir cualquier aspecto superfluo solo me haría incurrir en el mismo error que ya he criticado, y cumplo así mi intención de desarrollar una

---

[17] L. Hansen y H. Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School”, *International Studies Quarterly,* vol. 53, no. 4, 2009, p. 1155. Su utilización se remonta a los análisis de seguridad que realizaban los informáticos en esa época, pero se puso de manifiesto que debía desarrollarse al entender que los peligros derivados del uso de algunas tecnologías podían tener efectos sociales devastadores.

[18] T.W. Edgar y D.O. Manz, *Research Methods for Cyber Security,* Cambridge, Elsevier, 2017, pp. 37 – 39.

[19] G. Escrivá Gascó et al., *Seguridad Informática,* 1ª ed., Madrid, Macmillan Profesional, 2013, pp. 7 – 8.

definición de ciberseguridad sucinta y exacta que, al mismo tiempo, contenga un nivel de detalle tal que revele su esencia. Además, al hacer referencia esta definición al fin, y no al medio, cumple también el requisito de poder integrarse en el desarrollo de medidas y protocolos orientados a salvaguardarla. Se corresponde, también, con el objetivo de la seguridad informática[20]: la minimización de los riesgos asociados al acceso y utilización de las redes de forma no autorizada.

El objetivo principal (aunque, como ya he expuesto, no el único) de la ciberseguridad es, sin duda, garantizar la seguridad de la información contenida en soportes informáticos[21] a través de la protección de la disponibilidad, la integridad y la confidencialidad tanto de los datos informáticos como de los sistemas informáticos que los contienen.

En primer lugar, la disponibilidad hace referencia a la posibilidad de acceder a la información en el momento que el usuario desee durante todo el tiempo que sea necesario. Si, ante un intento de acceso, el usuario comprueba que no es posible llevarlo a cabo satisfactoriamente o, habiéndolo conseguido en un primer momento, su actividad se ve interrumpida de forma indebida, la disponibilidad de dicha información deja de estar garantizada, puesto que la imposibilidad de acceder a la misma la convierte en no disponible.

En segundo lugar, la integridad se refiere al mantenimiento de todas las partes de la información, a su inalterabilidad y a la ausencia de modificaciones indeseadas. Este segundo lugar respecto a la disponibilidad le corresponde porque es posible que unos datos estén disponibles y, sin embargo, presenten problemas relacionados con la integridad, como no permitir el acceso a zonas específicas o permitirlo solo para comprobar que,

[20] *Guía práctica de Ciberseguridad,* Cizur Menor, Navarra, Aranzadi, 2019, p. 167.

[21] J.M. Cardona Pastor y J.S. Cuñat Ferrando, *Guía Rápida Ciberseguridad para Despachos y Profesionales*, 1ª ed., Madrid, Francis Lefebvre, 2018, pp. 16 – 18. Es importante señalar que la seguridad de la información pretende proteger la información contenida en diferentes medios o formas, pero a efectos de esta investigación solo resulta de interés aquella información que contienen los medios informáticos.

aunque disponible, la información ha visto afectada su integridad al haber sido alterada o modificada.

Por último, en tercer lugar, está la confidencialidad, que garantiza que solo acceda a los datos quien deba tener acceso a los mismos, y nunca usuarios no autorizados.

No obstante, la existencia de las medidas de ciberseguridad no resulta pacífica, puesto que estos mecanismos a través de los cuales se trata de garantizar la ciberseguridad se ven constantemente amenazados y atacados. Es necesario introducir, en este sentido, dos definiciones: una amenaza es un peligro posible que podría aprovecharse de una vulnerabilidad, quebrantando las medidas de seguridad y causando un perjuicio[22]; mientras que un ataque es la ejecución deliberada de uno o más pasos orientados a vulnerar las medidas de ciberseguridad aprovechando las vulnerabilidades existentes, que pueden ir desde la ausencia de protección física de un equipo a los defectos en el diseño de un sistema. Se conoce como adversario a quien podría estar planeando un potencial ataque, y atacante a quien no solo lo planea, sino que lo ejecuta[23]. Los ataques deben cumplir siempre una característica: deben ser intencionados; en caso contrario, nos encontraríamos ante lo que se denomina un error o acción fortuita. Pueden ser físicos, cibernéticos, o una combinación de ambos (es decir, pueden originarse en el ámbito físico y extender sus efectos negativos en el ciberespacio, o viceversa). Sus fases son cinco: reconocimiento (obtención de toda la información necesaria sobre la víctima, ya se trate de una persona física o jurídica); exploración (obtención de información sobre el sistema a atacar); obtención de acceso (intento de explotar las vulnerabilidades detectadas); mantenimiento del acceso (a través de la implantación de herramientas que permitan accesos posteriores al sistema); y borrado de huellas (con objeto de evitar la detección de la actividad ilícita).

---

[22] W. Stallings, *Fundamentos de Seguridad en Redes. Aplicaciones y Estándares,* 2ª ed., Madrid, Pearson Educación, 2004, p. 5.

[23] P.C. Van Oorschot, *Computer Security and the Internet: Tools and Jewels,* 1ª ed., Cham, Springer, 2020, p. 5.

Mención aparte merecen las estrategias orientadas a explotar las debilidades del factor humano, como la ingeniería social, consistente en la obtención de información confidencial o sensible de un usuario utilizando métodos propios de la condición humana[24]. De un modo u otro, estas vulneraciones tienen como objetivo eludir las medidas de ciberseguridad por lo general como medio para la consecución de una finalidad distinta al mero acceso indebido, aunque tampoco resulta conveniente menospreciar sin más este fin.

En efecto, los ataques criminales contra las medidas de ciberseguridad se caracterizan, en la mayoría de los casos, por su carácter medial o instrumental, puesto que el objetivo último del delincuente es lesionar no la ciberseguridad en sí misma, sino bienes jurídicos protegidos que solo puede alcanzar rebasando la barrera que suponen estas medidas. En consecuencia, para categorizar los delitos que afectan a la ciberseguridad desde una perspectiva jurídico-penal (o delitos contra[25] la ciberseguridad, por mucho que, en la mayoría de los casos, la lesión a la misma tenga carácter medial o instrumental, siendo solo un medio para la consecución de un fin), el criterio es que afecten a la seguridad física o lógica de las redes o sistemas informáticos[26], no estando relacionada la ciberseguridad con aquellos delitos

[24] Escrivá Gascó et al., *Seguridad Informática,* p. 10.

[25] Siguiendo los cánones establecidos en el CP, y al tratarse del nombre común *seguridad* (solo que precedido por el prefijo *ciber-*), utilizo la preposición *contra*, igual que en los delitos contra la seguridad colectiva o los delitos contra la Seguridad Vial. Para realizar esta investigación me apoyaré en, entre otras, las versiones del año 2022 del CP y de la LECrim impresas por la Ed. Colex., las más actualizadas posibles.

[26] C.M. Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos,* 1ª ed., Valencia, Tirant lo Blanch, 2004, pp. 74 – 75. Estas dos vertientes de la seguridad se complementan mutuamente.

que, por sus características, no lo hacen[27] [28], por mucho que se traten de ciberdelitos[29]. Como veremos en el capítulo tercero, al proyectarse sobre bienes jurídicos de distinta naturaleza, se encuentran dispersos y no se recogen en un título o capítulo determinado del CP. De lo que no cabe duda es de que la ciberseguridad ha adquirido entidad propia[30] [31], y de que delitos

[27] T.K. Mackey y G. Nayyar, "Digital danger: a review of the global public health, patient safety and cybersecurity threats posed by illicit online pharmacies", *British Medical Bulletin,* vol. 118, no. 1, 2016, pp. 122 – 123. Al analizar el delito, se analizan en primer lugar las consecuencias de la existencia de farmacias ilegales en línea, como los riesgos sanitarios para los pacientes derivados del autodiagnóstico o el consumo de medicamentos innecesarios desde un punto de vista terapéutico. Después, se desarrolla un apartado propio relativo a las amenazas relacionadas con la ciberseguridad, evidenciando que, aunque estas actividades se llevan a cabo en línea y son ilegales, no están necesariamente relacionadas, en su totalidad, con la ciberseguridad, excepto en lo relativo a aspectos como el uso de *malware* durante las mismas.

[28] D.J. Maldonado Guzmán, "El mal denominado delito de *grooming online* como forma de violencia sexual contra menores. Problemas jurídicos y aspectos criminológicos", *Revista Electrónica de Estudios Penales y de la Seguridad: REEPS,* no. Extra 5, 2019, pp. 1 – 18. En último lugar, después de mencionar una modalidad delictiva que sí está relacionada con la ciberseguridad y una que solo lo está parcialmente, expongo en último lugar una sin relación alguna con la misma. En efecto, el *grooming* o engaño pederasta por Internet es un delito que se lleva a cabo mediante alguna de las TIC y supone una innegable amenaza para la seguridad de la víctima. Sin embargo, no está relacionado con la ciberseguridad de acuerdo con la definición que he desarrollado, no siendo, en consecuencia, un delito contra la ciberseguridad.

[29] A.A. Gillespie, *Cybercrime: Key Issues and Debates,* 1ª ed., Abingdon, Routledge, 2016, pp. 8 – 11.

[30] Consejo de Europa, *Organised crime in Europe: the threat of cybercrime,* Estrasburgo, Consejo de Europa, 2005, pp. 87 – 134. Ya en 2005, hace más de quince años, el Consejo de Europa diferenciaba, al abordar el fenómeno de los ciberdelitos en este texto, entre aquellos que atentaban contra las redes y sistemas informáticos y los que se englobaban en una categoría todavía genérica reservada para delitos tradicionales relacionados con ordenadores, como un incipiente y aún no denominado como tal *grooming*.

[31] En ediciones anteriores (2017 – 2018), dentro de la Parte VI, relativa al ámbito penal, se trataron en el capítulo vigésimo los ciberdelitos y la ciberseguridad de manera conjunta. En cambio, en A. González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 - 2021*, Madrid, Francis Lefebvre, 2019, p. 5, se ha reservado un capítulo individual a cada una de estas disciplinas (vigesimonoveno y trigésimo, respectivamente) dentro de su Parte VI, dedicado al Derecho penal. A esta tendencia de la doctrina hay que añadir el establecimiento de centros especializados en prevenir y combatir específicamente los delitos que afectan a la ciberseguridad, como la European Union Agency for Network and Information Security (ENISA) en 2005, el Instituto Nacional de Ciberseguridad (INCIBE) en España en 2006, el Nationales Cyber-Abwehrzentrum (NCAZ) en Alemania en 2011, el National Cyber Security Centre (NCSC) en el Reino Unido en 2016 y, a nivel regional, el Centro Vasco de Ciberseguridad (BCSC, por responder el acrónimo a sus siglas en inglés) en 2017. La persecución de los ciberdelitos en sentido general mantiene intacta su importancia, pero resulta evidente, por los motivos que expondré en el subapartado III, que era necesario

como, entre otros, el *cracking*, que analizaré en profundidad en dicho capítulo tercero, evidencian la necesidad de plantearse la posibilidad de otorgar a aquella la categoría de bien jurídico protegido autónomo.

Al tratarse de una investigación en la que la medicina resulta trascendental, se convierte en imperativo distinguir entre ciberseguridad y bioseguridad[32] [33], toda vez que su confusión puede resultar fatal al tratarse de dos disciplinas en ocasiones conectadas[34], pero independientes. Así, y de acuerdo con la traducción que yo mismo realicé para la Enciclopedia de Bioderecho y Bioética de la definición desarrollada por la Academia Nacional de Ciencias de Estados Unidos[35], la bioseguridad es: "La seguridad frente al

---

otorgar de manera específica la trascendencia que merecen a los delitos que afectan a la ciberseguridad.

[32] E. Liu, E. Effiok y J. Hitchcock, "Survey on health care applications in 5G networks", *IET Communications,* vol. 14, no. 7, 2020, pp. 1073 – 1080. Es indudable que las TIC, cuando se utilizan de manera correcta, pueden ser un apoyo para la protección de la bioseguridad y para el sistema sanitario en su conjunto.

[33] R.N. Kostoff et al., "Adverse health effects of 5G mobile networking technology under real-life conditions", *Toxicology Letters,* vol. 323, 2020, pp. 38 – 39. La tecnología 5G es el ejemplo perfecto para exponer cómo las TIC pueden afectar a la bioseguridad, incluso cuando la hipotética pretensión tras su uso es beneficiar, entre otros, a los pacientes. Las protestas en relación con la misma debido a su impacto en la salud humana han traspasado las barreras de la academia y se han convertido en un verdadero clamor popular, especialmente cuando su instalación masiva se ha llevado a cabo no solo sin la aprobación, sino con la opinión en contra de amplios sectores tanto de la academia como del pueblo. Y es que las mejoras que pretende introducir el 5G, en un entorno ya de por sí saturado de radiación, no compensan los peligros que conlleva para la salud humana. En este caso, el peligro no estaría en la ciberseguridad, sino en la bioseguridad. De ahí la importancia de distinguirlas y de proteger ambas, comprendiendo sus diferencias.

[34] R.S. Murch et al., "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy", *Frontiers in Bioengineering and Biotechnology,* vol. 6, no. 39, 2018, pp. 1 - 2. Aunque no es la última vez que mencionaré la llamada ciberbioseguridad, no soy partidario de esta clase de categorías híbridas porque restan riqueza a las dos categorías ya existentes (ciberseguridad y bioseguridad), mediante las cuales ya puede abordarse intelectualmente cualquier controversia que plantee la relación entre las nuevas tecnologías y la salud humana. Habiendo desarrollado una adecuada definición de ambas, y habiendo acotado los campos de estudio de cada una, solo hay que decidir desde qué perspectiva pretende abordarse un problema, como en el caso del 5G, en el que podríamos evaluar su grado de seguridad y garantía de la disponibilidad, la integridad y la confidencialidad desde el punto de vista de la ciberseguridad y, al mismo tiempo, analizar su pernicioso impacto en la salud humana desde el prisma de la bioseguridad.

[35] P.F. Walsh, *Intelligence, Biosecurity and Bioterrorism,* 1ª ed., Londres, Palgrave Macmillan, 2018, p. 11.

uso equivocado, inapropiado o intencionadamente malicioso o perverso de agentes biológicos o biotecnologías potencialmente peligrosos, incluyendo el desarrollo, producción, almacenamiento o uso de armas biológicas, así como los brotes de enfermedades nuevamente emergentes y epidémicas". La bioseguridad no es uno de los objetos de estudio de esta investigación, salvo cuando esté inevitablemente relacionada con la ciberseguridad o con el Derecho penal, e incluso en esos casos será secundaria. No obstante, no hay que olvidar que los escenarios más lesivos posibles para los pacientes son aquellos en los que de una crisis de ciberseguridad se deriva una de bioseguridad, y aquellos en los que una crisis sanitaria en la que no es posible garantizar la bioseguridad impide una adecuada utilización de los sistemas informáticos, paralizando los sistemas de salud y facilitando la comisión de delitos en estas infraestructuras críticas, como expondré en el capítulo cuarto.

No cabe duda de la creciente conexión entre las nuevas tecnologías y la medicina, cuyo resultado inevitable es la aparición de nuevas cuestiones legales[36] y éticas[37] relativas a la ciberseguridad. Aunque los ciberataques más relevantes en el ámbito internacional han tenido lugar en un contexto ajeno al mismo[38], el sector sanitario, por su importancia, también se ha visto

[36] M.A. Lozano Merino, "Ciberseguridad y COVID-19 nos empujan para la transformación digital", *Aranzadi digital,* no. 1/2020, 2020, p. 2. La crisis sanitaria ocasionada por la enfermedad del coronavirus COVID-19 de Wuhan, China, ha obligado a acelerar los procesos de digitalización para permitir que sectores como el sanitario continúen con su actividad con el menor perjuicio posible para los pacientes, suponiendo esto un inevitable aumento del riesgo para unos sistemas de ciberseguridad que también deberán adaptarse.

[37] M.J. Parker et al., "Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic", *Journal of Medical Ethics,* 2020, pp. 3 – 4. A pesar de que la ética de la ciberseguridad resulta fascinante, me centraré en la perspectiva jurídica y no entraré a valorar en profundidad los aspectos éticos de la misma, salvo de manera muy puntual. No obstante, el hecho de que a causa de la pandemia de coronavirus COVID-19 se hayan desarrollado aplicaciones de rastreo de la localización para descargar en los teléfonos móviles, y un 74% de usuarios encuestados estén de acuerdo con su utilización siempre que se les garantice su seguridad, evidencia que la confianza ciega de las personas en las nuevas tecnologías podría tener graves consecuencias para la libertad humana. La discusión en relación con la posible obligatoriedad de utilizar la aplicación y, como consecuencia, de llevar en todo momento un teléfono móvil para poder ser rastreado es, por sí misma, enormemente preocupante desde un punto de vista ético.

[38] L. Pérez-Prat Durbán, "Los ciberataques y el uso de la fuerza en las relaciones internacionales", en G. Fernández Arribas (edit.), *Ciberataques y ciberseguridad en la*

atacado con gravísimas consecuencias en un contexto en que la tecnología avanza de manera exponencial[39]. Así sucedió en mayo de 2017 con el ataque masivo del *ransomware* WannaCry[40], que paralizó los servicios sanitarios de varios países del mundo y obligó a sus gobiernos a replantear sus estrategias de ciberseguridad, sobre todo en relación con las infraestructuras críticas. En Reino Unido, hay que destacar entre las consecuencias más graves para su Servicio Nacional de Salud la cancelación de las citas de 7.000 pacientes, retrasando la atención médica de 139 personas aquejadas de patologías tan graves como el cáncer. Hubo que cancelar también operaciones ya programadas y derivar pacientes a instalaciones de emergencia alternativas. En sentido más amplio, WannaCry[41] produjo daños a más de 360.000 dispositivos electrónicos de más de 180 países, afectando también a prestigiosas empresas privadas españolas e internacionales. Después del ataque, quedó claro que era necesario desarrollar e implementar una estrategia de ciberseguridad para proteger los elementos más vulnerables y esenciales del sistema de salud como medio para proteger a los pacientes de las nuevas modalidades delictivas. Esto no ha impedido que, ya iniciado 2020, la OMS y distintas instituciones sanitarias alrededor del mundo se convirtiesen en el blanco de ciberataques, en lo que cierto sector de la opinión pública ha interpretado como un intento de disminuir su capacidad de

escena internacional, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2019, pp. 23 – 31. Sirvan como ejemplo los ciberataques a Estonia en el año 2007 después de retirarse en Tallin un monumento dedicado al ejército rojo soviético, los intentos de aislar internacionalmente a Georgia durante su invasión en 2008, o el ciberataque NotPetya en Ucrania en 2017.

[39] R. Chelala Riva, "La nueva delincuencia cibernética", en J. Andújar Urrutia y J.A. Tuero Sánchez (coords.), *Actualidad Penal 2017,* Valencia, Tirant lo Blanch, 2017, pp. 321 – 342. Los criminales tienen en cuenta esta circunstancia, y hay que dar por hecho que se valdrán de ella para desarrollar nuevas formas de delitos.

[40] G. Martin et al., "WannaCry - A year on", *The BMJ,* vol. 361, 2018, p. 1. El ataque evidenció que era necesario no solo invertir más en ciberseguridad, sino cambiar la mentalidad en relación con la misma.

[41] E. Velasco Núñez y C. Sanchís Crespo, *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015,* 1ª ed., Valencia, Tirant lo Blanch, 2019, pp. 253 – 259. Rusia se contó entre los países más afectados por el ataque del *ransomware* WannaCry.

respuesta ante las emergencias más graves. El problema, por lo tanto, continúa existiendo en la actualidad.

También en 2017, un *hacker*[42] consiguió acceder a un servidor del Ministerio de Justicia de España y obligó a detener la actividad de LexNET, el sistema de gestión de notificaciones telemáticas de la Administración de Justicia española que conecta los juzgados con los profesionales de la justicia, así como con los abogados y los procuradores. Un fallo de seguridad permitió que el *hacker* tuviese acceso de manera incontrolada a los expedientes de distintos casos judiciales, desde grandes causas de interés nacional hasta pequeños pleitos. La AEPD abrió un expediente y determinó que había habido una infracción grave por parte del Ministerio de Justicia de acuerdo con la LOPD[43]. A pesar de esto, al no poder ser sancionadas económicamente las Administraciones Públicas, no pudo imponerse la correspondiente multa. No se condenó, tampoco, a ninguna persona física por el acceso a los expedientes, incluso teniendo en cuenta que el CP recoge como conducta típica en su art. 197 bis 1 el mero acceso por cualquier medio o procedimiento a parte de un sistema de información. Si a casos como este añadimos la voluntad de avanzar en el uso y consolidación de la prueba digital[44] en los tribunales, queda claro que la ciberseguridad es un asunto

[42] En el original citado, se afirma que un *hacker* fue quien realizó la conducta prohibida. Aunque en español existe una tendencia a confundir ambos términos, *hacker* y *cracker* tienen significados distintos que resulta indispensable conocer si se pretende abordar un asunto desde una perspectiva penal. Y es que el *hacker,* en el ámbito anglosajón, es solo una persona con grandes habilidades en el manejo de ordenadores que investiga un sistema informático para avisar de los posibles fallos existentes con objeto de facilitar la elaboración de técnicas de mejora. Es posible, incluso, contratar a esta clase de personas para que lleven a cabo dicho cometido. En español, en cambio, se identifica automáticamente al *hacker* con la piratería informática, cuando esta categoría corresponde al *cracker*, quien accede siempre con fines delictivos a los sistemas informáticos ajenos para apropiárselos u obtener información secreta. Por todo lo anterior, utilizaré el término *cracker*, y no *hacker,* cuando los actos de una persona tengan como objetivo cometer un delito.

[43] La resolución se basó en el art. 44.3.d de la antigua LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Esta norma está actualmente derogada al haber sido sustituida por la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

[44] M. Barrio Andrés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos,* 1ª ed., Madrid, Wolters Kluwer, 2018, p. 225. La *e-evidence* o prueba digital, en el contexto de una adecuada legislación comunitaria, agilizaría y aseguraría la

prioritario que puede tener profundas repercusiones para la Administración de Justicia, tanto en lo que respecta a la seguridad de sus propias redes informáticas como a la seguridad de unas actuaciones policiales y judiciales cada vez más digitalizadas.

La defensa del ciberespacio, el ámbito virtual creado por medios informáticos, ha crecido tanto en importancia que las ciberamenazas y los ciberataques ocupan un lugar destacado en las nuevas agendas de seguridad nacional y defensa[45]. Su protección supone un desafío a nivel internacional que requiere una sólida colaboración entre países y la realización de ajustes a nivel nacional[46]. El riesgo de ataques cibernéticos a gran escala se estima superior al promedio de otros riesgos, pudiendo suponer tanto un grave daño a infraestructuras críticas, como las sanitarias, como el germen de un conflicto que afecte a la convivencia pacífica entre naciones. Por esto, los principales países occidentales han desarrollado una legislación orientada a prevenir y sancionar conductas delictivas, pero también a neutralizar ciberamenazas o ciberataques a su seguridad nacional. En cualquier caso, de lo que no cabe duda es de que, a causa del deber de gestionar este riesgo tecnológico, los ciberdelitos, entre los que se encuadran los delitos que afectan a la ciberseguridad, son una de las mayores preocupaciones internacionales en el campo de la legislación penal.

En consecuencia, y atendiendo a la trascendencia de los delitos que afectan a la ciberseguridad y a la manera en que han comprometido tanto al

---

recogida de correos electrónicos, mensajes de texto o datos almacenados en la nube, entre otros materiales informáticos, por parte de las autoridades policiales y judiciales de un Estado miembro, pudiendo presentarlas después en un proceso penal transnacional. Por las graves consecuencias para las personas implicadas que podría tener su alteración o su destrucción, es necesario garantizar la seguridad de dichas pruebas antes de implementar un sistema de este tipo.

[45] D. Fernández Bermejo y G. Martínez Atienza, *Ciberseguridad, Ciberespacio y Ciberdelincuencia,* Cizur Menor, Navarra, Aranzadi, 2018, pp. 126 – 127. Gestionar de manera estratégica la información científico-tecnológica es fundamental para innovar y sobrevivir en un entorno complejo sometido a continuos cambios.

[46] J.J. Piernas López, *Ciberdiplomacia y ciberdefensa en la Unión Europea*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2020, p. 52. Y es que la seguridad nacional, muy relacionada con la ciberseguridad, es responsabilidad de los Estados miembros, como establece el art. 4.2 del Tratado de la Unión Europea.

mundo del derecho como al de la medicina, y con la intención de proteger muy especialmente los derechos de los pacientes, esta investigación se centrará, desde la perspectiva del Derecho penal, en un análisis crítico de los mismos a nivel internacional, con especial mención al ámbito sanitario.

Se trata de una investigación documental o teórica, para la cual he recopilado datos de fuentes documentales (principalmente libros y artículos, por considerarlos más fiables). Mi propósito, mediante una exposición ordenada de los antecedentes documentales, es profundizar en las leyes, teorías y conceptos existentes para, sobre las mismas, realizar mis propias aportaciones intelectuales. Además de la guía en materia penal del director del Grupo de Investigación Cátedra de Derecho y Genoma Humano y de los materiales disponibles en la biblioteca de la Universidad del País Vasco (UPV/EHU), mis estancias de investigación en la Universidad de Oxford (Inglaterra) y la Universidad de Melbourne (Australia) me han permitido ampliar los datos sobre Derecho internacional, comunitario y comparado, y contraponer mis ideas con especialistas de distintas partes del mundo.

La investigación, después de esta introducción orientada a conceptualizar la seguridad, la ciberseguridad y relacionar esta última con el Derecho penal y, por último, realizar una breve descripción del objetivo a conseguir y del *status quaestionis* en la práctica, así como de la metodología empleada y de su estructuración, se divide en cuatro capítulos. El primero es el resultado del innegable carácter internacional[47] [48] de la ciberseguridad: se

[47] J. Matusitz, "Postmodernism and Networks of Cyberterrorists", *Journal of Digital Forensic Practice,* vol. 2, no. 1, 2008, pp. 17 – 26. La internacionalización de la tecnología no solo facilita la comisión de ciberdelitos, sino que también ha afectado a la manera en que se organizan quienes los cometen. De estructuras jerarquizadas y con una verticalidad muy marcada se ha pasado a organizaciones sin un núcleo concreto.

[48] M.R. Torres-Soriano, "Cómo contener a un califato virtual", *Cuadernos de estrategia,* no. 180, 2016, pp. 170 – 171. La capacidad del Estado Islámico para difundir propaganda en todo tipo de formatos a nivel internacional no conoce parangón en la historia. Solo en una semana de 2015, distribuyó ciento cuarenta y un productos propagandísticos. Para valorar como corresponde esta cifra hay que tener en cuenta que entre los años 2000 y 2014 Al Qaeda, por su parte, había difundido ya seiscientos veintiocho videos. De continuar esta progresión, dentro de diez años los representantes del islam radical podrían producir y distribuir a nivel internacional casi veinte mil videos, con nefastas consecuencias para la seguridad mundial.

trata de un análisis del Derecho internacional y de la UE en relación con la misma, con objeto de obtener una visión más amplia y entender cómo la legislación penal actual se ha visto influenciada por estas normas de rango superior, y cómo podrían afectar a los futuros tipos delictivos creados para garantizar la ciberseguridad de las nuevas tecnologías sanitarias. El segundo capítulo pretende enriquecer la exposición posterior sobre Derecho penal español comparándolo, donde resulte posible y apropiado, con la legislación penal de Reino Unido, Estados Unidos de América, Canadá, Australia, Nueva Zelanda, Suiza y la Federación de Rusia. El tercer capítulo analiza de manera genérica los delitos que afectan a la ciberseguridad en el Derecho penal español teniendo en cuenta su notable aumento en España[49] [50], donde, solo en 2018, se registraron 2.750 delitos dentro de la categoría de acceso e interceptación ilícita. El cuarto capítulo introduce de lleno un elemento sanitario[51] ya insinuado en el tercero y, manteniendo el Derecho penal y la

[49] Ministerio del Interior de España, *Estudio sobre la cibercriminalidad en España 2018,* Madrid, Ministerio del Interior de España, 2019, p. 42. La progresión es al alza: en 2015 se registraron 2.386 delitos de acceso e interceptación ilícita. En 2016, 2.579, y en 2017, 2.505. En el último año sobre el que el Ministerio del Interior ha publicado datos, 2018, se registraron 2.750 delitos dentro de esta categoría, un 2,5% del total.

[50] C.J. Del Canto Masa, "Ciberseguridad, una cuestión prioritaria", *Cuadernos de energía,* no. 56, 2018, p. 49. En 2017, el INCIBE gestionó un total de 123.064 incidentes de seguridad, un 6,77% más de los registrados en 2016. De acuerdo con los resultados del propio INCIBE en su informe Instituto Nacional de Ciberseguridad de España, *Balance de ciberseguridad 2018,* León, Instituto Nacional de Ciberseguridad de España, 2019, p. 2, en 2018, la cifra de incidentes de seguridad gestionados descendió hasta los 111.519. El informe del Instituto Nacional de Ciberseguridad de España, *Balance de ciberseguridad 2019,* León, Instituto Nacional de Ciberseguridad de España, 2020, p. 2 acusó un descenso aún mayor de los mismos durante el año 2019, bajando su número hasta los 107.397. Esta tendencia se vio abruptamente interrumpida en 2020, puesto que tal y como refleja el informe del Instituto Nacional de Ciberseguridad de España, *Balance de ciberseguridad 2020,* León, Instituto Nacional de Ciberseguridad de España, 2021, p. 2, los incidentes de seguridad gestionados durante dicho año se dispararon hasta llegar a los 133.155, superando así en más de diez mil a la ya de por sí elevada cifra de incidentes correspondiente a 2017. La última fuente de información disponible, el *Balance de ciberseguridad 2021*, León, Instituto Nacional de Ciberseguridad de España, 2022, p.2, evidenció un notable descenso en los incidentes de seguridad gestionados durante el año 2021, cuyo número fue de 109.126, una cifra más parecida a la del año 2019.

[51] G. Martin, J. Kinross y C. Hankin, "Effective cybersecurity is fundamental to patient safety", *The BMJ,* vol. 357, 2017, p. 1. El ataque del *ransomware* WannaCry en 2017, pese a haber paralizado la actividad de numerosos servicios sanitarios a nivel mundial, podría haber sido mucho peor de haber estado orientado a la alteración o eliminación de datos. Es necesario reducir la vulnerabilidad de los sistemas sanitarios frente a esta

ciberseguridad como columna vertebral, me sirve para relacionar estos con los hospitales[52], los centros de salud y las tecnologías sanitarias emergentes, siendo quizá el más especulativo sin que esto signifique en ningún momento abandonar las sólidas bases científicas de los anteriores. Se trata, en efecto, de un estudio sobre Derecho penal y ciberseguridad en relación con las tecnologías sanitarias emergentes[53], como la IA, la robótica, los drones, los hospitales inteligentes, el IdCM, o la salud electrónica, analizando la existencia de tipos delictivos adecuados a las mismas o la hipotética necesidad de adaptar el Derecho penal español a estas nuevas tecnologías[54].

clase de ataques, siendo el Derecho penal fundamental para su prevención y persecución.

[52] Ministerio de Defensa de España, *El ciberespacio. Nuevo escenario de confrontación,* Madrid, Ministerio de Defensa de España, 2012, p. 57. Como infraestructura crítica, las actividades en el ciberespacio del sector de la salud merecen especial protección contra ataques deliberados físicos o cibernéticos, ya se esté utilizando para la gestión interna, para la provisión de servicios o para su vinculación con otros sistemas.

[53] T. Shryock, "The growing cyber threat to physician practices", *Medical Economics,* vol. 96, no. 10, 2019, p. 24. Una de las mayores amenazas para la ciberseguridad son los dispositivos médicos conectados a Internet, que forman parte del IdC. La gama de productos conectados va desde equipamiento sanitario (como el IdCM que analizaré en el capítulo cuarto) a termostatos. Aunque muchos de ellos almacenan datos igual que los ordenadores, no se suele poner el mismo cuidado en su seguridad. A esto hay que añadir que, mientras que los equipos informáticos suelen cambiarse cada pocos años, los dispositivos médicos se utilizan, en ocasiones, durante más de una década, de manera que, sin importar el esfuerzo que se ponga en garantizar su ciberseguridad, los dispositivos obsoletos pueden suponer un riesgo por sí mismos.

[54] R. Bermejo García y E. López-Jacoiste Díaz, *La ciberseguridad a la luz del Jus ad Bellum y del Jus in Bello,* 1ª ed., Pamplona, Ediciones Universidad de Navarra, 2020, p. 63. Se considera que, por sus características, la regulación a nivel internacional de ciertas tecnologías será especialmente compleja.

CAPÍTULO I

LA CIBERSEGURIDAD EN EL DERECHO PENAL INTERNACIONAL Y DE LA UNIÓN EUROPEA

1.1 Génesis del Derecho penal de la ciberseguridad: antes de los grandes acuerdos internacionales

Las primeras reivindicaciones libertarias en relación con Internet[55] pronto se vieron eclipsadas por el debate sobre la naturaleza jurídica del ciberespacio y sobre la necesidad de desarrollar una normativa adecuada que garantizase los derechos de sus usuarios[56].

En los primeros tiempos de la Red existió, no obstante, una admirable línea de pensamiento que defendió que el Estado debía alejarse del ciberespacio por considerarlo el último reducto de libertad auténtica y real, y que, además de estar abierto a todos, la propia Red podría autorregularse con mejores resultados de los que hubiese podido conseguir cualquier ente externo, ya fuese público o privado[57]. Quienes la defendían, lejos de proponer

[55] A. Rutkowski, "Public international law of the international telecommunication instruments: cyber security treaty provisions since 1850", *Info,* vol. 13, no. 1, 2011, pp. 13 – 22. Antes de la existencia de Internet, las naciones occidentales, mediante la UIT, llevaban ya desde el año 1850 regulando la seguridad de las comunicaciones a través de las innovaciones tecnológicas de cada época, como el telégrafo o la radio.

[56] A. Segura Serrano, "Ciberseguridad y Derecho Internacional", *Revista española de derecho internacional,* vol. 69, no. 2, 2017, pp. 291 – 292. Aunque al principio parte de la doctrina era reticente a ello, en la actualidad el ciberespacio se configura como un ámbito sujeto al Derecho internacional. No obstante, no se ha avanzado mucho en la adopción de normas convencionales en relación con el mismo. El origen de este problema no es jurídico, sino político. Y es que ciertos países y gigantes tecnológicos se niegan a avanzar en la regulación internacional de Internet por motivos estratégicos, ya que se benefician de la aplicación analógica de las normas generales de Derecho internacional. Las organizaciones internacionales avanzan, por lo tanto, hacia una cooperación internacional de carácter asistencial para hacer frente al cibercrimen.

[57] M. Castells, *La Galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*, 1ª ed., Madrid, Areté, 2001, p. 31. En opinión de Castells, el origen de Internet se encuentra en la encrucijada entre la gran ciencia, la investigación militar y la cultura libertaria. En cuanto a este último concepto, Castells utiliza la acepción europea del mismo asociándolo a una cultura de la libertad, puesto que en Europa se entiende como una cultura o ideología basada en la defensa a ultranza de la libertad individual entendida como valor supremo.

una indeseable anarquía, eran partidarios del derecho, pero de un verdadero derecho hecho por las personas en su beneficio[58]. Por desgracia, la realidad se impuso, e Internet pronto estuvo regulado por cada vez más normas, materializando la máxima *ubi societas, ibi ius*[59].

A pesar de que los diferentes países llegaron a conclusiones distintas en relación con la ciberseguridad, incluso en lo que se refería a su definición, coincidieron en que se trataba de un interés común compartido por todos[60]. Esto se debió no tanto a la suma de los intereses de cada país como a la notoria intersección existente entre los mismos. A pesar de que la ciberseguridad llegó a considerarse como fundamental para garantizar la paz en el mundo, la actuación tanto a nivel nacional como internacional fue lenta y progresiva, muy ligada a los acontecimientos y necesidades de cada momento. Antes de la misma, hubo un periodo en que el avance de la tecnología fue muy por delante del desarrollo del derecho. Se ha llamado a este periodo prehistoria de la ciberseguridad[61], por corresponder a un tiempo en que la revolución de la informática ya había comenzado, pero todavía no existía una legislación que regulase los delitos que afectan a la

---

[58] M. Barrio Andrés, *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet,* 1ª ed., Valencia, Tirant lo Blanch, 2018, pp. 42 – 60. A pesar de todo, ya existían inquietudes en relación con su utilización, como el miedo a una invasión sistemática de la privacidad.

[59] I. Álvarez Rodríguez, "Constitución y Derecho del Ciberespacio", en C. Mallada Fernández (dir.), *Nuevos Retos de la Ciberseguridad en un Contexto Cambiante*, Cizur Menor, Navarra, Aranzadi, 2019, p. 36.

[60] M.C. Kettemann, "Ensuring Cybersecurity through International Law", *Revista española de derecho internacional,* vol. 69, no. 2, 2017, pp. 283 – 284. El ataque del *ransomware* WannaCry en 2017 demostró la desorganización existente, puesto que informes posteriores determinaron que podría haberse evitado si se hubiesen adoptado precauciones de seguridad básicas. En ausencia de una adecuada regulación, las instituciones no pudieron prever ni enfrentarse al ataque, lo que evidenció la necesidad de desarrollar una.

[61] M. Warner, "Cybersecurity: A Pre-History", *Intelligence and National Security,* vol. 27, no. 5, 2012, p. 781. Al mencionar que incluso las personas que no poseían un ordenador personal corrían el riesgo de ser víctimas de delitos que afectan a la ciberseguridad, se pone de manifiesto el cambio que ha habido en apenas unas décadas no solo a nivel legislativo, sino de expansión del uso de la tecnología, ya que hoy resulta imposible realizar una distinción entre un sector de la población que tenga acceso a los ordenadores y otro que no lo tenga. Para bien o para mal, se ha generalizado el acceso a los mismos gracias a la tecnología vía satélite, al mismo tiempo que se ha generalizado también el uso de un Internet omnipresente.

ciberseguridad. El mundo sufrió profundos cambios derivados de la misma: semiconductores microscópicos otorgaron a millones de personas un poder para procesar la información con el que ni siquiera se hubiese podido soñar cien años antes, e hicieron posible una comunicación interpersonal casi instantánea.

No obstante, al mismo tiempo, aumentó de manera proporcional la vulnerabilidad de las redes informáticas y sus usuarios. Los *crackers* eran capaces de causar daños amparándose en el anonimato gracias a la utilización de técnicas de control remoto y automatizadas. Los titulares en la prensa se hacían eco continuo de nuevos ataques contra intereses sensibles pertenecientes al sector público o a las empresas privadas. Internet se llenó tanto de empresas como de estafadores que informaban sobre las nuevas modalidades delictivas, ofreciendo sus propias soluciones. Con el paso del tiempo, hubo un cambio en relación con la percepción de los ciberdelitos: en la década de los sesenta, se comenzó a plantear la posibilidad de que un ciberataque se tradujese en una fuga de información y, por lo tanto, se llegó a la conclusión de que las redes informáticas debían ser protegidas; en la década de los setenta, se reafirmó la idea de que las redes informáticas podían ser atacadas y la información sustraída; en las décadas de los ochenta y los noventa, se vislumbró la posibilidad de realizar ciberataques dirigidos contra arsenales militares de terceros países y, por último, en la década de los noventa se comprendió que si existía la posibilidad de realizar esta clase de ciberataques, también debía existir la posibilidad de recibirlos[62].

Esto no pasó desapercibido para el Gobierno federal de los Estados Unidos. Los ordenadores comenzaron a conectarse a través de redes a principios de la década de los sesenta. En aquel tiempo, la mayoría de los estadounidenses nunca habían visto uno, y además de ser físicamente grandes, caros y de suponer un enorme gasto de energía, requerían personal especializado que los manejase. Por este motivo, requerían una habitación separada o instalaciones propias, y sus dueños los alquilaban a empresas o

[62] Warner, “Cybersecurity: A Pre-History”, p. 782.

investigadores que necesitaban utilizarlos pero no podían permitirse adquirir uno. Lo más parecido a la ciberseguridad era el *software* desarrollado de manera que impidiese a un usuario acceder a datos pertenecientes a otro. La NSA manifestó su preocupación por la seguridad, pero las investigaciones de uno de sus miembros, Bernard Peters, respaldadas por el también miembro de la NSA Willis H. Ware, determinaron que no podía haber seguridad absoluta en un sistema de multiprogramación equipado con terminales remotos, y que la introducción de información sensible en el sistema conllevaría siempre un riesgo. El usuario debía ser consciente del riesgo inherente a su uso y asumir la posible filtración[63].

En 1967, el número de técnicos con acceso a la información almacenada en los ordenadores había crecido exponencialmente y, con ello, también crecieron las posibilidades de delinquir. En 1968, la policía de Alemania Occidental detuvo a un espía de Alemania Oriental en la filial alemana de IBM, en lo que se podría considerar el primer caso en el mundo de espionaje a través de la informática. La década de 1970 trajo consigo numerosas innovaciones orientadas a mejorar la seguridad, como los privilegios de administrador o la encriptación de los datos que circulaban entre ordenadores. En los años ochenta, las redes informáticas se extendieron a nivel mundial, al igual que lo hicieron los virus informáticos y el *hacking*. El principal problema residía en que los datos podían no solo robarse, sino también manipularse para hacer actuar a los sistemas de manera confusa y, en ocasiones, peligrosa. Como consecuencia de la preocupación que esto provocó entre los altos cargos gubernamentales, quienes sabían que la cantidad de información clasificada almacenada en ordenadores era muy elevada, la integridad de los datos pasó a ser otro elemento a tener en cuenta para la ciberseguridad. Aunque en aquel tiempo no se tenían pruebas de espionaje informático por parte de los soviéticos, las intrusiones originadas

[63] Warner, “Cybersecurity: A Pre-History”, pp. 782 – 783.

en el propio territorio estadounidense ya resultaban lo suficientemente preocupantes[64].

En 1983, un agente especial del FBI expuso que algunos *crackers* pasaban doce horas diarias intentando acceder a los ordenadores de la CIA y del Pentágono, y que tenían un profundo interés en los sistemas del ejército de Estados Unidos. Al año siguiente, se publicó la Decisión Directiva de Seguridad Nacional (NSDD) 145, que encargó a la NSA el establecimiento de estándares y la dirección, así como la investigación y la monitorización parcial de todos los sistemas gubernamentales de información automatizados y de telecomunicaciones. La motivación detrás de la misma fue que mucha información considerada sensible estaba al alcance de los enemigos del país, algo que quedó demostrado cuando, en 1986, un administrador de sistemas detectó a un grupo de *crackers* de Alemania Occidental pagados con dinero y drogas por el KGB para que accediesen a la red del DOD. A raíz de las críticas por la excesiva intervención del ejército en este ámbito, la Ley de Seguridad Informática de 1987 disminuyó la influencia de la NSA, aunque esta continuaría defendiendo las redes relacionadas con la seguridad nacional. En julio de 1990, se implementó la Directiva Nacional de Seguridad (NSD) 42, "Política Nacional de Seguridad de Seguridad Nacional de Telecomunicaciones y Sistemas de Información" que, aunque no respondió a las preocupaciones sobre la monitorización de Internet por parte del ejército y los servicios de inteligencia ni resolvió los problemas de seguridad de las redes informáticas gubernamentales, estableció un consenso sobre las crecientes ciberamenazas existentes[65].

Aunque ya se había oído hablar del *malware* autorreplicable conocido como gusano Morris en 1988, fue el virus Michelangelo de principios de 1991, junto al primer ataque DoS conocido por el público en la Nueva York de 1996, lo que hizo que la importancia de la ciberseguridad calase en una sociedad

[64] Warner, "Cybersecurity: A Pre-History", pp. 784 – 787.
[65] Warner, "Cybersecurity: A Pre-History", pp. 787 – 789.

que ya se estaba incorporando[66] a Internet a través de la adquisición de ordenadores personales que incluían el sistema operativo Windows.

De acuerdo con la opinión de ciertos oficiales y asesores del Gobierno de Estados Unidos, las infraestructuras críticas, que incluían el sector sanitario, también se encontraban en grave riesgo a mediados de la década de 1990. La posibilidad de que individuos o países hostiles manipulasen datos para destruir infraestructuras críticas estadounidenses suponía una preocupación tan grande que el DOD encargó unos ejercicios que tuvieron lugar entre enero y junio de 1995, gracias a los cuales se puso de manifiesto que era posible devastar infraestructuras críticas en territorio de Estados Unidos desde el extranjero mediante ataques contra sus redes informáticas. Las redes del DOD también sufrieron los mismos problemas que comenzaban a ser una plaga en el Internet utilizado por los civiles: el DOD informó de que recibía unos 250.000 ataques diarios que, en el mejor de los casos, suponían un gasto multimillonario y, en el peor, una seria amenaza para la seguridad nacional[67]

El rápido crecimiento del número de personas con conocimientos informáticos conllevó que cada vez más individuos poseyesen las habilidades necesarias para ejecutar esa clase de ataques. Los ciberataques pasaron de estar reservados a expertos a ser algo común y corriente que podía llevarse a cabo con un ordenador o un teléfono conectados a Internet. En ese escenario, y habiendo quedado claro que las soluciones apresuradas y simplistas, aunque brevemente satisfactorias, no solo resultaron ineficaces, sino que empeoraron los problemas[68], era necesario el desarrollo de una adecuada legislación internacional. No obstante, antes de entrar a analizarla,

---

[66] S. Landau, *Listening in Cybersecurity in an Insecure Age,* 1ª ed., New Haven, Yale University Press, 2017, pp. 50 – 51. Históricamente, los primeros ciberataques consistieron en la sustracción de secretos militares y en arrogantes demostraciones por parte de los criminales de sus habilidades informáticas. Sin embargo, a medida que las personas y las empresas añadían más y más datos a sistemas accesibles a través de Internet, la naturaleza de los ciberataques cambió, y el robo de información con fines criminales adquirió un cariz más serio, puesto que la revolución digital dio lugar a la posibilidad de cometer nuevos tipos de delitos.

[67] Warner, “Cybersecurity: A Pre-History”, pp. 794 – 795.

[68] Warner, “Cybersecurity: A Pre-History”, pp. 797 – 799.

creo conveniente, para adquirir una perspectiva más completa, repasar los principales ataques internacionales contra la ciberseguridad que tuvieron lugar durante estos años, así como la aproximación legislativa inicial a los mismos que llevó a cabo el Consejo de Europa al otro lado del océano atlántico.

1.1.1 Ataques históricos contra la ciberseguridad

En la década de 1980, destacan los casos de Kevin Mitnick, consistente en el robo de correos electrónicos privados, *software* utilizado para el control de teléfonos móviles y varias herramientas de seguridad informáticas, así como ciberataques dirigidos contra los principales sistemas informáticos corporativos de Estados Unidos; los 414, que pusieron en peligro los sistemas informáticos de numerosas instituciones de alto perfil, como el Memorial Sloan Kettering Cancer Center de Nueva York; la *Legion of Doom*, considerada durante un tiempo como el mejor grupo de *hackers* a nivel mundial; el *Chaos Computer Club,* la asociación de *hackers* más grande de Europa, capaces de reconstruir las huellas dactilares de sus víctimas a partir de fotografías de sus dedos efectuadas desde el ángulo adecuado; *Fry Guy*, quien se hizo con la contraseña del sistema informático del restaurante donde trabajaban algunos de sus amigos y, una vez hubo accedido, aumentó sus salarios; Fred Cohen, figura esencial para distinguir los *hackers* de los *crackers*, toda vez que sus investigaciones sobre virus informáticos ha sido utilizada dentro de la legalidad para desarrollar sistemas de defensa frente a los mismos; y el ya mencionado gusano Morris de 1988, que fue el primero en atraer la atención de los medios de comunicación y tuvo un gran impacto en la percepción de los usuarios de la fiabilidad y la seguridad de Internet[69].

[69] B. Middleton, *A History of Cyber Security Attacks: 1980 to Present,* 1ª ed., Boca Raton, FL, CRC Press, 2017, pp. 3 – 35. Al igual que sucede en lugares físicos como los domicilios privados, es imposible garantizar la seguridad total en el ciberespacio. Por eso, lo importante es que existan profesionales capaces de investigar los delitos cometidos en el mismo, y disponer de una legislación adecuada que facilite dicha tarea.

En la década de 1990, fueron notorios los casos de Nahshon Even-Chaim (o *Phoenix*), especializado en accesos indebidos a redes de investigación sobre armas nucleares y defensa; los *Masters of Deception* neoyorquinos, detenidos por explotar la infraestructura de una compañía telefónica como medio para obtener sus fines; la operación *Sun Devil*, que permitió la detención de grupos de *hackers* repartidos a lo largo de toda la geografía estadounidense, especialmente en Arizona; el caso de la Base de la Fuerza Aérea Griffiss y el Instituto de Investigación Atómica de Corea, en el que hubo más de ciento cincuenta intrusiones; Ehud Tenenbaum, detenido junto a sus cómplices por acceder a los sistemas informáticos de distintas instituciones financieras para robar números de tarjetas de crédito y por ponerlos después a la venta en Internet; la hermandad de Warez, que hizo caer la página web de la corporación de radiotelevisión pública de Canadá, sustituyéndola por un mensaje que afirmaba que los medios de comunicación son unos mentirosos[70].

El último de los grandes casos previos a la existencia de un gran tratado internacional en materia de ciberdelincuencia fue el de Michael Calce, alias *Mafiaboy*, quien, en febrero del año 2000, llevó a cabo numerosos ataques DoS contra objetivos muy conocidos, como la compañía multinacional estadounidense Dell Inc. La CIA hizo una lectura positiva de los mismos, ya que ayudaron a evidenciar las profundas carencias de seguridad existentes en aquella época, lo que tuvo como resultado un incremento en la preocupación del Gobierno federal de los Estados Unidos por la seguridad en Internet durante los diez años siguientes[71].

1.1.2 Los instrumentos jurídicos no vinculantes: las recomendaciones del Consejo de Europa

Hay que tener en cuenta que las recomendaciones no son vinculantes, solo permiten a las instituciones exponer sus puntos de vista y sugerir una

[70] Middleton, *A History of Cyber Security Attacks*, pp. 39 – 66.
[71] Middleton, *A History of Cyber Security Attacks*, pp. 69 – 70.

determinada línea de actuación. No obstante, no solo no imponen obligación legal alguna, sino que pueden no tener ninguna consecuencia legal. Sí son útiles como documentos históricos que permiten analizar la perspectiva con la que el Consejo de Europa, la organización internacional de ámbito regional que tiene como objetivo promover la configuración de un espacio político y jurídico común en el continente mediante la cooperación de los países europeos, se aproximó de manera inicial a la ciberseguridad entre los años 1981 y 1995, al mismo tiempo que en Estados Unidos tenía lugar el desarrollo legislativo ya descrito. La Recomendación no. R (81) 12 sobre criminalidad económica incluyó el 25 de junio de 1981 una sucinta referencia sobre los ciberdelitos (en aquel entonces, aún crímenes informáticos) en el apartado cuarto de su único apéndice, enumerando entre los mismos el robo de datos, la violación de secretos y la manipulación de datos informatizados. En una nota al pie de página, se matizó que solo habría que tenerlos en consideración en circunstancias específicas, como cuando provocasen o supusiesen un riesgo de provocar pérdidas considerables. El acceso todavía limitado a la informática de la época podría ser una explicación a este matiz. Aunque la presencia de los ciberdelitos en la misma sea aún anecdótica, esta Recomendación supuso una primera invitación a los gobiernos de los Estados miembros a la colaboración y a la armonización de las distintas legislaciones estatales con objeto de coordinar esfuerzos.

La Recomendación no. R (89) 9 sobre criminalidad informática de 13 de septiembre de 1989 fue sucinta y directa: después de reconocer la importancia de una respuesta adecuada y rápida al nuevo desafío de la criminalidad informática, y teniendo en cuenta su carácter habitualmente transfronterizo, y con afán de mejorar la cooperación internacional en materia legal, hizo dos recomendaciones a los gobiernos de los Estados miembros. La primera, que tuviesen en cuenta, al revisar la legislación existente o introducir leyes nuevas, el informe sobre criminalidad informática elaborado por el CEPC del Consejo de Europa que se publicaría en Estrasburgo en 1990, sobre todo las directrices para los legisladores nacionales. En las mismas, se incluyó un listado de actos que deberían o podrían ser objeto de

sanción penal[72], como el fraude en el campo de la informática, la falsificación en materia informática, los daños causados a datos o programas informáticos, el sabotaje informático, el acceso no autorizado, la interceptación no autorizada, la reproducción no autorizada de un programa informático protegido y la reproducción no autorizada de una topografía. A las conductas anteriores se añadieron como opcionales actos que se recomendó incriminar siempre que se cometiesen de manera intencionada, como la alteración de datos o de programas informáticos, el espionaje informático, la utilización no autorizada de un terminal o de un programa informático protegido. Además, se postuló la sanción penal de otros abusos, como el tráfico de contraseñas obtenidas de forma ilegal y de otras informaciones que permitiesen el acceso no autorizado a sistemas informáticos, así como la distribución de virus. La segunda de las recomendaciones era la de informar al secretario general del Consejo de Europa sobre cualquier novedad en su legislación, jurisprudencia y colaboraciones legales internacionales en lo concerniente a crímenes informáticos.

El 11 de septiembre de 1995, se aprobó la Recomendación no. R (95) 13, relativa a los problemas de Derecho procesal penal conectados con las tecnologías de la información. Si la Recomendación no. R (89) 9 se había centrado en aspectos de Derecho penal sustantivo, esta abordó aspectos de Derecho procesal penal como los problemas de búsqueda y captura, la vigilancia técnica, la obligación de cooperar con las autoridades investigadoras, la prueba electrónica, el uso de encriptado, la investigación, estadísticas y formación y, por último, la cooperación internacional. No obstante, ambas recomendaciones destacaron la necesidad de crear un instrumento internacional de carácter formalmente vinculante[73] que se

[72] J.L. De la Cuesta Arzamendi y C. San Juan Guillén, "La cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad", en J.L. De la Cuesta Arzamendi (dir.), *Derecho Penal Informático*, Cizur Menor, Navarra, Aranzadi, 2010, pp. 59 – 60. La distribución de virus o de programas similares merece una atención especial por suponer la posible incriminación de la imprudencia o la creación de riesgos.

[73] J. Richet, *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*, 1ª ed., Hershey, PA, IGI Global, 2015, p. 228. Hasta la fecha, solo ha habido un tratado internacional que reúna estas características en el ámbito de la ciberdelincuencia: el Convenio sobre la Ciberdelincuencia de Budapest del año 2001.

centrase tanto en aspectos materiales como procesales e impulsase la cooperación internacional orientada a permitir las investigaciones conjuntas, así como a aplicar otros mecanismos de asistencia mutua en materia jurídica por parte de los Estados[74].

1.1.3 La necesidad de avanzar hacia la armonización legislativa internacional

Aunque los riesgos que conlleva el uso de la informática serán siempre inevitables[75], los ataques contra intereses nacionales y privados incrementaron el interés de los Estados en cooperar internacionalmente para ir más allá de las meras recomendaciones y desarrollar herramientas jurídicas[76] que garantizasen el mayor nivel posible de ciberseguridad[77].

La cooperación entre países fue, desde un punto de vista técnico, lo que permitió elaborar textos jurídicos mejores y más consistentes a ambos lados del atlántico. Esto es perceptible, incluso, desde un punto de vista léxico, puesto que a partir de las normas internacionales empezó a utilizarse la misma nomenclatura en relación con los ciberdelitos, permitiendo que juristas de distintos países encontrasen un denominador común que facilitó sus actividades tanto a nivel internacional como estatal[78]. La progresiva disminución de divergencias entre ordenamientos jurídicos conllevó una colaboración[79] cada vez más fluida, evitando el trabajo adicional innecesario.

---

[74] De la Cuesta Arzamendi y San Juan Guillén, *Derecho Penal Informático,* pp. 62 – 63.

[75] A. Kohnke, K. Sigler y D. Shoemaker, *Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework*, 1ª ed., Boca Raton, FL, CRC Press, 2017, p. 2.

[76] C. Zárate, "Hacia un marco normativo supranacional en materia de ciberseguridad", *Actualidad jurídica Aranzadi,* no. 916, 2016, p. 12. Estas herramientas debían vincular a los países que se adhiriesen a ellas.

[77] A. Carlini, "Ciberseguridad: un nuevo desafío para la comunidad internacional", *Bie3: Boletín IEEE,* no. 2, 2016, p. 961. Las organizaciones internacionales llevaron la iniciativa de la cooperación en este ámbito.

[78] W. Pierotti, "Cyber Babel: Finding the Lingua Franca in Cybersecurity Regulation", *Fordham Law Review,* vol. 87, no. 1, 2018, pp. 429 – 431. Hasta entonces, las barreras del lenguaje dificultaron dicha colaboración.

[79] A.M. Weber, "The Council of Europe´s Convention on Cybercrime", *Berkeley Technology Law Journal,* vol. 18, no. 1, 2003, pp. 427 – 428. Dada la naturaleza

Habiendo quedado claro que eran los poderes públicos los que debían establecer las normas para garantizar la defensa de los intereses de toda la ciudadanía[80], solo quedó escoger las herramientas legales adecuadas para construir normas robustas que se desarrollasen y evolucionasen junto a la ciberseguridad[81].

1.2 Derecho penal internacional

En el ámbito de la ONU[82], el texto pionero es el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos de 1977, o Manual de Tallin. Mediante el mismo, se buscó trasladar a la ciberguerra las normas y los principios que regían en los conflictos del mundo físico. Con posterioridad, en el año 2016, se desarrolló el Programa Global de Cibercrimen de la UNODC, que también cuenta con un Grupo de Expertos Gubernamentales sobre seguridad internacional en el ciberespacio desde 2015.

---

transnacional de los ciberdelitos, resulta fundamental la colaboración internacional. No obstante, antes de la existencia del Convenio sobre la Ciberdelincuencia de Budapest, era mucho más difícil que dos países, sobre todo si sus relaciones eran tensas previamente, colaborasen. En la primavera del año 2000, tuvo lugar una serie de ciberdelitos en territorio estadounidense. Cuando las autoridades de este país identificaron a dos sospechosos en Rusia, las autoridades rusas se negaron a colaborar con la investigación. A pesar de que los EE.UU. eran parte de unos cuarenta TAJM, la colaboración no fue posible. En la actualidad, Rusia no es un Estado parte del Convenio porque sus autoridades consideran, en un ejercicio de autonomía totalmente respetable, que una de las bases del tratado, la relativa a compartir información, viola su soberanía. No obstante, los países que han decidido convertirse en Estados parte han avanzado mucho en la colaboración internacional contra los ciberdelitos.

[80] N.A. Sales, “Privatizing Cybersecurity”, *U.C.L.A. Law Review,* vol. 65, no. 3, 2018, pp. 622 – 624.

[81] M. Finnemore y D.B. Hollis, “Constructing Norms for Global Cybersecurity”, *The American Journal of International Law,* vol. 110, no. 3, 2016, p. 477. Aunque la casuística hace necesario que sea así, merece atención la excesiva rapidez con la que se están desarrollando las normas en relación con la ciberseguridad.

[82] C. Henderson, “The United Nations and the regulation of cyber-security”, en N. Tsagourias y R. Buchan (eds.), *Research Handbook on International Law and Cyberspace,* Cheltenham, Edward Elgar Publishing, 2015, p. 490. Un marco regulatorio completo no puede desarrollarse únicamente en el seno de la ONU. De hecho, la propia ONU ha señalado los valiosos esfuerzos que ha llevado a cabo el Consejo de Europa.

Entre las decisiones aprobadas por la OSCE, por su parte, destacó la Decisión no. 1202, de 10 de marzo de 2016, relativa a las medidas para el fomento de la confianza destinadas a reducir los riesgos de conflicto dimanantes del uso de las TIC. A través de las mismas se intentó facilitar e impulsar la comunicación directa entre los equipos de respuesta nacionales de los 57 Estados miembros frente a los incidentes de ciberseguridad y, al mismo tiempo, proteger las infraestructuras críticas y fomentar el intercambio de buenas prácticas[83].

A pesar de la existencia de estas herramientas jurídicas, los graves problemas ocasionados por la ciberdelincuencia despertaron la preocupación de la comunidad internacional, la cual, tras analizar su importancia en dimensión y efectos se esforzó en armonizar una normativa jurídica internacional específica que regulase esta materia[84] [85].

1.2.1 El Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001

Este tratado internacional[86] constituyó la primera norma dirigida a regular internacionalmente los ataques criminales contra los sistemas de

[83] Barrio Andrés, *Delitos 2.0,* pp. 58 – 59.

[84] N.J. De la Mata Barranco y A.I. Pérez Machío, "La normativa internacional para la lucha contra la cibercriminalidad como referente de la regulación penal española", en J.L. De la Cuesta Arzamendi (dir.), *Derecho Penal Informático*, Cizur Menor, Navarra, Aranzadi, 2010*,* p. 123. Las aportaciones de los órganos internacionales constituyeron un primer referente en relación con los interrogantes jurídicos que planteaba el nuevo fenómeno criminal, y sirvieron de base para que, posteriormente, cada uno de los países que habían tomado parte en su redacción desarrollasen la cuestión en el ámbito del derecho interno.

[85] J. Clough, "The Council of Europe Convention on Cybercrime: Defining Crime in a Digital World", *Criminal Law Forum,* vol. 23, 2012, pp. 363 - 364. En la época en que el grupo de expertos se reunió para escribir el borrador del primer instrumento multilateral sobre ciberdelitos, la tecnología informática podía considerarse, con base en los criterios actuales, casi primitiva: enormes monitores, CD-ROM, y conexiones a Internet que tardaban más de un minuto en permitir al usuario acceder a la Red desde el momento en que lo solicitaba.

[86] N. Ganuza Artiles, "Situación de la ciberseguridad en el ámbito internacional y en la OTAN", *Cuadernos de estrategia,* no. 149, 2011, p. 171. Para que la respuesta ante los ciberataques sea efectiva, debe ser internacional, y para ello es vital consolidar, entre otras cosas, acuerdos de colaboración entre Estados.

ordenadores, redes o datos, englobando tanto la perspectiva del derecho sustantivo como la del procesal, e instaurando un modelo rápido y eficaz de cooperación internacional[87]. Incluye, en efecto, elementos tanto de Derecho penal internacional sustantivo como de Derecho procesal penal internacional[88]. No obstante, en lo referente al primero, hay que recalcar que se trata de un instrumento jurídico que se limita a enunciar preceptos generales para la lucha contra la delincuencia cibernética, pero sus disposiciones no son susceptibles de aplicación directa en los ordenamientos jurídicos de los Estados parte, que deberán elaborar sus propias normas internas a través de las cuales el tratado podrá considerarse operativo[89]. En efecto, el principio de legalidad exige, mediante la intervención del poder legislativo estatal, que se elabore una ley interna que incluya una descripción de los tipos penales y una determinación de sus respectivas consecuencias jurídicas antes de ser incorporados al ordenamiento jurídico español. No es posible introducir directamente las disposiciones del Convenio. Es decir que, a pesar de su indudable utilidad como instrumento para construir una política penal común que prevenga la criminalidad en el ciberespacio y mejore la cooperación internacional, el tratado se limita a enunciar unas normas generales para combatir la delincuencia cibernética, y sus disposiciones no son, en ningún caso, susceptibles de aplicación directa en los ordenamientos

[87] De la Cuesta Arzamendi y San Juan Guillén, *Derecho Penal Informático,* p. 63.

[88] A. Díaz Gómez, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest", *Revista electrónica del Departamento de Derecho de la Universidad de la Rioja* (*REDUR)*, no. 8*,* 2010, pp. 183 – 184. Para comprender en profundidad los textos legales relacionados con los delitos que afectan a la ciberseguridad, es necesario establecer una diferenciación entre el Derecho penal internacional sustantivo y el Derecho procesal penal internacional. El primero engloba a las normas sustantivas de Derecho penal que configuran los distintos tipos de ciberdelitos, la punición de conductas específicas que se consideran lesivas para ciertos bienes jurídicos relacionados con la delincuencia informática. El Derecho procesal penal internacional se refiere, por su parte, a los procedimientos que permiten hacer efectivo dicho Derecho penal internacional sustantivo, y se compone de las técnicas, medios, facultades y procesos orientados a lograr el efectivo cumplimiento de los distintos tipos delictivos que lo configuran. Para una cooperación internacional plena, es necesario regular ambos.

[89] De la Mata Barranco y Pérez Machío, *Derecho Penal Informático,* p. 124.

de los Estados parte, a quienes les corresponde la labor de desarrollar normas internas que hagan plenamente operativas sus disposiciones[90].

España firmó este tratado el 23 de noviembre de 2001, pero no lo ratificó hasta el 3 de junio de 2010, por lo que, aunque entró en vigor de forma general el 1 de julio de 2004, no lo hizo en territorio español hasta el 1 de octubre de 2010. En el apartado dedicado a declaraciones y reservas, se formuló una declaración sobre las particularidades a tener en cuenta para su aplicación en Gibraltar. El preámbulo del tratado incluye una excelsa declaración de intenciones, por cuanto expresa el interés de los Estados miembros del Consejo de Europa y de los demás Estados signatarios de aplicar, con carácter prioritario, una política penal común que permita proteger a la sociedad[91] frente a la ciberdelincuencia, tanto a través de la adopción de una legislación adecuada como del fomento de la cooperación internacional. Ante la preocupación por el riesgo de que las redes informáticas y la información electrónica se utilicen para la comisión de delitos y de que las pruebas relativas a los mismos se almacenen y transmitan a través de dichas redes, el preámbulo recoge la creencia de que una cooperación internacional reforzada en material penal rápida y operativa es la única manera de luchar de forma efectiva contra la ciberdelincuencia.

La definición genérica que desarrollé de la ciberseguridad, según la cual se trata de la cualidad de seguras de las redes y sistemas informáticos en las que están garantizadas la disponibilidad, la integridad y la confidencialidad, encaja a la perfección en este tratado, puesto que,

[90] N.J. De la Mata Barranco, "Delitos informáticos (contra sistemas y datos)", en J.L. De la Cuesta Arzamendi (dir.), *Adaptación del derecho penal español a la política criminal de la Unión Europea,* Cizur Menor, Navarra, Aranzadi, 2017, p. 224. La delincuencia asociada al uso de las TIC tiene un carácter transnacional que ha obligado a los Estados a dejar atrás la idea de frontera a la hora de aplicar sus regulaciones penales, así como a desarrollar medidas de coordinación y armonización a nivel comunitario para conseguir una normativa eficaz que evite que la criminalidad se traslade a países con una legislación menos severa.

[91] E. Wales, "Draft Council of Europe Cybercrime Convention Upsets Civil Rights Bodies"*, Computer Fraud & Security,* no. 12, 2000, p. 7. La Global Internet Liberty Campaign criticó duramente incluso el borrador del Convenio, basándose en que suponía otorgar demasiado poder a los gobiernos de los Estados parte.

continuando con el preámbulo, este asegura que el Convenio es necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de, entre otros, las redes informáticas, así como su abuso, a través de la tipificación de dichos actos, siempre de acuerdo a su definición en el tratado. Además de lo anterior, se señala en el preámbulo que es importante la asunción de poderes suficientes para luchar de forma efectiva contra los delitos mencionados facilitando su detección, investigación y sanción, ya sea a nivel nacional o internacional, así como el establecimiento de disposiciones que permitan una cooperación internacional que pueda considerarse rápida y fiable.

1.2.1.1 Derecho penal sustantivo

1.2.1.1.1 Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

1.2.1.1.1.1 Acceso ilícito

Dentro del capítulo segundo, que recoge las medidas que deberán adoptarse a nivel nacional, se encuadra la sección primera, dedicada al Derecho penal sustantivo. En la misma, el título primero incluye los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. El primero de ellos es el acceso ilícito que, en el art. 2, se define como el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Mientras que esta definición viene precedida de un mandato para los Estados parte de adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar este delito, se permite cierto margen de discrecionalidad en lo concerniente a que el mismo se cometa vulnerando medidas de seguridad[92], con la intención de obtener datos

[92] B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations,* 1ª ed., New York, NY, Oxford University Press, 2016, p. 108. Matices como este tienen una importancia enorme, toda vez que la mayoría de accesos de este tipo se basan en

informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático. Estos últimos aspectos, reitero, quedan al arbitrio de los Estados parte, que podrán incorporarlos a su ordenamiento o no hacerlo[93].

1.2.1.1.1.2 Interceptación ilícita

El art. 3 define la intercepción ilícita como la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. A decisión de las partes queda exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro.

1.2.1.1.1.3 Interferencia en los datos

Considero que este art. 4 permite establecer un patrón en la estructura de estos arts., toda vez que se componen, primero, de un mandato a los Estados parte en relación con la adopción de medidas legislativas y de otro tipo que resulten necesarias para tipificar ciertas conductas como delito en su derecho interno y, segundo, de una posibilidad para los Estados parte de exigir ciertas particularidades en relación con las mismas, siempre de acuerdo

---

la credulidad irresponsable de los usuarios o en la explotación de vulnerabilidades que no necesariamente conllevan la existencia de medidas de seguridad.

[93] El art. 7 del Convenio no. 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, estaba dedicado a la seguridad de los datos, y obligaba ya desde hacía años a adoptar unas medidas de seguridad apropiadas para proteger los datos de carácter personal registrados en ficheros automatizados frente a conductas como el acceso no autorizado. El 18 de abril de 2018, el comité de Ministros del Consejo de Europa modificó mediante el Protocolo CETS no. 223 este Convenio como parte del proceso de reformas y modernización de la legislación europea en materia de protección de datos, siendo sus dos objetivos principales reforzar la protección de la privacidad en el ámbito digital y fortalecer el mecanismo de seguimiento del Convenio.

a sus preferencias. Hay, por lo tanto, una pretensión de armonizar las normas internas de los Estados parte a nivel básico, pero también se permite cierto margen de discrecionalidad a cada país, que podrá decidir en relación con ciertos matices siempre dentro de los límites establecidos por el tratado. El art. 4 está, en efecto, dividido en dos apartados que responden a este patrón. En el primer apartado se define la conducta que debe pasar a formar parte como delito del ordenamiento jurídico estatal, en este caso la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos. En el segundo apartado se ofrece la posibilidad a cada Estado parte de reservarse el derecho a exigir en su ordenamiento interno que dichos apartados provoquen daños graves.

1.2.1.1.1.4 Interferencia en el sistema

El art. 5 recoge esta conducta, que supone la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

1.2.1.1.1.5 Abuso de los dispositivos

El art. 6 recoge el que posiblemente sea el más complejo de los delitos de este título primero, para lo que se divide en tres apartados. El primer apartado recoge el mandato de adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en el derecho interno de cada Estado parte la comisión deliberada e ilegítima de dos conductas. La primera de ellas es la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de, a su vez, dos clases de elementos: primero, un dispositivo, incluido en un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5; segundo, una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin

de que sean utilizados para la comisión de cualquiera de los delitos contemplados en dichos artículos. La segunda conducta es la posesión de alguno de los elementos contemplados en los anteriores apartados con el fin de utilizarlos para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Dentro de este apartado, además del mandato, y siguiendo con el mencionado patrón, se incluye la posibilidad para los Estados parte de exigir, a la hora de desarrollar sus propias normas a nivel estatal, que se posea un número determinado de dichos elementos para que pueda considerarse la existencia de responsabilidad penal.

El apartado segundo introduce un matiz interpretativo, especificando que no deberá entenderse que el art. 6 impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado primero del mismo no tengan por objeto la comisión de un delito previsto en los artículos 2 a 5 del tratado, como sucede en casos específicos como determinadas pruebas autorizadas o la protección de un sistema informático.

El tercer y último apartado permite reservarse el derecho a no aplicar lo dispuesto en el apartado primero de este artículo, siempre que esta reserva no afecta a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) de este artículo, es decir, a una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático.

1.2.1.1.2 Delitos informáticos

1.2.1.1.2.1 Falsificación informática

Dentro del mismo capítulo segundo, que recoge las medidas que deberán adoptarse a nivel nacional, y de la misma sección primera, dedicada al Derecho penal sustantivo, el título segundo incluye, a su vez, los delitos

informáticos. El art. 7 define la falsificación informática como la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se trata de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Siguiendo con el patrón establecido en la mayoría de los artículos anteriores, el tratado obliga a los Estados parte a adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno esta conducta cuando se cometa de forma deliberada e ilegítima, pero les permite adoptar la decisión de exigir o no que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

1.2.1.1.2.2 Fraude informático

El art. 8 incluye dos conductas en relación con las cuales deben legislar los Estados parte para adaptarse a las exigencias del tratado: primera, cualquier introducción, alteración, borrado o supresión de datos informáticos; segunda, cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona. Es importante destacar el matiz que se incluye en este art. octavo, puesto que no se hace la ya habitual referencia a que los actos deben ser deliberados e ilegítimos, sino que es necesario que los mismos causen un perjuicio específicamente de tipo patrimonial a otra persona.

1.2.1.1.3 Reflexiones doctrinales en materia de Derecho penal internacional sustantivo

El Convenio sobre la Ciberdelincuencia de Budapest sobresale por su versatilidad, pues recoge no solo los intereses de los Estados miembros del Consejo de Europa, sino también los de aquellos otros que se unieron al Convenio en un momento en que adquiría una importancia cada vez mayor

el uso de Internet y de las nuevas tecnologías. Ante el desarrollo y la utilización cada vez mayor de las TIC, y ante las novedades que ofrecían para la comisión de nuevos tipos de delito, era necesario aplicar una política penal más amplia que protegiese a la sociedad frente a los mismos poniendo un acento especial en delitos como la lucha contra el fraude informático y las violaciones de ciberseguridad en la Red[94].

Su importancia reside en ser el primer instrumento jurídico en este ámbito que impone a los Estados firmantes la obligación de adoptar medidas legislativas en sus ordenamientos internos que prevean como infracciones penales las conductas contempladas en su articulado[95]. Ya he expuesto que, en lo que respecta a la definición de las conductas objeto de mi estudio, cada uno de los artículos que lo componen se divide (con algunas excepciones, como la del artículo 5) en una parte cuyo contenido es obligatorio desarrollar en el derecho interno y otra en relación con la cual existe cierto margen de discrecionalidad dentro de los límites impuestos por el propio tratado. En cuanto a su estructura, tras el preámbulo el Convenio se divide en cuatro capítulos divididos, a su vez, en dos secciones y títulos, contando con un total de 48 artículos. El capítulo primero fija las definiciones de los términos que, posteriormente, se emplean a lo largo de todo el articulado, como los datos informáticos. Es en el segundo capítulo donde se abordan cuestiones de Derecho penal internacional sustantivo o material y se especifican las conductas que deberán ser objeto de infracción penal, para tratar después las cuestiones de Derecho procesal penal internacional. El tercer capítulo está dedicado a disposiciones sobre cooperación internacional, mientras que el cuarto incluye únicamente cláusulas finales.

A pesar de que el Convenio hace referencia a comportamientos llevados a cabo en el ciberespacio, varios de ellos guardan cierta reminiscencia con las conductas de las que el Derecho penal se ha ocupado tradicionalmente, con la diferencia de que el medio de comisión difiere entre

[94] Barrio Andrés, *Delitos 2.0,* pp. 59 - 60.

[95] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 225.

unos y otros y de que es posible atribuirles un mayor desvalor tanto de acción como de resultado[96]. Sin embargo, los términos utilizados en el texto son los que han ido marcando la pauta de lo que ha de entenderse por delitos informáticos, tanto en sentido amplio como en sentido estricto. Así, además de agrupar las conductas cuya incriminación pretende, el Convenio prevé la sanción de la participación y la tentativa en su art. 11, así como la responsabilidad de las personas jurídicas en su art. 12. Entre estas conductas están la falsedad informática (art. 7) y la estafa informática (art. 8), las cuales, en relación con el mundo no virtual, ya se contemplan, con mayor o menor uniformidad, en la mayoría de ordenamientos penales, al menos en todos los de nuestro entorno más próximo, aunque con contenidos diferentes de los que señala el Convenio al describir estas infracciones. Lo que les otorga el carácter de delincuencia de nuevo cuño con un desvalor de acción y de resultado diferente es, por lo tanto, el medio empleo en su comisión[97].

La falsedad informática, tal y como la define el Convenio, se produciría al incurrir en conductas de introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Así descrito, este delito es muy próximo a las falsedades materiales del ordenamiento jurídico español, siempre que las mismas se plasmen en el concepto de documento, pero también a la falsificación de tarjetas y a los daños informáticos. La estafa informática, por su parte, es difícil de compatibilizar con los requisitos tradicionales de la estafa entre personas, si atendemos a la definición de la primera que se incluye en el Convenio. A pesar de esto, los distintos ordenamientos jurídicos estatales, entre los cuales se cuenta el nuestro, ya vienen refiriéndose a la misma. Es sorprendente que el tratado solo considere infracciones

[96] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 225.

[97] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 226.

informáticas a la falsedad informática y a la estafa informática, toda vez que conductas como los daños informáticos también podrían considerarse como tales[98].

Los comportamientos recogidos en los arts. 2 a 6 son los que, desde un punto de vista conceptual, más pueden encuadrarse dentro de la definición de delincuencia de nuevo cuño. Esto, al margen del medio de comisión. Entre ellos se encuentra, en el art. 2, la tipificación del mal denominado delito de *hacking,* que será el referente de la regulación europea sobre la materia. Se tipifican así los accesos ilícitos, entendidos como accesos dolosos y sin autorización a todo o parte de un sistema informático. Con la tipificación en el art. 3 de la interceptación ilícita se ordena a los Estados parte la persecución de las conductas de interceptación dolosa y sin autorización, a través de medios técnicos, de datos informáticos en el destino, origen o interior de un sistema informático, incluidas las emisiones electromagnéticas procedentes de un sistema informático que transporta tales datos informáticos. Los atentados contra la integridad de los datos del art. 4, al ser conductas que suponen dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos, estarían vinculados a los tradicionales delitos de daños en elementos lógicos, en una interpretación extensiva de los mismos. Lo mismo sucede con los abusos contra la integridad del sistema del art. 5, que podrían encuadrarse en el ámbito de los tradicionales delitos de daños con el matiz de que, en este caso, no sería por el perjuicio derivado del daño a un bien, sino por el perjuicio que supone la imposibilidad de utilizarlo al tratarse de la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos. En último lugar, el art. 6, bajo la denominación de abuso de equipos e instrumentos técnicos, considera necesario prever como infracción penal conductas vinculadas a la utilización de dispositivos, claves o códigos que permitan la comisión de los comportamientos de los arts. 2 a 5

[98] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 226.

del Convenio. Atendiendo a su genérica denominación, este art. 6 hubiese podido englobar las cuatro infracciones precedentes[99].

El Convenio plantea, en consecuencia, dos propuestas político-criminales claras. La primera de ellas es la distinción entre la protección de los sistemas informáticos y la protección de los datos o de la información contenida en dichos sistemas. La segunda es que, a pesar de la propuesta de tipificar como delito el mero acceso intencional en ausencia de autorización a la totalidad o parte de un sistema informático, en la práctica los Estados parte tendrán la opción de establecer ciertas exigencias en la configuración de dicha infracción penal, ya sea que el acceso se cometa vulnerando medidas de seguridad, o que el acceso se realice con la finalidad de obtener datos o con otra finalidad contraria a la ley o, por último, que los sistemas informáticos vulnerados se encuentren conectados a otros[100].

El Convenio sobre la Ciberdelincuencia de Budapest merece una valoración general positiva por suponer un esfuerzo para garantizar una política penal común en la descripción de las conductas que integran la ciberdelincuencia[101]. Hay que mencionar, sobre todo, el hecho de que afronte tanto conductas vinculadas a ataques a bienes jurídicos que ya son objeto de tutela penal (los cuales varían, sin embargo, en el modo de comisión y que, por lo tanto, podrían escapar del ámbito tradicional de actuación del Derecho penal), como conductas lesivas de la integridad en sí de datos y sistemas. No obstante, también es importante señalar que existen aún lagunas en relación con ciertas conductas[102], como la difusión de contenidos lesivos a intereses

[99] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 227.

[100] Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 350 – 352.

[101] M. Barrio Andrés, *Ciberdelitos: amenazas criminales del ciberespacio*, 1ª ed., Madrid, Reus, 2017, p. 54. En opinión de Barrio Andrés, el Convenio sobre la Ciberdelincuencia de Budapest llena un vacío en el ordenamiento jurídico internacional, y con su entrada en vigor ayuda a hacer frente a una criminalidad que, aprovechando las nuevas tecnologías, puede poner en peligro el futuro de las redes y sistemas informáticos.

[102] G. Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, 1ª ed., Londres, Palgrave Macmillan, 2016, p. 104. Y no solo en relación con las conductas. El Convenio no incluye normas sobre el almacenamiento seguro de la información incautada mientras se está llevando a cabo una investigación,

personales. Además, el Convenio, como todo tratado internacional, contiene disposiciones de carácter genérico algo alejadas del principio de taxatividad, las cuales, al no ser de aplicación directa, relativizan su eficacia, aspecto que se agrava respecto a su eficacia general según se deriva de su propio articulado, que permite que los Estados invoquen, en el momento de su adhesión o su ratificación, unas reservas de muy diversa naturaleza, como la exclusiva tipificación de las conductas que produzcan lesiones graves, o el incumplimiento de la obligación de sancionar en todo o en parte algunas de las conductas descritas por el mismo[103]. Esto podría dificultar la armonización que constituye el principal objetivo del tratado, pese a lo cual su importancia como pionero en el tratamiento mundial de los ciberdelitos resulta indudable[104]. Aunque comparto la idea de que el margen de discrecionalidad que el Convenio otorga a los Estados parte podría dificultar la armonización normativa, considero que hubiese sido utópica una aproximación diferente en un escenario en el que hay tantos intereses contrapuestos y un gran número de países involucrados. Si se hubiese optado por establecer únicamente disposiciones de obligada transposición al ordenamiento jurídico de cada país quizá las negociaciones que dieron lugar al Convenio no hubiesen cristalizado en este razonable acuerdo de mínimos de acuerdo con el cual cada Estado parte, al tiempo que se involucra a través de la armonización de su legislación interna, puede decidir también el nivel de involucramiento deseado graduando determinados aspectos de la misma.

No hay que olvidar, además, que el anterior no será el único criterio que haga necesaria la inclusión de nuevos tipos penales en este ámbito, sino que, cuando los tipos penales tradicionales relacionados con las redes y

lo que implica que la información legalmente almacenada en el CERT de un Estado parte podría no reunir los requisitos legales necesarios en un Estado parte distinto. Además de suponer un problema para compartir dicha información durante las investigaciones, implica que no está claro qué tipo de información puede considerarse como una prueba válida durante la investigación de los ciberdelitos.

[103] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 228.

[104] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 229.

sistemas informáticos no satisfagan del todo los objetivos protectores del legislador estatal, existe la posibilidad de crear tipos de equivalencia[105], es decir, nuevos tipos penales cuyo objetivo es complementar a los ya existentes mediante una corrección de las carencias detectadas en la descripción de sus respectivas acciones típicas. Aunque la concreción de nuevos tipos y su vinculación a bienes jurídicos merecedores de protección penal ayudan a consolidar la seguridad jurídica, no resulta difícil incurrir en un casuismo excesivo al tiempo que se despoja de protección penal a conductas que la merecerían. Además, atendiendo a las particularidades de cada país, el desarrollo de los mismos sin duda resultaría muy desigual dependiendo de los criterios de cada legislador estatal, por mucho que exista una base común derivada del Convenio.

No cabe duda de que esto podría conllevar, precisamente, lo que se intentó evitar creando una norma internacional de estas características: que los criminales seleccionen en qué países actuar después de analizar cual tiene la legislación más laxa[106] [107]. Sin embargo, esto no puede compararse al escenario anterior a la existencia del Convenio, en el que había países que ni siquiera castigaban determinadas conductas. En el escenario actual, hay al menos unas bases comunes[108] que, en el peor de los casos, han dificultado

[105] Ya propuesto en C.M. Romeo Casabona, *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las nuevas tecnologías de la información*, 1ª ed., Madrid, Fundesco, 1988, p. 116.

[106] N. Maroz, "Regionalization of international cooperation in the fight against cybercrime", *Law Review: Judicial Doctrine & Case Law*, vol. 10, no. 2, 2019, p. 227. Aunque se cree que la existencia de distintos sistemas de derecho interno que chocan al perseguir los ciberdelitos podría conllevar la creación de refugios para delincuentes, impedir la asistencia jurídica mutua y dificultar la extradición entre países de distintas regiones, esto no es necesariamente cierto, ya que si hubiese un adecuado trabajo diplomático podrían desarrollarse tratados internacionales más modestos y menos pretenciosos que resolviesen las necesidades específicas de los distintos países, ajustándose al exterior solo en lo estrictamente necesario y, sobre todo, pudiendo ser sometidos al control del pueblo con mayor facilidad que en el caso del Convenio.

[107] N. Machín y M. Gazapo, "La Ciberseguridad como factor crítico en la Seguridad de la Unión Europea", *Revista UNISCI,* no. 42, 2016, p. 52. Entre los beneficios derivados de la existencia del Convenio está la disminución de las desigualdades en el Derecho penal sustantivo y, sobre todo, de las zonas de impunidad.

[108] L. Kovács, "Cyber Security Policy and Strategy in the European Union and NATO", *Land Forces Academy Review,* vol. 23, no. 1, 2018, p. 18. Hay que insistir en la idea de

la actividad delictiva y obligan a los criminales[109] a un minucioso estudio previo a llevar a cabo las conductas prohibidas. Las herramientas de colaboración previstas en el propio texto, que facilitan que distintos países trabajen juntos en la persecución de estas conductas, son un elemento de dificultad añadido para los criminales y una ayuda para los agentes[110] de la ley.

Por último, aunque todo lo anterior puede aplicarse en un análisis de la situación a nivel mundial, no tiene por qué ser siempre así a nivel más reducido, como en el ámbito comunitario. Y es que nada impide a la UE, a pesar de tener solo competencia parcial en relación con el Derecho penal, el desarrollo de un reglamento que, respetando las líneas generales establecidas por el Convenio, regule esta materia con más profundidad y opte por establecer como obligatorio lo que el tratado internacional considera como opcional. Esto, si bien no solucionaría la disparidad en las legislaciones internas a nivel mundial, sí lo haría a nivel comunitario, beneficiando, a un tiempo, al conjunto de la UE y a cada uno de los Estados miembros. Creo que debemos entender este Convenio sobre la Ciberdelincuencia de Budapest no como una herramienta jurídica inamovible y definitiva, sino como un primer paso hacia una armonización legislativa en relación con ciertos ciberdelitos que podría ser, siempre manteniendo la debida cautela, muy beneficiosa para la seguridad informática[111].

---

que el Convenio es solo una base común a partir de la cual cada Estado parte deberá desarrollar su propia normativa específica a nivel interno.

[109] J. Leclair y G. Keeley, *Cybersecurity in Our Digital Lives,* 1ª ed., Albany, NY, Hudson Whitman / Excelsior College Press, 2015, p. 65. Los criminales, en la actualidad, son creativos y rastrean Internet con herramientas sofisticadas en busca de información de toda clase. No parece descabellado que también busquen información jurídica acerca del lugar con la legislación más idónea para cometer el delito.

[110] Comisión Europea, *Scientific Opinion no. 2/2017: Cybersecurity in the European Digital Single Market,* Bruselas, Comisión Europea, 2017, p. 82. Incluso en el ámbito comunitario, el hecho de tener que informar en relación con los incidentes relativos a la ciberseguridad en base a distintas legislaciones y ante distintas autoridades públicas se considera una pesada carga que conviene sustituir a través de la armonización.

[111] W. Madsen, "Cybercrime Convention Steams Ahead", *Network Security*, no. 5, 2001, p. 6. No obstante, parecemos haber aceptado el actual estado de las cosas como inamovible, cuando hubo un tiempo en que se consideraba que el Convenio era draconiano. Por eso la hemeroteca es tan importante: aunque este artículo que cito

1.2.1.2. Derecho procesal penal internacional y otros elementos de cooperación internacional

1.2.1.2.1 Competencia judicial

Por su carácter transnacional, uno de los aspectos más controvertidos en relación con los delitos que afectan a la ciberseguridad es la determinación del juez competente para conocer de cada caso concreto. El Convenio sobre la Ciberdelincuencia de Budapest incluye, también, una previsión en este sentido en su capítulo segundo, sección tercera, la cual recoge, a su vez, un único art. 22 con el que comparte su sucinto nombre: jurisdicción.

Del mismo modo que sucedía en el ámbito del Derecho penal internacional sustantivo, solo que en esta ocasión en el ámbito del Derecho procesal penal internacional, el primero de los cinco apartados obliga a los Estados parte a adoptar las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto en los arts. 2 a 11 del Convenio, siempre que se cometa en su territorio, a bordo de un buque que enarbole pabellón de dicho Estado parte, a bordo de una aeronave matriculada según las leyes de un determinado Estado parte, o cuando el delito lo cometa uno de sus nacionales, siempre que sea susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

El apartado segundo es, una vez más, la confirmación del patrón ya analizado en el ámbito del Derecho penal internacional sustantivo, puesto que permite a cualquier Estado parte reservarse el derecho a no aplicar o a aplicar

---

puede parecer anticuado e inservible, se escribió en mayo de 2001, meses antes del 11 de septiembre, y en el mismo se recoge cómo las autoridades estadounidenses aceptaron el Convenio solo porque temían que desde Europa se avanzase hacia una versión posterior todavía más rigurosa. Escándalo tras escándalo, crisis tras crisis, atentado tras atentado, avanzamos más y más hacia las fauces de la globalización y de un nuevo orden mundial luciferino. Estoy seguro de que deben existir alternativas que permitan perseguir esta clase de delitos sin necesidad de comprometer nuestra intimidad ni nuestra libertad.

solo en determinados casos o condiciones las normas sobre jurisdicción en los apartados 1.b) a 1.d) del art. 22 o, sostiene el tratado de manera muy confusa, en cualquier otra parte de los mismos. He tenido que acudir a la versión inglesa del mismo con la intención de comprobar si la redacción en dicho idioma permitía interpretar de manera más clara esa última frase, pero, salvo que se refiera al art. 22 en sí y no a los apartados mencionados (es decir, que la traducción correcta sea en cualquier otra parte del mismo, en singular, por referirse al art. 22, y no a dichos apartados) no hay muchas alternativas. Lo que no tiene sentido, por absurda e incomprensible, es la redacción actual, según la cual los Estados parte pueden no aplicar o aplicar solo en determinados casos o condiciones las normas de los apartados 1.b) a 1.d) del art. 22 o en cualquier otra parte de los mismos. La única respuesta que parece viable es que la traducción sea incorrecta y, en realidad, en una redacción alternativa más adecuada y que encaja con la versión inglesa, la frase deba hacer referencia, en singular, a cualquier otra parte del mismo, esto es, del art. 22 en sí. Esto, no obstante, daría libertad a los Estados parte para no aplicar o aplicar solo en determinados casos o condiciones no solo las normas de los apartados 1.b) a 1.d) del art. 22, sino también la norma del apartado 1.a) del mismo artículo y de los cinco apartados que lo componen. Si la intención del legislador era esa, hubiese sido más lógico no hacer específica referencia a dichos apartados y permitir directamente las reservas en relación con cualquier apartado del art. 22, y si su intención era limitarlas a dichos artículos, no optó por la redacción clara y sin aspectos confusos que se espera esta de un texto jurídico de esta categoría, en el que convergen tantos intereses.

El tercer apartado vuelve a introducir un mandato para los Estados parte, según el cual deberán adoptar las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del art. 24 del Convenio cuando el presunto autor del delito se encuentre en territorio de dicho Estado y no pueda ser extraditado a otro Estado parte a causa de su nacionalidad, previa solicitud de extradición. Los delitos a los que se refiere el apartado 1 del art. 24 al que nos remite este

tercer apartado del art. 22 son los delitos establecidos en los arts. 2 a 11 del Convenio, con el matiz de que en el art. 24 se exige para su aplicación que estén castigados en la legislación de los dos Estados parte implicados con una pena privativa de libertad de una duración máxima de, como mínimo, un año, o con una pena más grave. Si este matiz se extiende al apartado tercero del art. 22 y condiciona la aplicabilidad del apartado 1 del art. 24 al que nos remite, es algo que tampoco queda claro, porque no se especifica si la remisión es a los delitos de los arts. 2 a 11 del Convenio o a dichos artículos con los condicionantes recogidos en el art. 24. Si la interpretación adecuada es la primera, el legislador podría haber optado por mencionarlos también en este tercer apartado del art. 22 sin la complicación de remitir a otro artículo, y si espera de quien interprete la norma que incluya en su interpretación los matices del apartado 1 del art. 24, debería haber sido más específico para evitar graves confusiones.

El apartado cuarto del art. 22 sostiene que el Convenio no excluye ninguna jurisdicción penal ejercida por un Estado parte de conformidad con su derecho interno. Quizá en este apartado el legislador debería haber especificado que esto será así como último recurso, solo para cuando este art. 22 no permita determinar la competencia judicial internacional y haya que acudir, obligados por las circunstancias, al derecho interno de un determinado Estado parte. A mi juicio, con la redacción actual se corre el riesgo de que distintos Estados parte afirmen que les corresponde la jurisdicción penal basándose en su derecho interno. Esto, por supuesto, podría resolverse acudiendo al principio de jerarquía normativa, pero también es cierto que el legislador, incluyendo una línea adicional que considerase el derecho interno como último recurso, podría haber evitado las interpretaciones dispares en relación con un tratado que, reitero, obliga a una gran cantidad de Estados parte con intereses muy variados y tradiciones jurídicas de muy diversa índole.

Quizá por esto adquiere mayor importancia el apartado 5 de este art. 22 cuando introduce una interesante herramienta diplomática de acuerdo a la cual cuando varios Estados parte reivindiquen su jurisdicción respecto de un

presunto delito contemplado en el Convenio, los interesados celebrarán consultas, siempre que sea oportuno, para determinar cual es la jurisdicción más adecuada para desarrollar las actuaciones en el ámbito penal.

1.2.1.2.2 La Red 24/7

Una de las novedades más interesantes del Convenio fue la creación de la Red 24/7. En su capítulo tercero, dedicado a la cooperación internacional, se incluyó una sección segunda con disposiciones especiales en la que se incardinó el art. 35 dentro del título tercero, con el cual este art. 35 comparte denominación (Red 24/7). Su apartado primero establece un mandato para los Estados parte e introduce, al mismo tiempo, la definición de la Red 24/7, ya que deberán designar un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata por los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá, cuando lo permitan la legislación y la práctica internas, los actos tendentes a facilitar o a adoptar directamente las siguientes medidas: el asesoramiento técnico, la conservación de datos en aplicación de los arts. 29 y 30, y la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos[112].

El apartado segundo desarrolla la manera en que deberán relacionarse los distintos puntos de contacto. Así, su párrafo primero determina que el punto de contacto de un Estado parte estará capacitado para mantener comunicaciones con el punto de contacto de otro Estado parte con carácter urgente. Su párrafo segundo establece una cautela: en los casos en que el punto de contacto designado por un Estado parte no dependa de al autoridad

[112] M.J. Glennon, “The Dark Future of International Cybersecurity Regulation”, *Journal of National Security Law & Policy,* vol. 6, no. 2, 2013, p. 564. En los ciberdelitos posee especial importancia identificar y localizar a los sospechosos. Solo una vez identificados y localizados es posible poner en marcha los mecanismos legales necesarios para su persecución, los cuales dependerán, en gran medida, de dónde se encuentren.

o de las autoridades de dicho Estado responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente. Por último, el apartado tercero obliga a los Estados parte a garantizar la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de esta Red 24/7. Hay que destacar, en este sentido, que algunos de los Estados parte identificaron su punto de contacto nada más ratificar el Convenio. Tanto es así que su identidad consta en las declaraciones y reservas que lo acompañan, como en el caso de los EE. UU., que eligió a la CCIPS del DOJ en Washington D.C. para llevar a cabo esta labor. El CCIPS es una sección de la División Penal del DOJ que incluye a cuarenta juristas con experiencia en la obtención de pruebas electrónicas encargados de combatir la ciberdelincuencia. En España, le corresponde al GDT de la Guardia Civil ser el punto de contacto nacional de la Red 24/7 para cumplir con lo establecido en el Convenio.

1.2.1.2.3 Reflexiones doctrinales en materia de Derecho procesal penal internacional

Desde una perspectiva procesal, el Convenio incluye medidas orientadas a que los Estados parte incorporen a sus procedimientos penales determinadas exigencias[113], como la necesidad de conservación de los datos, la protección de la integridad de los datos que se hayan almacenado o la obligación de comunicar los datos de tráfico a las autoridades competentes cuando estas lo soliciten[114]. Además, una de las cuestiones procesales más controvertidas, la de la competencia judicial, se resuelve mediante la

[113] F. Jiménez García, "La ciberseguridad en el marco internacional. El sistema del Convenio de Budapest de 2001 sobre la ciberdelincuencia adoptado en el Consejo de Europa", en E.R. Jordá Capitán y V. De Priego Fernández (dirs.), *La protección y seguridad de la persona en Internet. Aspectos sociales y jurídicos",* Madrid, Reus, 2014, pp. 65 – 75. Uno de los asuntos de mayor interés en el Convenio son las obligaciones procesales, que empujan a los Estados parte a dotarse de los poderes y procedimientos necesarios para asegurar los fines de las investigaciones o procedimientos penales internacionales que correspondan.

[114] De la Mata Barranco y Pérez Machío, *Derecho Penal Informático,* p. 131.

aplicación del principio de territorialidad[115] (art. 22). Hay que destacar la normativa dedicada a la cooperación internacional en los arts. 23 a 35, por ser un intento de activar mecanismos de cooperación entre países que ofrezcan una solución rápida y eficaz en lo concerniente a la investigación, persecución y represión penal de los ciberdelitos. Es notable, también, el establecimiento de nuevas formas de cooperación al tiempo que se adaptan las ya conocidas, adquiriendo relevancia el desarrollo de medidas de ayuda mutua entre los Estados parte para los fines de investigación o procedimientos concernientes a infracciones recogidas en el tratado, las cuales se llevan a cabo mediante la colaboración de los prestadores de servicios de cada país y mediante el establecimiento de autoridades nacionales en cada Estado que canalicen las comunicaciones interestatales. En este sentido, se prevé la posibilidad de solicitar la conservación de datos de tráfico, el acceso a los datos almacenados, y la interceptación de estos dos tipos de datos ya mencionados.

Del mismo modo, con el objetivo de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos, o de recoger pruebas electrónicas de una infracción penal, el art. 23 contempla la necesidad de recurrir a los instrumentos internacionales sobre cooperación internacional en el ámbito penal y a acuerdos basados en la legislación uniforme o recíproca de cada Estado parte, así como al derecho nacional de cada uno, de la forma más amplia posible. La finalidad es la articulación de un sistema de colaboración mutua a través de una o varias autoridades centrales designadas por los Estados parte, las cuales, a modo de mediadores, facilitarían la tramitación de las demandas de extradición pertinentes (art. 27 y sucesivos) cuando no existan acuerdos internacionales que se puedan aplicar y sea necesaria la colaboración[116].

---

[115] J. Alonso Lecuit, “Relanzamiento del Plan de Ciberseguridad de la UE”, *Análisis del Real Instituto Elcano (ARI),* no. 97, 2017, p. 5. El principio de territorialidad es adecuado para la determinación de la competencia judicial en el ámbito internacional, pero resulta exiguo para determinar la ley aplicable a nivel estatal.

[116] De la Mata Barranco y Pérez Machío, *Derecho Penal Informático,* pp. 132 – 133.

No hay que olvidar la creación de la Red 24/7 como punto de contacto disponible las veinticuatro horas del día, siete días a la semana, que garantiza la prestación de ayuda inmediata a las investigaciones relacionadas con los delitos tipificados por el Convenio, o la obtención de pruebas electrónicas en relación con un delito (art. 35). El hecho de que exista una herramienta de colaboración ininterrumpida que, además, facilita el asesoramiento técnico, la conservación de datos, la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos evidencia los logros de este tratado[117].

No cabe duda, además, de que en el ámbito procesal el ordenamiento jurídico nacional ha conseguido adaptarse, en el caso de España[118], a las exigencias del Convenio. Sirva como ejemplo el art. 18.1 b) del Convenio, materia que en el derecho interno español se encuentra regulada en el art. 588 ter m) de la LECrim, incorporado a la misma por la reforma derivada de la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. De acuerdo al mismo, resulta posible reclamar de los proveedores de servicios de telecomunicaciones, de los que dan acceso a una red de esa naturaleza o de los prestadores de servicios de la sociedad de la información los datos sobre titularidades o sobre abonados que tengan a su disposición con objeto de utilizarlos en investigaciones criminales. El precepto de la LECrim, además, no especifica que el prestador de servicios deba radicar en España, por lo que se puede entender[119] que también pueden ser requeridos en este sentido proveedores

[117] Barrio Andrés, *Delitos 2.0,* p. 61.

[118] J. Clough, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation", *Monash University Law Review,* vol. 40, no. 3, 2014, p. 700. Aunque en España ha sido posible incorporar al ordenamiento jurídico interno lo dispuesto en el Convenio, la principal amenaza para este tratado internacional siguen siendo las iniciativas a nivel nacional que, aunque permiten expresar los diversos puntos de vista existentes, conllevan el riesgo de fragmentar el esfuerzo invertido en su desarrollo.

[119] E. Tejada de la Fuente, "Introducción: ciberseguridad y ciberdelincuencia: respuestas desde el estado de derecho. La armonización legislativa transnacional, en particular: las medidas de investigación criminal en la Convención de Budapest", en J.I. Zaragoza Tejada (coord.), *Investigación tecnológica y derechos fundamentales: comentarios a las*

que tengan su sede en otros países, siempre que la petición se ajuste a lo dispuesto en el art. 18.1 b) del tratado internacional.

Este Convenio supone un avance en relación con la adopción de previsiones que intenten garantizar las medidas necesarias para asegurar de la forma más eficaz posible la persecución, investigación y sanción de unas conductas que, a causa de su naturaleza trasnacional, sin duda van a generar numerosos problemas a nivel mundial[120] [121]. Además de haber llenado un vacío en el ordenamiento jurídico internacional, e incluso no habiendo sido desarrollado de la manera habitual (ya que, por lo general, el Derecho internacional armoniza legislaciones y prácticas nacionales preexistentes, mientras que en el ámbito de los ciberdelitos ha sido el Derecho internacional el que ha impulsado la adopción de medidas nacionales), ha ayudado a generalizar la percepción de que los ciberdelitos traspasan todas las

modificaciones introducidas por la Ley 13/2015, Cizur Menor, Navarra, Aranzadi, 2017, pp. 48 – 65. Los proveedores extranjeros tienden a facilitar datos sobre abonados o titularidades de manera directa, a simple solicitud del Ministerio Fiscal o de las Unidades de Policía Judicial.

[120] De la Mata Barranco y Pérez Machío, *Derecho Penal Informático,* p. 133.

[121] S. Kierkegaard, "Cybercrime convention: narrowing the cultural and privacy gap?", *International Journal of Intercultural Information Management,* vol. 1, no. 1, 2007, pp. 31 – 32. No hay que olvidar las voces críticas con toda esta legislación internacional, que consideran que se está entregando demasiado poder a los gobiernos en detrimento de la libertad. No cabe duda de que la persecución de los delitos no convierte en aceptable la violación de la ley natural ni de la ley eterna, a las que me referiré más adelante. Incluso teniendo esto en cuenta, la crítica que se realiza al Convenio es que otorga a los gobiernos no solo un margen de interpretación demasiado amplio, sino un excesivo poder sin un adecuado sistema de control que vele por los intereses del pueblo. Se invita a las personas y a los gobiernos, no sin razón, a rechazar este tratado y a defender su intimidad. El dilema consiste, en efecto, en encontrar un razonable equilibrio entre la persecución eficaz de los delitos y la salvaguarda de la intimidad de las personas. Sin embargo, considero que en un mundo en el que se aceptan los avances tecnológicos de manera irreflexiva y el pueblo otorga el poder a personas malvadas y sin escrúpulos, resulta inevitable, por desgracia, que lo primero acabe primando sobre lo segundo. La solución quizá no sea tanto intentar cambiar el sistema del príncipe de este mundo, sino abandonar dicho sistema perverso y dar la espalda voluntariamente a los avances tecnológicos que conllevan, a largo plazo, graves perjuicios para la salud física y espiritual de las personas.

fronteras[122], impulsando así un notable esfuerzo legislativo en el seno de la UE[123].

1.3 Derecho penal de la Unión Europea

1.3.1 La inexistencia de un *Corpus Iuris Poenalis* europeo

En la segunda mitad del siglo XX, los avances en la europeización del Derecho penal se vieron fuertemente lastrados por su percepción como dos realidades antinómicas. Ya el propio término, que desde una perspectiva estricta apunta a la influencia europea sobre los distintos Derechos penales de cada nación, comprende, desde un punto de vista más genérico, el desarrollo hacia la integración penal en Europa, es decir: hacia la creación de un Derecho penal europeo. Esto se conseguiría tanto a través de la armonización de las legislaciones penales como de los esfuerzos por construir un Derecho penal europeo común. Los artífices de lo que, con los años, y tras múltiples cambios internos, sería la Unión Europea, subestimaron la relevancia de la aplicación del Derecho comunitario y, a excepción de algunas normas, dejaron su cumplimiento en manos de las autoridades de los Estados miembros. Durante mucho tiempo, las infracciones en relación con el Derecho comunitario fueron respondidas mediante el Derecho administrativo, resistiéndose el Consejo a la utilización del Derecho penal para respetar la soberanía de los Estados miembros[124].

---

[122] S.D. Murphy, "Adoption of Convention on Cybercrime", *The American Journal of International Law,* vol. 95, no. 4, 2001, p. 890. Al carácter transnacional de los ciberdelitos hay que añadir lo lesivos que resultan para la seguridad y la economía. Pero, incluso teniendo en cuenta solo lo primero, un régimen legal internacional inadecuado, sobre todo en lo referente a extradición, podría traducirse en la imposibilidad de perseguir a determinados delincuentes, de manera que es esencial desarrollar una normativa suficiente.

[123] Barrio Andrés, *Delitos 2.0,* p. 62.

[124] J.L. De la Cuesta Arzamendi, "El proceso de integración penal europea", en J.L. De la Cuesta Arzamendi (dir.), *Adaptación del derecho penal español a la política criminal de la Unión Europea,* Cizur Menor, Navarra, Aranzadi, 2017, pp. 27 – 28. Las Comunidades se concibieron originalmente como entidades sin competencia penal directa, pero las sanciones administrativas no resultaban suficientes para hacer frente a

Ante la insuficiencia de las sanciones administrativas, y ante la necesidad de una aproximación legislativa, penalistas de distintos países de la UE (especialmente de Francia, pero también de Alemania, Italia y España) propusieron la construcción de un CP europeo común, así como la unificación de los CCPP de sus Estados miembros, como mínimo en lo concerniente a sus grandes principios rectores. En los años ochenta y noventa se llegó a defender la creación de un *Corpus Iuris Poenalis* europeo. No obstante, a pesar de los esfuerzos de la doctrina en este sentido, esto no llegó a materializarse. Las causas de este fracaso son cuatro: la ausencia de mención en la normativa constitutiva europea de competencias en materia penal, que conllevó que las instituciones europeas no dispusiesen de facultades legislativas directas en este sector; la escasa cohesión a nivel comunitario en aquella época; la falta de experiencia y conocimientos de las instituciones europeas en este sentido; y, por último, la inexistencia de una conciencia precisa sobre la cada vez más elevada presencia y presión de ciertos delitos y nuevas formas de criminalidad en los espacios transfronterizos, incluyendo a los ciberdelitos. A causa de todos estos motivos, los planteamientos de estos penalistas europeos no fueron bien acogidos en la época: la situación estructural y política existente hacía que los mismos no pareciesen realistas[125].

Sí hubo, durante aquel periodo, una cooperación judicial y policial limitada, derivada de la influencia y la presión de los órganos judiciales y de las autoridades gubernamentales relacionadas con la seguridad, más que de las propuestas de los penalistas. Desde entonces, existieron numerosas

ciertos comportamientos que atentaban contra importantes bienes jurídicos de interés comunitario.

[125] C.M. Romeo Casabona, "La penetración del Derecho penal económico en el marco jurídico europeo: los delitos contra los sistemas de información", en C.M. Romeo Casabona y F. Flores Mendoza (eds.), *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica,* Granada, Comares, 2012, pp. 332 – 333. Los cambios en las circunstancias y el régimen jurídico europeo en materia penal motivaron que los penalistas intensificasen su empeño, exhortando a la elaboración de una legislación penal europea sectorial siempre sometida a principios, garantías y límites fruto del desarrollo de la ciencia penal europea como los de intervención mínima o *ultima ratio*, subsidiariedad, legalidad, culpabilidad o proporcionalidad.

disposiciones, principalmente no penales, orientadas a mejorar la seguridad de las TIC, al tiempo que las formas de criminalidad relacionadas con dichas tecnologías crecían y se ampliaban. Hay que mencionar dos particularidades en este sentido: primera, el acierto de las autoridades europeas al prevenir los delitos contra las TIC de forma integral, esto es, con el recurso simultáneo a medidas jurídicas penales y no penales, e incluso a otro tipo de medidas no legales, como las educativas, cumpliendo así el principio de mínima intervención del Derecho penal; y segunda, que aunque a lo largo de los últimos años se ha reafirmado la competencia europea en materia penal, no es posible encontrar, a nivel comunitario, un equivalente del Convenio sobre la Ciberdelincuencia de Budapest, sino que la UE, en la actualidad, se sirve de actos legislativos variados para materializar esta competencia[126]. Es decir: que aunque la UE está esforzándose por adaptarse a las nuevas realidades[127] y siempre ha tratado de estar a la vanguardia del desarrollo legislativo en materia de ciberseguridad con su riguroso régimen de protección de datos[128], no existen en el ámbito comunitario ni un texto legal únicamente dedicado a los delitos que afectan a la ciberseguridad ni un CP europeo común en el que se recojan los mismos.

Habiendo analizado en apartados anteriores actos normativos no vinculantes como las recomendaciones, es necesario también analizar los vinculantes, como las directivas, los reglamentos, y las decisiones marco para, entendiendo la miríada de legislación extrapenal existente en relación

[126] Romeo Casabona, *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica,* pp. 333 – 373. Hay que tener en cuenta la tendencia actual a establecer disposiciones penales en las que no está clara la tutela de interés alguno, así como a descuidar el principio de *ultima ratio* y a reaccionar ante cualquier problema social con un incremento de la represión utilizando el Derecho penal.

[127] Álvarez Rodríguez, *Nuevos Retos de la Ciberseguridad en un Contexto Cambiante*, p. 33.

[128] J.D. Rhodes y R.S. Litt, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals,* 2ª ed., Chicago, IL, ABA Publishing, 2018, p. 104. La primera norma que, aún sin mencionarla, incluyó disposiciones relativas a la ciberseguridad en la historia de la UE fue la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

con la ciberseguridad, extraer de ellas una información ahora dispersa y fragmentada que permita determinar específicamente desde la perspectiva del Derecho penal cual es el estado de los delitos que afectan a la ciberseguridad en la legislación de la UE.

Sin embargo, no es posible entender la importancia de las directivas y las recomendaciones sin comprender primero que la UE dispone de una capacidad limitada para legislar en el ámbito del Derecho penal, puesto que el mismo se considera un símbolo de la soberanía de los Estados miembros. La UE, como organización principalmente comercial, solo está dotada de una competencial parcial en lo que respecta a la regulación en el ámbito penal. Esto responde a dos motivos: por un lado, que la delincuencia puede considerarse un obstáculo al comercio entre los países que la forman; por otro, la creencia de que un desarrollo económico y social estable solo es posible si existe una adecuada cooperación en materia penal. El Tratado de la Unión Europea o Tratado de Maastricht de 1993 y el Tratado de Ámsterdam de 1999 introdujeron cambios que afectaron parcialmente al Derecho penal, sobre todo en lo referente a la justicia y los asuntos de interior, pero la UE continuó sin tener competencia real para crear Derecho penal. No obstante, la aproximación de las normas en materia penal estaba permitida sobre la base de lo dispuesto en el art. 29 del primero de los tratados mencionados. Lo que la UE sí puede hacer, basándose en el art. 83.1 del TFUE, es adoptar directivas con normas mínimas que definan las infracciones penales y las sanciones, aunque solo en caso de delitos que sean especialmente graves y tengan una dimensión transfronteriza, entre los que se incluye la delincuencia informática[129].

Gran parte de la actividad de la UE consiste en la coordinación de esfuerzos. Además de la ya mencionada ENISA[130], hay que destacar la

[129] Barrio Andrés, *Delitos 2.0,* p. 62.

[130] D. Markopoulou, V. Papakonstantinou y P. De Hert, “The new EU cybersecurity framework: The NIS Directive, ENISA´s role and the General Data Protection Regulation”, *Computer Law & Security Review,* vol. 35, no. 6, 2019, p. 7. ENISA proporciona servicios de secretariado y apoya la cooperación entre los CSIRT.

actividad del EC3[131] [132], el organismo de la Europol que, desde 2013, funciona como un centro de inteligencia que coordina los esfuerzos de los Estados miembros en la lucha contra la ciberdelincuencia[133].

1.3.2 Análisis de los principales actos legislativos para la creación de un Derecho penal sobre ciberdelincuencia de la Unión Europea

1.3.2.1 La Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión (Directiva NIS)

Las directivas son actos legislativos vinculantes que establecen objetivos a cumplir por todos los países de la UE, correspondiendo a cada uno de ellos la elaboración de sus propias leyes para conseguir dicho objetivo. En el ámbito de la UE, fue la preocupación por la protección de datos lo que llevó a dar los primeros pasos para garantizar su seguridad[134].

No obstante, fue la Directiva 2000/31/CE, de 8 de junio de 2000, relativa a determinados aspectos de los servicios de la sociedad de la

[131] G. Christou, "The challenges of cybercrime governance in the European Union", *European Politics and Society,* vol. 19, no. 3, 2018, p. 364. La operación del EC3 para hacer frente al *botnet* ZeroAccess demostró que es posible la colaboración interjurisdiccional siempre que se actúe con la misma rapidez que el criminal.

[132] G. Christou, "The collective securitisation of cyberspace in the European Union", *West European Politics,* vol. 42, no. 2, 2019, p 280. Se destaca el EC3 y su investigación de la actividad criminal en Internet.

[133] Barrio Andrés, *Delitos 2.0,* p. 64.

[134] De la Mata Barranco y Pérez Machío, *Derecho Penal Informático,* p. 135. Así, a mediados de los años noventa, comenzaron a publicarse directivas como la ya mencionada Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; la Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones; la Directiva 1998/34/CE, del Parlamento Europeo y del Consejo, de 20 de noviembre de 1998, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información; y la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica.

información, en particular el comercio electrónico en el mercado interior, la que estableció por primera vez el objetivo de armonizar la lucha europea contra la ciberdelincuencia. Este objetivo se fundamentó sobre la idea de que el desarrollo de los servicios de la sociedad de la información en un espacio sin fronteras interiores era un medio esencial para eliminar las barreras que dividían a los países europeos, y la única manera de garantizar un nivel elevado de integración jurídica en la UE para establecer un espacio sin fronteras en el que se suprimiesen los obstáculos derivados de la disparidad de legislaciones y de la inseguridad jurídica resultante de los distintos regímenes nacionales. Las medidas previstas se limitaron, por lo tanto, al aseguramiento del mínimo indispensable necesario para conseguir que el mercado interior funcionase correctamente. No era posible encontrar en la misma referencia expresa alguna a la responsabilidad penal, si bien, siguiendo el espíritu marcadamente mercantilista que inspiró la creación de la UE y que, por tanto, impregnó su legislación[135] [136], sí vislumbró la necesidad de intervenir frente a conductas que se cometiesen en el comercio electrónico y afectasen a sus cuatro grandes áreas de tutela: menores, dignidad humana, consumidores y salud pública[137]. Además, impuso la obligación para los prestadores de servicios de comunicar sin demora a las autoridades públicas competentes los presuntos datos ilícitos o las actividades ilícitas que llevasen a cabo los destinatarios de su servicio, así como la obligación de transmitir a las autoridades competentes, en respuesta a una petición, información que

[135] D. Stitilis, P. Pakutinskas e I. Malinauskaite, "EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis", *Security Journal*, vol. 30, no. 4, 2016, p. 1154. Uno de los aspectos destacados en la adopción de estrategias por parte de la UE es el efecto adverso de la ciberdelincuencia sobre su economía. Aunque es razonable preocuparse por la misma, creo que el carácter prioritario que se otorga al dinero en el seno de la UE define la triste escala de valores de sus dirigentes.

[136] M. Holzleitner, J. Reichl, "European provisions for cyber security in the smart grid: An overview of the NIS-directive", *e & i Elektrotechnik und Informationstechnik,* no. 134, 2017, p. 14. La obstaculización del desarrollo económico de la UE figura como una de las principales consecuencias de los ciberataques.

[137] R. Piggin, "NIS Directive and the Security of Critical Services", *ITNOW,* vol. 60, no. 1, 2018, p. 44. Más adelante, la Directiva NIS reconoció específicamente la importancia de la fiabilidad y de la seguridad de las redes y de los sistemas informáticos, puesto que, ante la creciente digitalización, de los mismos dependen servicios esenciales para el funcionamiento de la sociedad, como, entre otros, la asistencia sanitaria.

les permitiese identificar a los sujetos con los que hubiesen celebrado acuerdos para almacenar datos. Esta Directiva 2000/31/CE fue, en definitiva, una de las primeras iniciativas europeas orientadas hacia la incriminación de la ciberdelincuencia[138].

La Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, fue más específica, pues autorizó a los Estados miembros a regular por ley la obligación, a cargo de los prestadores de servicios, de conservar los datos electrónicos de tráfico de sus clientes durante un tiempo limitado que cada gobierno podía establecer de acuerdo a sus propios criterios. Para justificar esta petición, se esgrimieron razones de seguridad nacional, defensa, seguridad pública y lucha contra la criminalidad. El art. 15 que la recogía levantaba excepcionalmente, y en nombre de la seguridad nacional, la garantista prohibición de su art. 5, que establecía la obligación de garantizar, a través del ordenamiento interno de cada Estado, la confidencialidad de las comunicaciones y de los datos de tráfico asociados a ellas, y prohibía la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y de los datos de tráfico asociados a las mismas por personas distintas a los usuarios en ausencia de su consentimiento. Se trató, por lo tanto, de un sistema de protección de datos demasiado frágil, sometido a las decisiones estatales. Esta tendencia empeoró, si cabe, con la Directiva 2006/24/CE, sobre conservación de datos de tráfico en las comunicaciones electrónicas, que impuso a los prestadores de servicios de comunicaciones electrónicas en su art. 3 la obligación de conservar los datos que permitiesen identificar el origen, destino, fecha, hora y duración de cualquier comunicación electrónica, así como el tipo de comunicación realizada, el equipo utilizado y la localización de dicho equipo. Se consideró, con mucha razón, que estas medidas, entre las que se incluía la conservación de datos por un periodo de hasta 24 meses sin necesidad de sospecha o presunción ilícita alguna, suponían un sacrificio de la privacidad

[138] De la Mata Barranco y Pérez Machío, *Derecho Penal Informático,* pp. 136 – 137.

de los ciudadanos en aras de la seguridad, incluso en ausencia de cualquier sospecha de actividad delictiva[139].

Todas estas herramientas jurídicas, aunque pueden encuadrarse, desde un punto de vista genérico, en la lucha contra la ciberdelincuencia, no articularon un sistema efectivo de criminalización general de conductas lesivas de bienes jurídicos merecedores de tutela penal en el ciberespacio. Se limitaron al establecimiento de medidas orientadas a favorecer, sobre todo, aspectos de cooperación policial y judicial y, hasta cierto punto, de medidas de armonización legal, aunque limitadas a sus respectivas materias. La influencia del Convenio sobre la Ciberdelincuencia de Budapest fue perceptible en la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero, si bien tuvo un carácter limitado y mucho más modesto que este en lo concerniente a sus objetivos[140]. No obstante, hay que destacar los avances que introdujo, como la distinción clara entre la protección de los sistemas informáticos y la protección de los datos o de la información que albergaban dichos sistemas informáticos[141]. En cualquier caso, no tardó en ser sustituida por la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI, del Consejo[142].

Aunque la propuesta que condujo a su creación basaba la necesidad de su existencia en, entre otros argumentos, la mejora de las deficiencias que se habían observado en los distintos informes sobre la implementación de la Decisión Marco 2005/222/JAI, en realidad se trataba de una necesidad técnica, toda vez que las decisiones marco, en general, estaban siendo sustituidas de acuerdo a las nuevas formas de proceder de los órganos comunitarios. El texto de la Directiva 2013/40/UE finalmente aprobado marcó como objetivos en su art. 1 la aproximación del Derecho penal de los Estados

[139] De la Mata Barranco y Pérez Machío, *Derecho Penal Informático,* pp. 137 – 138.

[140] De la Mata Barranco y Pérez Machío, *Derecho Penal Informático,* pp. 139 – 141.

[141] Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 352 – 354.

[142] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 233.

miembros en lo relativo a los ataques contra los sistemas de información a través de la implantación de una normativa mínima que definiese las infracciones penales y las sanciones aplicables, así como la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes, como las policiales. Para conseguir esos objetivos, exigió a los Estados miembros que adoptasen las medias necesarias para sancionar como infracciones penales el acceso ilegal a los sistemas de información, la interferencia ilegal en los sistemas de información, la interferencia ilegal en los datos y la interceptación ilegal, añadiendo así una cuarta conducta respecto a las previstas en la sustituida Decisión Marco 2005/222/JAI[143].

Sus arts. 3 a 6 recogen la descripción de las conductas a sancionar como infracciones penales. El art. 3 el acceso sin autorización al conjunto o a una parte de un sistema de información cuando se haya cometido con violación de una medida de seguridad. El art. 4 la obstaculización o interrupción significativas del funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, intencionalmente y sin autorización. El art. 5 borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización. Por último, el art. 6. hace referencia a la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización. Los cuatro artículos, al finalizar la descripción de las conductas, afirman que todas deberían ser sancionadas como infracciones penales al menos en los casos que no sean de menor gravedad, algo extensible al art. 7, relativo al tratamiento de los instrumentos utilizados para cometer las infracciones enumeradas. A través del mismo se pretendió la adopción de las medidas necesarias para garantizar que fuesen sancionables como infracciones

[143] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* pp. 234 – 235.

penales la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de un programa informático, concebido o adaptado principalmente para cometer una infracción de las mencionadas en los arts. 3 a 6, o una contraseña de ordenador, un código de acceso o datos similares que permitiesen acceder a la totalidad o a una parte de un sistema de información, sin autorización y con la intención de ser utilizados con el fin de cometer cualquiera de las infracciones mencionadas en los arts. 3 a 6[144].

El art. 8 exige que se sancionasen la inducción y la complicidad para los supuestos de los arts. 3 a 7, así como la tentativa, solo que, en el caso de esta última, limitándose a las conductas recogidas en los arts. 4 y 5. El art. 9, por su parte, está dedicado a las sanciones, siendo fundamental el art. 9.1, en el que se demanda que se adopten las medidas necesarias para garantizar que las infracciones mencionadas en los arts. 3 a 8 se castiguen con penas efectivas, proporcionadas y disuasorias. En el art. 9.2 se introduce un límite a esta facultad de castigar, especificando que la sanción máxima de las infracciones mencionadas deberá ser de privación de libertad igual o superior a dos años (de nuevo, al menos en los casos que no sean de menor gravedad). En el apartado 2 del art. 9 se prevé una pena algo más grave solo para las infracciones mencionadas en los arts. 4 a 5 cuando se cometan intencionalmente y afecten a un número significativo de sistemas de información, o cuando, cumpliendo el primero de los requisitos, se utilice para su comisión alguno de los instrumentos previstos en el art. 7. En este caso, el castigo será una sanción máxima de privación de libertad de al menos tres años. El art. 9.4 también exige una sanción agravada consistente en una pena máxima de privación de libertad de al menos cinco años para aquellos casos en que la interferencia ilegal en los sistemas de información o en los datos se cometan en el contexto de una organización delictiva con arreglo a la Decisión Marco 2008/841/JAI sin importar el nivel de la sanción que se establezca en la misma, cuando se causen daños graves o cuando se cometan contra el

[144] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 236.

sistema de información de una infraestructura crítica. Por último, el art. 9.5, refiriéndose en exclusiva a las infracciones de los arts. 4 y 5, pide que se pueda contemplar como agravante que las mismas sean cometidas utilizando de manera ilícita datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando con ello daños al propietario legítimo de la identidad. Los artículos 10 y 11, por su parte, exigen en relación a la responsabilidad de las personas jurídicas sanciones efectivas, proporcionadas y disuasorias que incluyan multas de carácter penal o de otro tipo, como, entre otras, la vigilancia judicial[145].

No cabe duda de que esta Directiva 2013/40/UE es la que más previsiones ha introducido en lo que respecta al Derecho penal. Mucho mayores también en importancia que las escuetas menciones al ámbito penal incluidas en la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida también como Directiva NIS. Aunque la misma ha supuesto, no sin motivo, una auténtica revolución en lo que se refiere a la regulación extrapenal de la ciberseguridad en el ámbito comunitario, su existencia responde, sin duda, a esa voluntad de las autoridades de la UE ya señalada con anterioridad según la cual se recurre de forma simultánea a medidas jurídicas penales y no penales. Y es que, si se analiza en profundidad el texto de la Directiva NIS, solo es posible encontrar, en medio de sus elaboradas disposiciones pertenecientes a otros ámbitos, dos escuetas menciones al Derecho penal.

La primera se encuentra en su considerando 8, que afirma que su existencia debe entenderse sin perjuicio de que los Estados miembros puedan adoptar las medidas necesarias para garantizar la protección de los intereses esenciales de su seguridad, preservar el orden público y la seguridad pública, y permitir que se investiguen, detecten y enjuicien las

[145] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* pp. 236 – 237.

infracciones penales. Además, remitiéndose al art. 346 del TFUE, dispensa a los Estados miembros de facilitar información cuya divulgación consideren contraria a los intereses esenciales de su seguridad, remarcando la relevancia de la Decisión 2013/488/UE del Consejo, de 23 de septiembre de 2013, sobre las normas de seguridad para la protección de la información clasificada de la UE, y los acuerdos sobre confidencialidad o los acuerdos informales sobre confidencialidad como el Protocolo para el intercambio de información.

La segunda y última mención al Derecho penal se incardina en el artículo 1.6, que afirma que la Directiva NIS se entenderá sin perjuicio de las acciones emprendidas por los Estados miembros para salvaguardar sus funciones estatales esenciales, sobre todo en lo concerniente a la seguridad nacional, incluyendo las acciones que protejan la información cuya revelación los Estados miembros consideren contraria a los intereses esenciales de su seguridad, así como para mantener el orden público, en particular para permitir la investigación, la detección y el enjuiciamiento de infracciones en el ámbito penal. Se trata, reitero, de dos menciones sumamente escuetas que evidencian la falta de interés del legislador por introducir novedades legales jurídico-penales mediante este texto jurídico.

Algo más de información[146], aunque no mucha más, puede encontrarse en el Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, a través del que se transpuso la Directiva NIS al ordenamiento jurídico español.

En su art. 5, sobre la salvaguarda de funciones estatales esenciales, encontramos, básicamente, una transposición de los elementos que daban forma al considerando 8 y al art. 1.6 de la Directiva NIS, puesto que de acuerdo con el mismo lo dispuesto en el Real Decreto Ley[147] se entenderá

[146] V. Moret Millás, "Un nuevo escenario jurídico para la ciberseguridad en España: el Real Decreto-Ley 12/2018, de Seguridad de las redes y sistemas de información", *Diario La Ley,* no. 9270, 2018, p. 8.

[147] F.J. Donaire Villa, "La nueva regulación sobre ciberseguridad de redes y sistemas de información en España: preguntas y respuestas sobre el Real Decreto-ley 12/2018, de transposición de la Directiva NIS", *Revista de privacidad y derecho digital,* vol. 4, no. 14,

sin perjuicio de las acciones emprendidas para salvaguardar la seguridad nacional y las funciones estatales esenciales, incluyéndose las dirigidas a proteger la información clasificada o cuya revelación fuere contraria a los intereses esenciales del Estado, o las que tengan como propósito el mantenimiento del orden público, la detección, investigación y persecución de los delitos, y el enjuiciamiento de sus autores[148].

El art. 14.3, sobre la cooperación con otras autoridades con competencias en seguridad de la información y con las autoridades sectoriales, resulta mucho más interesante, puesto que ayuda a entender la manera en que el legislador pretende la comunicación entre los ámbitos penal y no penal con el objetivo último de salvaguardar la ciberseguridad. De acuerdo al mismo, cuando los incidentes que se notifiquen presenten caracteres de delito, las autoridades competentes y los CSIRT de referencia darán cuenta de ello, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, al Ministerio Fiscal a los efectos oportunos, trasladándole al tiempo cuanta información posean en relación con ello. A mayor abundamiento, el art. 19.6 establece el deber legal de denunciar los hechos que revistan caracteres de delito ante las autoridades competentes, de acuerdo con lo dispuesto en los arts. 259 y siguientes de la LECrim y en el art. 14.3 del propio Real Decreto Ley. En consecuencia, a pesar de que el despliegue de medios previsto no está dedicado específicamente a la persecución de delitos desde una perspectiva penal, sí existe una conexión entre los mismos y el Derecho penal gracias a la previsión del legislador, que

2019, p. 123. El contenido del Real Decreto Ley es, en su mayor parte, de carácter extrapenal, pero es compatible con la lucha penal contra la ciberdelincuencia.

[148] S. Haataja, “The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach”, *Law, Innovation and Technology,* vol. 9, no. 2, 2017, p. 3. La identificación del autor del delito, indispensable para su enjuiciamiento, es una cuestión esencial en un ámbito en el que el anonimato protege especialmente a los criminales. Quizá el mejor ejemplo sean los ciberataques masivos sufridos por Estonia en el año 2007. Después de negar el Gobierno de la Federación de Rusia todo conocimiento sobre el origen de los mismos, se multó a un estudiante estonio de veinte años por haber lanzado uno de ellos. Aunque algunos expertos valoraron la posibilidad de que los rusos hubiesen otorgado su aprobación a los atacantes para llevar a cabo los ciberataques, otros mantuvieron que resultaba imposible probar quién era el responsable de los mismos en base a la información técnica disponible.

introduce el deber de notificar a las autoridades pertinentes los hechos constitutivos de delito, permitiendo así que se pongan en marcha los mecanismos penales que resulten oportunos por mucho que quien detecte las conductas prohibidas sea, en primera instancia, alguien cuya actividad está centrada en otros ámbitos del derecho.

1.3.2.2 El Reglamento (UE) 2019/881 relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación

Al igual que las decisiones, los reglamentos son actos legislativos vinculantes, con la fundamental diferencia de que estos deben aplicarse en su integridad en toda la UE.

El art. 1.2 del Reglamento (UE) 2019/881, dedicado a determinar su objeto y ámbito de aplicación, deja claro desde el inicio que se entenderá sin perjuicio de las competencias de los Estados miembros en materia de actividades relacionadas con la seguridad pública, la defensa, la seguridad nacional y las actividades del Estado en ámbitos del Derecho penal.

Las únicas referencias al Derecho penal, la ciberdelincuencia o los ciberdelitos que existen en el mismo se encuentran, sobre todo, en los considerandos, y están dedicadas a establecer el papel de ENISA en relación con los mismos. Así, el considerando 15 hace una exposición sobre las importantes medidas que la UE ya ha adoptado para garantizar la ciberseguridad y aumentar la confianza en las tecnologías digitales, entre ellas la Directiva (UE) 2016/1148. ENISA tendría atribuido, en este sentido, un papel clave para respaldar su aplicación, puesto que la lucha eficaz contra la ciberdelincuencia constituye una prioridad importante de la Agenda Europea de Seguridad, la cual, a su vez, contribuye al objetivo general de conseguir un elevado nivel de ciberseguridad. El considerando 40 recoge el deber de ENISA de contribuir a la sensibilización del público sobre los riesgos relacionados con la ciberseguridad, y a la concienciación sobre las ciberamenazas potenciales, incluyendo actividades criminales en línea como

los ataques por suplantación de identidad, o *phishing*, las redes infectadas, o *botnets*, o los fraudes bancarios y financieros, e incidentes de fraude en materia de datos. En último lugar, el art. 7.2, sobre cooperación operativa a nivel de la UE, determina ENISA cooperará a nivel operativo y establecerá sinergias con, entre otros, los servicios que abordan la ciberdelincuencia, evidenciando una vez más, esta vez en el ámbito comunitario, la voluntad de conectar los ámbitos penal y no penal.

Estas escasas referencias al Derecho penal, junto al hecho de que el Reglamento (UE) 2019/881 mencione la Directiva (UE) 2016/1148 y la actividad ya realizada por la UE en relación con el mismo, evidencian que no existía necesidad de introducir regulaciones relativas al ámbito penal en el Reglamento, puesto que, con mejor o peor fortuna, textos jurídicos anteriores habían abordado ya esa tarea, y los objetivos del legislador eran otros[149].

1.3.3 Influencia del Derecho penal de la Unión Europea en la legislación de los Estados miembros

1.3.3.1 Francia

En 2016, se llevó a cabo una renovación completa de la estrategia nacional de ciberseguridad francesa. Tras un periodo de consultas, se realizaron cambios sutiles pero decisivos en el marco conceptual de esta nueva estrategia, incluyendo dentro de la misma a las infraestructuras críticas. El objetivo fue diferenciar la estrategia nacional de Francia tanto desde un punto de vista tecnológico como doctrinal a través de una defensa de sus intereses fundamentales en el ciberespacio. La estrategia no diferenciaba entre la defensa de los intereses nacionales y la lucha contra la ciberdelincuencia, continuando con la tendencia iniciada ocho años atrás

[149] V. Moret Millás, "Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español", *Bie3: Boletín IEEE*, no. 5, 2017, p. 746. Se mencionan lagunas de la Directiva NIS y la ausencia de novedades en aspectos importantes, como los relativos a la cooperación en materia de Derecho penal.

según la cual la seguridad debía entenderse como un continuo que engloba desde la protección del pueblo hasta la defensa en los ámbitos militar y estratégico. La defensa conjugaría, por lo tanto, elementos pasivos y activos, incluyendo tanto la monitorización pasiva como las represalias activas para proteger el país cuando los intereses nacionales de Francia estuviesen en riesgo a causa de un ciberataque[150].

La principal influencia del Derecho penal francés en relación con la ciberseguridad no procede, sin embargo, del ámbito de la UE, sino del internacional, en particular del Convenio sobre la Ciberdelincuencia de Budapest, a partir del cual el Estado francés reforzó la normativa orientada a lucha contra este tipo de delitos. Antes de su existencia, Francia ya disponía en su CP de varios artículos cuyo objetivo era la erradicación del espionaje industrial y comercial a través de la sanción de distintas conductas como la alteración de datos (art. 321-1), la intrusión en un sistema informático, sobre todo para el conocimiento de datos confidenciales (art. 323-1) y los atentados contra un sistema (art. 323-2). El denominador común de todas estas conductas sancionables residía en el hecho de su ejecución en ausencia de autorización y en el ámbito de su comisión: el ciberespacio[151].

Al ratificar el Convenio, el Estado francés asumió las obligaciones que había contraído internacionalmente y adoptó todo un arsenal de medidas legislativas para combatir la delincuencia informática según lo dispuesto en

[150] P. Baumard, *Cybersecurity in France*, 1ª ed., Cham, Springer, 2017, pp. 60 – 62. No sorprende comprobar que esta nueva actitud por parte de Francia estuvo motivada por los ataques terroristas sufridos por la población gala en territorio francés en los años 2015 y 2016. Las normas desarrolladas en aquella época recibieron enormes críticas tanto de la ciudadanía como de los políticos, que, como es lógico, no toleraron la pretensión de aceptar la interceptación en tiempo real todas las comunicaciones digitales francesas, incluyendo correos electrónicos, llamadas telefónicas, e incluso mensajería instantánea.

[151] A.I. Pérez Machío, "Consideraciones de derecho comparado: la proyección de la normativa internacional en el tratamiento penal de la delincuencia informática", en J.L. De la Cuesta Arzamendi (dir.), *Derecho Penal Informático*, Cizur Menor, Navarra, Aranzadi, 2010, pp. 147 – 148. A través de un análisis de la implementación de las normas internacionales en países como Alemania o Francia es posible obtener una visión legal más completa. Incluyo dicho análisis en este capítulo primero porque ambos países pertenecen a la UE, y la mayoría de los analizados en el capítulo segundo, dedicado al derecho comparado, no.

el tratado internacional. A partir de entonces, el legislador francés distinguió dos grandes categorías de infracciones: las que estaban relacionadas de manera directa con las TIC y las que suponían la comisión a través de Internet de hechos lesivos que afectasen a bienes jurídicos tradicionalmente tutelados.

En la primera de estas dos categorías se ubicaron los atentados contra el sistema de tratamiento automático de datos, la difusión de programas que permitiesen cometer un atentado contra el sistema de tratamiento automático de datos, las infracciones a la ley informática y a la libertad sobre la protección de datos personales, las infracciones relativas a cheques (entre las que se encuentra la difusión de programas que permitiesen la fabricación de cheques falsos) y las infracciones a la legislación sobre criptología. En la segunda categoría, el legislador francés incluyó y sancionó las estafas informáticas.

Además, hubo un esfuerzo por reforzar la cooperación policial en un intento de combatir más eficientemente lo que, en aquel entonces, se consideraba una delincuencia de nuevo cuño. Dentro de la Gendarmería fueron surgiendo, también, grupos especializados en esta clase de delitos, como el Departamento de lucha contra la cibercriminalidad o la Oficina Central de lucha contra la criminalidad, los cuales llevan desde el año 1998 investigando los delitos relacionados con las TIC que afecten al Estado francés[152]. En 2014, se creó un cargo de prefecto encargado de la lucha contra las ciberamenazas.

1.3.3.2 Alemania

Desde un principio, el pueblo alemán percibió el *hacking* con cierta ambivalencia: por un lado, los ataques que sucedían hicieron que se concienciase de los riesgos de las TIC para los usuarios, sobre todo en lo relativo a la protección de datos[153]; al mismo tiempo, se consideró el *hacking*

[152] Pérez Machío, *Derecho Penal Informático*, pp. 148 – 149.

[153] K. Dimmroth y W.J. Schünemann, “The Ambiguous Relation Between Privacy and Security in German Cyber Politics: A Discourse Analysis of Governmental and

como un nuevo tipo de delito que preocupó notablemente a la población. Como resultado, Alemania fue uno de los primeros países en tipificar el delito de *hacking* en 1986. No obstante, el parágrafo 202a del StGB solo incluyó el robo de datos, mas no la intrusión en un sistema tras atravesar sus medidas de seguridad. Desde 2007, y con la intención de ajustarse a las disposiciones del Convenio sobre la Ciberdelincuencia de Budapest, la mera intrusión en un sistema informático protegido también es castigada[154].

El Estado alemán ha estructurado su política de ciberseguridad sobre tres pilares: la actitud preventiva basada en el uso de la tecnología, la importancia de la protección de los datos personales a través de medidas legales, técnicas y organizativas inspiradas en la elevada importancia que la intimidad tiene para la ciudadanía y, por último, el fortalecimiento de los poderes de investigación contra la ciberdelincuencia de las autoridades. Estos tres pilares tienen algo en común: son de tipo preventivo y requieren la colaboración[155] de los ciudadanos. Se basan en la idea de que es posible garantizar la ciberseguridad a través de la estructuración adecuada de esta tecnología, de la protección legal de las personas frente al uso indebido de la misma y de la persecución constante del quebrantamiento de la ley[156].

Centrándonos en el ámbito del Derecho penal, existen dos particularidades a destacar. La primera es que, de nuevo, la influencia sobre el ordenamiento jurídico interno del Estado alemán es mayor por parte del Derecho internacional (esto es, del Convenio sobre la Ciberdelincuencia de Budapest) que del Derecho de la UE. La segunda es que no existen grandes

---

Parliamentary Debates", en W.J. Schünemann y M. Baumann (eds.), *Privacy, Data Protection and Cybersecurity in Europe,* Cham, Springer, 2017, p. 100. Tradicionalmente, la protección de datos personales siempre ha tenido una gran importancia en Alemania.

[154] M. Schallbruch e I. Skierka, *Cybersecurity in Germany,* 1ª ed., Cham, Springer, 2018, p. 6. Algunos de los estados federados de Alemania, como la Baja Sajonia, tienen fiscales especializados en los ciberdelitos.

[155] M. Górka, "The Cybersecurity Strategy of the Visegrad Group Countries", *Politics in Central Europe,* vol. 14, no. 2, 2018, p. 83. En la República Checa también se promueve la intervención no solo gubernamental, sino de los ciudadanos, de quienes se espera que tomen parte activa en las medidas de prevención.

[156] Schallbruch y Skierka, *Cybersecurity in Germany,* p. 12.

diferencias en el tratamiento que el Derecho penal francés otorga a la ciberdelincuencia respecto al StGB alemán. Igual que en el primero, en el StGB se sancionan conductas tradicionalmente típicas, solo que consideradas como novedosas a causa del medio comisivo empleado. Se sancionan también en ambos los comportamiento ilícitos previstos en el Convenio. En cuanto a la estructura, el StGB incardina los delitos informáticos en distintos parágrafos ubicados en ámbitos tan dispares como los destinados a tipificar la inviolabilidad del secreto, la estafa o los daños. Se incrimina, así, el acceso dolosa no autorizado a datos transmitidos electrónicamente, magnéticamente o de forma inmediatamente accesible (parágrafo 202a del StGB). También la alteración de los mismos borrándolos, eliminándolos, inutilizándolos o alterándolos (parágrafo 303a del StGB), cuando se trate de los datos a los que se refiere el parágrafo 202a antes mencionado. Lo mismo sucede con el sabotaje informático, que consiste en destruir una elaboración de datos que sea de esencial importancia para una industria ajena, una empresa ajena o una autoridad (parágrafo 303b del StGB). Por último, la estafa informática se tipifica en el parágrafo 263a del StGB. Es necesario realizar una serie de precisiones sobre este delito[157].

Los elementos esenciales del tipo (la acción engañosa, la causación del error y la disponibilidad patrimonial) requirieron una readaptación por tratarse de engaños al equipo informático. Atendiendo a la redacción final del precepto, el perjuicio patrimonial que tiene lugar consiste esencialmente o bien en influir en el resultado de la elaboración de datos a través de la manipulación del programa informático relacionado con aquellos datos, o bien en la utilización de datos incorrectos o incompletos, o en la utilización no autorizada o intromisión ilegítima en una red o sistema informáticos que permita acceder a datos reales y correctos. Una de las críticas de la doctrina penalista alemana consistió en que el StGB otorgaba una protección excesiva

[157] Pérez Machío, *Derecho Penal Informático*, p. 149.

a la integridad de los datos en detrimento de la integridad del sistema, que no gozaba del mismo nivel de protección a pesar de ser muy importante[158].

Mención aparte merece la tipificación como delito del espionaje de datos en el parágrafo 202a del StGB, que planteó cierta polémica hasta la nueva redacción de su apartado 1, con la que se aclaró que la conducta típica no consistía en la adquisición de datos, sino en el acceso ilícito[159] del usuario a ciertos datos que no le están destinados, llevando aparejada una pena privativa de libertad de hasta tres años, o una pena de multa[160].

1.4 Límites del Derecho penal internacional y comunitario en relación con la ciberseguridad

Nunca hay que considerar justa, por sí misma, la ley positiva, sino que es conveniente mantener una actitud crítica ante la misma[161]. Igualmente, en un mundo en que las nuevas tecnologías han permitido que las personas emitan opiniones en ocasiones carentes de fundamento que pueden crear situaciones lesivas para los intereses ajenos[162], tampoco debe considerarse que las masas tienen siempre la razón solo por su número[163].

---

158 Pérez Machío, *Derecho Penal Informático*, p. 150.

159 A. T. Drăgan, "Illegal Access to a Computer System from the Standpoint of the Current Criminal Code", *Journal of Legal Studies,* vol. 23, no. 37, 2019, p. 37. En el CP de países como Rumanía, la existencia de medidas de seguridad orientadas a restringir o prohibir el acceso se contempla solo en el tipo agravado.

160 Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 354 – 356.

161 M. Dobrinoiu, "Opinions on the Unconstitutionality Aspects Related to the Cybersecurity Law", *Challenges of the Knowledge Society,* vol. 5, no. 1, 2015, p. 28. El debate parece ser el mismo en todas partes: el equilibrio entre la seguridad y la libertad. Incluso en Rumanía se han llevado a cabo análisis sobre su legislación relativa a la ciberseguridad llegando a la conclusión de que determinados aspectos de la misma eran inconstitucionales por no proteger la norma suficientemente los datos personales y la intimidad.

162 C. Stahn, *A Critical Introduction to International Criminal Law,* 1ª ed., Cambridge, Cambridge University Press, 2019, p. 50. Las nuevas tecnologías pueden resultar aún más incendiarias que la prensa tradicional.

163 T. Owen, W. Noble y F.C. Speed, *New Perspectives on Cybercrime,* 1ª ed., Cham, Springer, 2017, p. 48. Las redes sociales y los cada vez más frecuentes linchamientos que se producen en las mismas son el mejor ejemplo de esto. Hoy, una persona puede

Teniendo esto en cuenta, las voces críticas de los expertos se convierten en fundamentales para valorar determinados aspectos técnicos, como los límites que existen en el Derecho penal internacional y comunitario en lo que respecta a la persecución de los delitos que afectan a la ciberseguridad. En un escenario complejo[164] en el que países con tradiciones jurídicas muy distintas se ven obligados a colaborar[165], pervive aún la confusión incluso en la terminología utilizada. Como ya señalé con anterioridad, un *hacker* no tiene que ser necesariamente un criminal, puesto que su definición es la de una persona que se deleita en tener una comprensión íntima del funcionamiento interno de un sistema, de los ordenadores y de las redes informáticas en particular. El *hacker* busca hacer de Internet un sitio más seguro para los organismos públicos y para cualquier usuario que vaya a utilizarlo. Sin embargo, se ha generalizado la utilización de este nombre para definir lo que, en puridad, es un *cracker*, cuya actividad orientada a alcanzar fines contrarios al ordenamiento jurídico sí encaja con la figura del ciberdelincuente[166]. Si no se ha sabido aclarar algo tan sencillo en un ámbito como el Derecho penal, en el que resulta esencial la precisión, deben analizarse con el mismo espíritu crítico todos los demás elementos que componen las herramientas jurídicas internacionales relacionadas con los ciberdelitos que afectan a la ciberseguridad.

No todo el mundo considera que el Convenio sobre la Ciberdelincuencia de Budapest sea el tratado internacional adecuado para

enfrentarse al acoso y derribo de las multitudes en las redes sociales antes incluso de haber sido condenada en firme en un juicio con todas las garantías.

[164] R. Zafra Espinosa de los Monteros, "La bunkerización del Espacio de Libertad, Seguridad y Justicia", en M.I. González Cano (coord.), *Integración europea y justicia penal*, Valencia, Tirant lo Blanch, 2018, p. 165.

[165] A. Kańciak, "An Analysis of the Legal Systems and Mechanisms Introduced in the European Union in the Fight Against Cyberspace Threats", *Internal Security,* vol. 8, no. 2, 2016, p. 219. A esta obligación de colaborar entre países se suma el deber de cada país de adaptarse a la armonización de la UE.

[166] Y. Rubio Viñuela, "Los claroscuros de la ciberseguridad", *Revista Tribuna norteamericana,* no. 30, 2019, p. 21. Si todavía existen dudas incluso a nivel terminológico, creo que lo más prudente, en un ámbito tan sensible como el del Derecho penal, es tener una actitud precavida y garantista con los derechos ajenos.

perseguir esta clase de delitos[167]. Las profundas deficiencias señaladas por sus críticos son, entre otras, la exageración que supone, atendiendo al escaso número de Estados parte, considerar el Convenio como referente mundial en la materia; el plazo de tiempo excesivo que, en determinados casos, requiere su proceso de implementación, siendo la media de más de ocho años y medio para países que no son miembros del Consejo de Europa; el hecho de que algunos de los países que lo han ratificado no lo han implementado en su totalidad; lo difícil que resulta para países pequeños o con problemas económicos ponerlo en práctica, toda vez que existen costes indirectos como mantener el punto de contacto de la Red 24/7 que no son asumibles por todos los países; la ausencia de un enfoque integral, al haber lagunas en relación con aspectos como la admisibilidad de la prueba electrónica; lo desactualizado que está, como demuestra el hecho de que ni mencione el uso de Internet con fines terroristas, y la reticencia del Consejo de Europa a actualizarlo; y que contradice principios fundamentales de Derecho internacional, como sucede en el caso de su controvertido art. 32 b), el cual, durante las investigaciones, permite unas injerencias que no respetan la soberanía nacional ajena[168].

Por último, también hay que dejar claro que el Convenio no es un cheque en blanco en la lucha contra la ciberdelincuencia. Además de los

[167] I. Rogachev, "The European Convention on Cybercrime is Inadequate to the Task", *Security Index: A Russian Journal on International Security,* vol. 17, no. 4, 2011, p. 8. Conviene reiterar que, hoy en día, Rusia no es un Estado parte del Convenio porque sus autoridades consideran, en el ejercicio de su autonomía, que la base del tratado que obliga a compartir información supone una violación de su soberanía.

[168] M. Gercke, "10 years Convention on Cybercrime: Achievements and Failures of the Council of Europe´s Instrument in the Fight against Internet-related Crimes", *Computer Law Review International,* vol. 12, no. 5, 2011, pp. 144 – 149. El mencionado art. 32 b) del Convenio de Budapest permite a un Estado parte, sin necesidad del consentimiento de otro, tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en el territorio de otro Estado parte, siempre que obtenga el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos por medio de ese sistema informático. Lo dispuesto en este art. 32 b) contradice, por lo tanto, el deber de respetar la soberanía nacional ajena durante las investigaciones consagrado en el Derecho internacional.

necesarios límites impuestos por la ética[169] [170] [171], desde una perspectiva legal no siempre corresponderá aplicar la responsabilidad penal. Así, en el caso de la interceptación ilícita, esta debe cometerse de manera deliberada e ilegítima, estando justificada si la persona que intercepta la comunicación dispone de un permiso para hacerlo, si actúa siguiendo las órdenes o está autorizado por los participantes en la transmisión, o si la vigilancia está autorizada legítimamente en el interés de la seguridad nacional o la detección de delitos por parte de las autoridades pertinentes. Además de excepciones como las anteriores, tampoco se prevé que constituyan un delito como tal, por no ser ilegítimas, las prácticas comerciales comunes como el empleo de *cookies*[172]. Del mismo modo, las medidas puramente defensivas de ciberseguridad tienen muy pocas posibilidades de conllevar un ilícito penal. Las medidas ofensivas, en cambio, sí suelen ser idóneas para ser encuadradas en alguno de los tipos previstos por el legislador, de ahí que suela recomendarse que se eviten[173]. Queda claro, a partir de lo anterior, que el Convenio tiene establecidos unos límites en relación con las conductas a perseguir, y que bajo ningún concepto es posible ir más allá de las mismas.

En cuanto a la UE, el principal límite de su derecho viene impuesto por la propia escasez de su contenido, toda vez que, como ya he expuesto, goza de una capacidad limitada para legislar en el ámbito del Derecho penal, por

---

[169] J. Pattison, "From defence to offence: The ethics of private cybersecurity", *European Journal of International Security,* vol. 5, no. 2, 2020, p. 253. A las empresas privadas se les permite lanzar medidas de ciberseguridad defensivas, pero no medidas ofensivas, a causa de los problemas que llevan aparejadas.

[170] I. Van de Poel, "Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security", en M. Christen, B. Gordijn, M. Loi (eds.), *"The Ethics of Cybersecurity",* Cham, Springer, 2020, p. 45.

[171] M. Manjikian, *Cybersecurity Ethics: An Introduction,* 1ª ed., Abingdon, Routledge, 2018, p. 23.

[172] Consejo de Europa, *Informe explicativo del Convenio sobre la Ciberdelincuencia de Budapest*, Estrasburgo, Consejo de Europa, 2001, p. 11. Este informe se compone de 330 apartados que explican y ayudan a matizar algunas de las disposiciones del Convenio sobre la Ciberdelincuencia de Budapest.

[173] A. Van Dine, "When is Cyber Defense a Crime? Evaluating Active Cyber Defense Measures Under the Budapest Convention", *Chicago Journal of International Law,* vol. 20, no.2, 2020, pp. 563 – 564.

considerarse el mismo un símbolo de la soberanía[174] de los Estados miembros. Esto tiene como consecuencia que los Estados miembros que también son Estados parte en el Convenio sobre la Ciberdelincuencia de Budapest puedan elegir con libertad la extensión con la que trasladar a sus ordenamientos jurídicos estatales sus disposiciones, con la única limitación de lo dispuesto en el tratado.

[174] N.J. De la Mata Barranco, "La influencia del Derecho de la Unión Europea en el Derecho penal de sus estados miembros", en J.L. De la Cuesta Arzamendi (dir.), *Adaptación del derecho penal español a la política criminal de la Unión Europea,* Cizur Menor, Navarra, Aranzadi, 2017, p. 107. En efecto, los Estados son reacios a la limitación de soberanía que supondría la creación de un Derecho penal supraestatal. Además, se han apuntados otras causas para este subempleo del Derecho penal en el ordenamiento de la UE, como la tipología de materias objeto del Derecho penal comunitario y la tipología de sus destinatarios.

CAPÍTULO II

LA CIBERSEGURIDAD EN EL DERECHO PENAL COMPARADO DE PAÍSES FUERA DEL ÁMBITO DE LA UNIÓN EUROPEA

2.1 La diversidad de estrategias nacionales en materia de ciberseguridad a nivel mundial

Garantizar un nivel elevado de ciberseguridad mediante, entre otras herramientas legales, un CP capaz de proteger las redes y sistemas informáticos frente a las últimas novedades tecnológicas requiere información abundante y actualizada sobre la manera en que están afrontando este desafío legal otros países que, aunque fuera del ámbito de la Unión Europea, comparten una tradición cultural y jurídico-penal en sentido amplio (*lato sensu*, puesto que en su mayoría son países anglosajones) con España. Resulta imposible, por encontrarse mezclados los datos en las investigaciones de referencia, separar por completo los Estados miembros de la UE de aquellos que no pertenecen a la misma, de manera que, siendo, como veremos, muchas de sus características comunes, y no pudiendo realizar con todos los países un análisis diferenciado tan específico como el dedicado a Francia y a Alemania en el capítulo anterior, es inevitable que se mencionen también Estados comunitarios dentro de este capítulo principalmente destinado a analizar aquellos que no pertenecen a la UE. Considero esta manera de estructurar la presentación de información la más lógica, como pone de manifiesto el análisis de las formas de regulación en el Derecho penal comparado del delito de acceso ilícito a un sistema de información.

Y es que, sin importar el país al que nos refiramos, la recopilación y análisis de datos veraces sobre la ciberseguridad en el Derecho penal comparado resulta muy compleja[175], puesto que, a nivel internacional, existe

[175] J. Kosseff, *Cybersecurity Law,* 1ª ed., Hoboken, NJ, Wiley, 2017, p. 339. Esta complejidad es aún mayor teniendo en cuenta la diversidad de formas en las que cada

una tendencia por parte de cada país a reservarse los datos sobre ciberdelincuencia. La lógica que subyace tras esta reserva es que compartir información sobre la misma equivale a confesar una vulnerabilidad propia, toda vez que muchos ciberataques están dotados de cierto carácter innovador. Algunos países son reticentes, por tanto, a cooperar con otros, pues dicha cooperación implica revelar su nivel real de capacidad para detectar y responder a los ciberataques, así como otras posibles vulnerabilidades susceptibles de ser explotadas o de ser señaladas como debilidades.

Una vez compartidas, las vulnerabilidades se traducen en oportunidades para desarrollar campañas orientadas a atacar a otros países. La decisión de revelarlas o no es, por lo tanto, un constante dilema del prisionero: compartir demasiada información es un error desde un punto de vista estratégico, pero compartir poca puede poner en peligro un sistema de defensa al ignorar o subestimar una amenaza. De lo que no cabe duda es de que las vulnerabilidades en el ámbito informático son susceptibles de ser utilizadas como armas. En un escenario en el que no existe el respaldo de entidades geopolíticas como la UE, y en el que cada país debe tomar decisiones individuales en sus relaciones con otros países cuyos gobiernos no siempre albergan buenas intenciones, no existen incentivos para compartir información sobre las vulnerabilidades propias[176]. Esto explica la existencia de distintas estrategias nacionales elaboradas por cada país para hacer frente a, entre otras amenazas, los delitos que afectan a la ciberseguridad, las cuales ven definido y delimitado su grado de desarrollo por las diferentes realidades socioeconómicas y tecnológicas que caracterizan a cada nación. En áreas con un bajo índice de penetración de Internet, la concienciación respecto al valor estratégico del ciberespacio es muy baja. En el polo opuesto, la controvertida actividad de la FVEY (compuesta por Reino Unido, EE. UU., Canadá, Australia y Nueva Zelanda, países obligados por el tratado de

país ha regulado delitos como el acceso ilícito a los sistemas de información y las divergencias históricas apreciables entre sus distintos textos penales.

[176] Baumard, *Cybersecurity in France*, p. 40.

cooperación conjunta en la inteligencia de señales UKUSA), está a la vanguardia del uso estratégico del ciberespacio[177].

Es importante aclarar que el hecho de que muchos países no hagan públicas sus estrategias nacionales por los motivos a los que ya he hecho referencia no significa que no dispongan de ellas. Aunque la antigüedad no está relacionada con su grado de implantación y ni con su madurez, existen diferencias en este sentido entre los países que sí las han hecho públicas. En efecto, Canadá desarrolló su propia estrategia nacional de ciberseguridad en el año 2010, Reino Unido, Australia y Nueva Zelanda en 2011, y Suiza en 2012. A pesar de estas diferencias, todas las estrategias tienen unas características que pueden utilizarse para determinar sus convergencias y divergencias a efectos comparativos.

2.1.1 Convergencias

Los puntos en común que pueden apreciarse entre las distintas estrategias nacionales en materia de ciberseguridad son tres: primero, todas vertebran la ciberseguridad como materia prioritaria para sus respectivos gobiernos, y proponen el establecimiento de un liderazgo único para la coordinación de las acciones relacionadas con la misma; segundo, destacan la gravedad y complejidad de las ciberamenazas y del grado de organización que han alcanzado los grupos de delincuentes y de terroristas detrás de ellas; tercero, ponen de manifiesto la importancia de la cooperación internacional ante este riesgo, puesto que el mismo tiene alcance mundial. Lo anterior permite determinar que la gran mayoría de estas estrategias se estructuran sobre los mismos tres pilares: la identificación de las ciberamenazas, la delimitación de responsabilidades[178], y el establecimiento de líneas de

[177] C. Solé Pascual y A. Hernández, “Estrategias nacionales de ciberseguridad en el mundo”, *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones,* no. 66, 2014, p. 34. La alianza de inteligencia FVEY fue acusada en 2013 de espiar a los ciudadanos y de no responder ante las leyes de los países que la integran. A pesar de todo, esto no ha afectado a su actividad.

[178] Solé Pascual y Hernández, “Estrategias nacionales de ciberseguridad en el mundo”, p. 36.

actuación y de medidas concretas que permitan responder a las mismas como corresponde.

2.1.2 Divergencias

Un análisis más detallado de las estrategias nacionales en materia de ciberseguridad evidencia que, además de los puntos en común, existen diferencias sustanciales, en especial en la manera en que cada país prevé hacer frente a las ciberamenazas. Los elementos que las diferencian son, más concretamente, cuatro: primero, en lo concerniente a la organización, en algunos países existe una elevada fragmentación entre los actores estatales dotados de competencia en el ámbito de la ciberseguridad, sin que muchas de las estrategias solucionen este aspecto ni tampoco lo aborden a nivel internacional, puesto que no mencionan los medios para cooperar con otros países en materia de ciberdelitos; segundo, solo algunos países, como Reino Unido o EE. UU., prevén una dotación presupuestaria expresa para la estrategia; tercero, en muchos casos, no es posible encontrar una tipificación formal interna de los actos que se consideran delictivos en el ciberespacio, dificultando su persecución y propiciando la existencia de lagunas jurídicas y de paraísos para la ciberdelincuencia en regiones con normativas opacas; cuarto, la fragmentación jurídica que existe a nivel internacional, incluso a pesar de los acuerdos internacionales existentes en este ámbito, dificultan la colaboración transnacional[179].

2.2 Interpretación de los datos contenidos en los cinco pilares del Global Cybersecurity Index

La UIT lleva a cabo de manera periódica una encuesta entre los 193 países que la forman con objeto de elaborar el Índice Global de

[179] Solé Pascual y Hernández, “Estrategias nacionales de ciberseguridad en el mundo”, p. 37.

Ciberseguridad, más conocido como Global Cybersecurity Index[180]. Este índice examina los cinco pilares (legal, técnico, organización, desarrollo de capacidades y cooperación) del Programa Mundial de Ciberseguridad de la UIT, realizando preguntas relativas a 25 indicadores para cada uno de los pilares que cada país debe responder para su posterior análisis y comparación. Estos datos permiten medir, en relación con los países participantes, la evolución de su compromiso con la ciberseguridad, los progresos que han realizado, los avances regionales y los desequilibrios entre sus niveles de participación en iniciativas de ciberseguridad, aspectos todos ellos que, aunque no hacen referencia específica al Derecho penal, sin duda resultan influyentes en el desarrollo de la tipificación de los delitos que afectan a la ciberseguridad.

A nivel mundial, destacan con diferencia los países europeos y las naciones más desarrolladas de Occidente. En el continente europeo, Reino Unido encabeza la clasificación, seguido de Francia, Lituania, Estonia y España. Aunque todos los indicadores mejoran a nivel mundial, el mayor progreso se aprecia en el pilar legal, destacando la importancia de la cooperación entre países para el desarrollo de la ciberseguridad, aspecto que es posible extender al Derecho procesal penal y a las novedades en desarrollo en relación con el mismo que analizaré en el capítulo siguiente de esta investigación.

[180] Unión Internacional de Telecomunicaciones, *Global Cybersecurity Index (GCI) 2018*, Ginebra, Unión Internacional de Telecomunicaciones, 2018, pp. 2 – 6. Más de la mitad de la población mundial dispone ya de acceso a Internet. A finales de 2018, el 51,2% de dicha población, un porcentaje equivalente a casi cuatro mil millones de personas, podía conectarse a la Red. Esto convierte en un objetivo esencial la adecuada protección del ciberespacio. De acuerdo a las previsiones de la propia UIT, esta protección será aún más necesaria, puesto que se espera que el 70% de la población mundial tenga acceso a Internet en el año 2023. Un estudio de IBM determinó que en 2018 el coste mundial derivado de la sustracción de datos ascendió en un 6,4%. Al mismo tiempo, ciertas proyecciones previeron que los daños derivados de los ciberdelitos se cuantificarían económicamente en dos billones de dólares estadounidenses a finales de 2019. En cuanto a las modalidades delictivas, los ataques de *ransomware* han disminuido, pero han aumentado tanto la sustracción de datos como los ataques a las infraestructuras críticas. Son destacables, por último, las profundas diferencias existentes entre países en lo concerniente al nivel de conocimiento de que disponen para la implementación de legislación orientada a hacer frente a los ciberdelitos.

España se sitúa en el séptimo puesto a nivel mundial, solo por detrás de Reino Unido, EE. UU., Francia, Lituania, Estonia y Singapur. Su puntuación es de 0,896 (sobre un total de 1,000), desglosable de acuerdo a los cinco pilares mencionados: legal (nota máxima de 0,200), técnico (0,180), organización (de nuevo, nota máxima de 0,200), construcción de capacidades (0,168) y cooperación (0,148). El informe destaca aspectos positivos a nivel legislativo y organizativo como la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional o la existencia del CNCS, que fortalece la coordinación, la colaboración y la cooperación entre quienes ostentan responsabilidades en el ámbito de la ciberseguridad. Con objeto de comprender mejor el Global Cybersecurity Index y de profundizar en su relación con el Derecho penal, es necesario interpretar los datos correspondientes a cada uno de sus cinco pilares: legal, técnico, organización, construcción de capacidades y cooperación.

2.2.1 Legal

El pilar legal es, sin duda, el más relacionado con el Derecho penal, puesto que evalúa la existencia de un marco legal relativo a la ciberseguridad y a los ciberdelitos en un país concreto. Los países europeos destacan en el mismo, como sucede en el caso de Bélgica, que ha desarrollado un plan de acción para garantizar la seguridad en su entorno digital haciendo frente de forma efectiva a las prácticas ilegales. En Dinamarca, se ha promovido la utilización de la firma digital como factor adicional para garantizar aún más la seguridad en las transacciones en línea. Lituania, por su parte, no solo tiene una ley específicamente dedicada a la ciberseguridad desde 2015, sino que cuenta con distintos planes dedicados a, entre otros objetivos, la gestión de incidentes en el ciberespacio, que permiten que la Oficina de Policía Criminal de Lituania investigue determinados ciberdelitos. En Moldavia se ha implementado un programa de ciberseguridad entre cuyos objetivos está la prevención y la persecución de la ciberdelincuencia. Por último, en el Reino Unido la NCA lidera y coordina la lucha contra los ciberdelitos en su territorio

en estrecha colaboración con sus socios nacionales e internacionales, entre los que se cuenta el EC3. Entre sus operaciones exitosas está el cierre en 2018 de una página web que había servido para llevar a cabo cuatro millones de ataques DDoS a nivel mundial, atacando sus dueños, que fueron detenidos durante la operación, incluso a los principales bancos del Reino Unido[181].

2.2.2 Técnico

El pilar técnico evalúa la existencia de medidas técnicas que permitan afrontar el desarrollo de la ciberseguridad a nivel nacional. En Bélgica, el CCB proporciona cobertura a nivel nacional en relación con las incidencias en el ciberespacio, y en Dinamarca se está desarrollando la tecnología necesaria para hacer un seguimiento en tiempo real de las ciberamenazas desde el CFCS. Serbia permite, desde 2017, que se denuncien actividades ilegales cometidas en Internet a través de un portal creado al efecto, las cuales son trasladadas a la autoridad correspondiente en caso de que se trate de delitos tipificados[182].

2.2.3 Organización

El tercer pilar, dedicado a la organización, se centra en la evaluación de la existencia de un marco organizativo capaz de afrontar los desafíos relacionados con la ciberseguridad a nivel nacional, incluyendo tanto las estructuras como las medidas de gobernanza. Aunque toda Europa destaca en este ámbito, hay que mencionar especialmente a Albania, a los Países Bajos y a España, contando esta última con una herramienta de análisis de riesgos y de gestión de sistemas de información aprobado por la OTAN y

[181] Unión Internacional de Telecomunicaciones, *Global Cybersecurity Index (GCI) 2018*, pp. 31 – 35.

[182] Unión Internacional de Telecomunicaciones, *Global Cybersecurity Index (GCI) 2018*, pp. 36 – 41.

adaptado a las últimas modificaciones legislativas a nivel de la UE y a las actuales necesidades de seguridad[183].

2.2.4 Construcción de capacidades

El pilar dedicado a la construcción de capacidades evalúa la existencia de programas de I+D, educación y capacitación en el ámbito de la ciberseguridad, así como de profesionales cualificados y de entidades del sector público que los fomenten. Europa, de nuevo, destaca en este ámbito, especialmente en lo relativo a los programas de I+D, que casi duplican a los de las regiones que más se le acercan en la clasificación. A nivel estatal, en Bélgica el CCB ha llevado a cabo múltiples campañas para educar en ciberseguridad. En Dinamarca se han destinado fondos para la investigación en nuevas tecnologías, incluyendo la ciberseguridad, y además se han creado y financiado unidades de ciberseguridad especializadas en cada uno de los sectores críticos para la sociedad, como el sanitario, entre cuyos objetivos se encuentra el desarrollo de estrategias adaptadas tanto a las amenazas que se prevean en relación con los mismos como a sus vulnerabilidades específicas[184].

2.2.5 Cooperación

El último de los cinco pilares evalúa la cooperación, es decir, la existencia de asociaciones y redes de intercambio de información que la hagan posible. En España, el CNCS fortalece las relaciones de coordinación, colaboración y cooperación entre las autoridades públicas con responsabilidades en el ámbito de la ciberseguridad, así como entre el sector público y el sector privado, facilitando la coordinación de acciones orientadas

[183] Unión Internacional de Telecomunicaciones, *Global Cybersecurity Index (GCI) 2018*, pp. 41 – 43.

[184] Unión Internacional de Telecomunicaciones, *Global Cybersecurity Index (GCI) 2018*, pp. 43 – 48.

a garantizar un elevado nivel de seguridad[185]. Aunque no se refleje expresamente en el Global Cybersecurity Index, los países más avanzados han realizado grandes progresos en el ámbito del Derecho procesal penal, reformando de manera expresa su legislación procesal para enfrentarse a los nuevos problemas que plantea la ciberdelincuencia, incluyendo la creación de nuevas medidas tecnológicas de investigación. En la UE, Bélgica reformó su legislación procesal penal hace ya veinte años mediante la Ley de 28 de noviembre de 2000 Relativa a Delitos Informáticos, que introdujo medidas como las ya mencionadas en dicho país. Reino Unido, por su parte, adaptó también su legislación en el año 2000 a través de la Regulation of Investigatory Powers Act 2000 (popularmente conocida como RIPA). En Francia destacan, en este sentido, la Ley no. 2004-575 de 21 de junio de 2004 sobre la confianza en la economía digital y la reforma del Código de Procedimiento Penal francés en virtud de la Ley no. 2011-267 de 14 de marzo de 2014 de orientación y programación del desarrollo de la seguridad interior. En Italia, sobresale el Codice in materia di protezione dei dati personali, aprobado mediante el Decreto legislativo no. 196, de 30 de junio de 2003. En último lugar, en Portugal las disposiciones del Convenio de Budapest en este ámbito se adaptaron a su derecho interno a través de la Ley no. 109/2009, de 15 de septiembre[186].

2.3 Regulación en el Derecho penal comparado del delito de acceso ilícito a un sistema informático

El Convenio sobre la Ciberdelincuencia de Budapest, en cuyos arts. 2 a 6 se imponía a sus Estados parte la obligación de regular en sus propias normas penales internas los delitos contra la disponibilidad, la integridad y la confidencialidad de las redes y sistemas informáticos, tuvo una influencia decisiva a nivel mundial en la regulación del delito de acceso ilícito a un

[185] Unión Internacional de Telecomunicaciones, *Global Cybersecurity Index (GCI) 2018*, pp. 48 – 51.

[186] Barrio Andrés, *Delitos 2.0,* p. 58.

sistema informático, delito de intrusión informática o, de acuerdo a mi propuesta de *lege ferenda* en el capítulo tercero de esta investigación, delito de *cracking*.

En el ámbito de la UE, la ya mencionada Decisión Marco 2005/222/JAI del Consejo de la UE, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, desarrolló en gran medida el citado Convenio, obligando a los Estados miembros a castigar penalmente tanto el acceso intencionado no autorizado a un sistema de información (art. 2) como la perturbación de los sistemas informáticos (art. 3). A pesar de su sustitución por la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra sistemas de información[187], muchos de los países de nuestro entorno comunitario incluyeron en sus legislaciones penales el intrusismo informático. No obstante, y pese a compartir el mismo marco normativo europeo, existe una gran disparidad en lo referente a la manera en que esta conducta se ha tipificado en la legislación penal interna de cada país en concreto. Atendiendo a dicho criterio, resulta posible establecer tres categorías: primera, la regulación de este delito en normas especiales; segunda, la tipificación del *cracking* en un título o capítulo propio y diferenciado del CP; y tercera, que corresponde a España, la regulación de esta conducta junto a otros delitos ya existentes.

2.3.1 Primera categoría: regulación del delito en normas penales especiales

Países como Estados Unidos, Reino Unido, Francia u Holanda han optado por esta vía, que supone la creación de una norma penal especial para regular el acceso ilícito a un sistema informático. En EE. UU., la Computer Fraud and Abuse Act (CFAA) de 1986 prohibió el acceso a un sistema informático sin contar con autorización, o excederse de la misma en caso de disponer de ella. La CFAA ha sido reformada en 1988, 1989, 1990, 1994, 1996, 2001, 2002 y 2008. En Reino Unido, fue un grave caso de

[187] Almenar Pineda, *El delito de hacking*, p. 98.

cracking lo que impulsó la promulgación de la Computer Misuse Act 1990 (CMA), que castiga los accesos indebidos.

En la UE, Francia prohibió el acceso fraudulento a un sistema de elaboración de datos o el mantenimiento en el mismo mediante su Ley no. 88-19, de 5 de enero de 1988, sobre el fraude informático, que incluía la posibilidad de aumentar la sanción si de estas acciones se derivaba la supresión o la modificación de los datos en él contenidos, o si se alteraba el funcionamiento de dicho sistema[188]. En Chipre, la Ley no. 22(III)/2004 ratificó el Convenio de Budapest prohibiendo de manera explícita los accesos ilícitos. Por último, en Portugal, la Lei da criminalidade informática (Ley no. 109/91, de 17 de agosto), por influencia de la Recomendación no. R (89) 9 sobre criminalidad informática de 13 de septiembre de 1989, regulaba en su art. 7 los supuestos de acceso no autorizado a una red o sistema informáticos con la intención de obtener un beneficio o ventaja ilegítimas. No obstante, este art. 7 fue derogado por el art. 6 de la ya mencionada Ley no. 109/2009, de 15 de septiembre, que transpuso el Convenio de Budapest y la Decisión Marco 2005/222/JAI y tipificó el acceso ilegítimo a un sistema informático tras desarrollar en su art. 2 una serie de definiciones relativas a estas conductas[189]. Además de la promulgación de estas normas especiales, la otra técnica empleada para hacer frente al desafío de incluir el *cracking* en el CP ha sido la tipificación de un nuevo delito en el mismo, ya sea otorgándole un título o capítulo propio y diferenciado, o bien regulándolo junto a otros delitos ya existentes, como en España[190].

2.3.2 Segunda categoría: regulación del delito en un título o capítulo propio y diferenciado

Los países pertenecientes a esta categoría, que se caracterizan por regular el intrusismo informático en un título o capítulo propio y diferenciado

[188] Barrio Andrés, *Delitos 2.0,* p. 57.

[189] Almenar Pineda, *El delito de hacking*, p. 99.

[190] Barrio Andrés, *Delitos 2.0,* p. 57.

del CP, han optado por dotar de un cierto grado de autonomía al delito de *cracking*, apartándolo de otros delitos pero sin llegar a desarrollar una norma penal especial. Es el caso de Bélgica, que a través de la Ley de 28 de noviembre de 2000 relativa a la criminalidad informática introdujo un Título IX bis en su CP de 8 de junio de 1867 dedicado a los delitos contra la disponibilidad, la integridad y la confidencialidad de los sistemas y datos informáticos almacenados, procesados o transmitidos por dichos sistemas. El art. 550 bis del mismo texto regula, en ese mismo Título IX bis, las conductas consistentes en acceder a un sistema informático o en mantenerse dentro del mismo. El CP búlgaro, tras su reforma en el año 2007, dedica su Capítulo IX a la ciberdelincuencia, recogiendo el *cracking* en el art. 319a. En Croacia, el CP de 26 de octubre de 2011 regula los delitos contra los sistemas informáticos, los programas y los datos en su Capítulo XXV, y el tipo básico de intrusismo informático en su art. 266.

Finlandia introdujo un Capítulo 38 dedicado a los delitos contra las informaciones y las comunicaciones en su CP de 19 de diciembre de 1889 mediante la Ley 578/1995, de 21 de abril, que fue reformada por la Ley 368/2015, de 10 de abril, estando el delito de *cracking* regulado penalmente en la Sección 8, bajo la rúbrica de acceso informático. En último lugar, Hungría incluyó la regulación penal de este delito en el art. 300/C del Capítulo XLIII de su CP del año 1978, bajo la rúbrica dedicada a los crímenes contra la informática y los sistemas de información. No obstante, tras la reforma llevada a cabo el 18 de diciembre de 2001, este precepto pasó a referirse al acceso no autorizado a un sistema informático mediante la vulneración de medidas de seguridad o a la permanencia no autorizada en el mismo[191].

2.3.3 Tercera categoría: regulación del delito junto a otros delitos ya existentes

Pertenecen a este grupo los países como España, que se caracterizan por haber tipificado el delito de *cracking* junto a otros delitos que tutelan

[191] Almenar Pineda, *El delito de hacking*, p. 100.

bienes jurídicos distintos a la ciberseguridad. Esta ha sido la vía elegida por la mayoría de países de nuestro entorno.

En Alemania, tras la enmienda introducida el 7 de agosto de 2007, el StGB tipifica en su Capítulo XV, parágrafo 202a, las conductas de espionaje, en las que se puede encuadrar el acceso no autorizado a datos protegidos mediante la superación de medidas de seguridad. Desde su reforma del año 2002, el CP austríaco contiene en su Sección V (dedicada a las violaciones de la privacidad y de ciertos secretos profesionales), parágrafo 118a, el acceso ilícito a los sistemas informáticos. En Dinamarca, el CP de 27 de septiembre de 2005, reformado el 21 de diciembre de ese mismo año, recoge el delito de *cracking* en el art. 263, que está encuadrado en el Capítulo XXVII, en el cual se regulan los delitos contra el honor y contra ciertos derechos individuales. El CP de Eslovaquia tiene la particularidad de contener en su sección 247 un requisito típico consistente en la intención de causar daño o perjudicar a un tercero, o de obtener un beneficio injusto al acceder sin permiso a un sistema informático. En Eslovenia, el intrusismo informático se encuentra tipificado en el art. 225 de su CP bajo la rúbrica dedicada a la entrada a un sistema de información en ausencia de autorización, que forma parte del Capítulo XXIII, y por lo tanto se considera un delito contra la propiedad. Tras la reforma llevada a cabo por la denominada RT I 12.07.2014, también se considera un delito contra la propiedad en Estonia, en cuyo CP, Capítulo XIII, División II, Subdivisión III, art. 217, se regula el acceso ilegal a los sistemas informáticos.

Francia fue uno de los países pioneros en la tipificación del acceso ilícito a los sistemas informáticos, puesto que esta conducta forma parte del CP francés desde el año 1988. Después de la firma por parte de las autoridades galas del Convenio de Budapest el 10 de enero de 2006, se encuentra recogida en su art. 323-1, que forma parte de un Capítulo III dedicado a los ataques contra los sistemas de tratamiento automatizado de datos[192].

[192] Almenar Pineda, *El delito de hacking*, p. 101.

No fue hasta 2001 cuando Grecia introdujo en su CP de 1951 el art. 370Γ, dentro de un Capítulo XXII en el que se regula la vulneración de secretos. Por su parte, Holanda incluyó en el Título V (referido a los delitos contra el orden público) de su CP de 3 de marzo de 1881, mediante Ley de 1 de junio de 2006, el art. 138ab, que exige, también, el elemento intencional en el acceso indebido[193]. El caso de Irlanda es muy particular, puesto que aunque posee una norma especial que regula el intrusismo informático, tipifica la conducta junto a otros delitos en la Sección 5 de la llamada Criminal Damage Act de 1991. En Italia, el CP de 19 de octubre de 1930 ya regulaba el *cracking* en su art. 615 ter antes de firmar el Convenio de Budapest, como consecuencia de la Ley no. 547 de 23 de diciembre de 1993. En la actualidad, este artículo no ha sufrido modificaciones, y continúa bajo la rúbrica relativa al acceso abusivo a un sistema informático o telemático, que pertenece a la Sección IV, es decir, a los delitos contra la inviolabilidad del domicilio. En Letonia, el CP de 17 de junio de 1998 dedica su Capítulo XX a los delitos contra la seguridad general y el orden público, estando reguladas las conductas de acceso arbitrario a sistemas de procesamiento automatizado de datos en su sección 241, creada a raíz de la Ley de 28 de abril de 2005.

El CP lituano de 26 de septiembre de 2000 regula el *cracking* de forma específica en el art. 198-1 de su Capítulo XXX, relativo a los delitos contra la seguridad de los datos electrónicos y sistemas de información, que fue introducido en la reforma del CP de Lituania del año 2004. La Ley de 15 de julio de 1993 hizo posible que el CP de Luxemburgo de 16 de junio de 1879 incluyese en su Título IX, Capítulo II, Sección VII.1, delitos como el intrusismo informático en su art. 509. El CP de Malta de 10 de junio de 1854 destaca por su exhaustiva regulación del *cracking* en su art. 337. Esto se debe a la reforma llevada a cabo el 27 de marzo de 2001, que añadió un Subtítulo V relativo a abusos informáticos dentro de su Título IX (dedicado a los delitos contra la propiedad y la seguridad pública)[194]. En Polonia, el Acta de 24 de octubre de 2008 reformó el CP polaco de 6 de junio de 1997, incluyendo

[193] Almenar Pineda, *El delito de hacking*, p. 102.

[194] Almenar Pineda, *El delito de hacking*, pp. 102 – 103.

dentro de su Capítulo XXXIII (que recoge los delitos contra la información protegida) un art. 267 que tipifica el acceso indebido a los sistemas de información. En la República Checa, la Ley 571/1991 hizo posible que el antiguo CP checo de 29 de noviembre de 1961 dedicase, dentro de su Capítulo IX, relativo a los delitos contra la propiedad, un art. 257.a a los daños o abusos contra los datos contenidos en soportes de grabación. Tras la aprobación del nuevo CP mediante la Ley de 8 de enero de 2009, el acceso no autorizado a sistemas informáticos y soportes de información pasó a estar directamente tipificado en el art. 230, dentro del Título V, relativo a los delitos contra la propiedad. En Rumanía, la Ley Anticorrupción 161/2003 incluía un Título III específicamente dedicado a la prevención y a la lucha contra la ciberdelincuencia, en cuyo Capítulo III, Sección 1 (dedicada a los delitos contra la integridad y la confidencialidad de datos y sistemas informáticos), el art. 42.1 tipificaba el acceso no consentido a un sistema informático. La Ley 161/2003 estaba destinada de manera expresa a garantizar la transparencia de figuras como altos cargos oficiales, funcionarios y empresarios, así como a prevenir y sancionar la corrupción, de modo que era necesario que el nuevo CP aprobado a través de la Ley de 17 de julio de 2009 incluyese en el mismo, como hizo, los delitos de acceso a sistemas y datos informáticos. Esto se materializó en su art. 360, recogido dentro de su Título VII, Capítulo VI, dedicado a los delitos contra la seguridad y la integridad de los sistemas de información y de los datos.

Por último, Suecia también castiga el *cracking* en su CP de 21 de diciembre de 1962 tras la reforma introducida por la Ley de 26 de abril de 2007 y la Ley de 15 de mayo de 2014, encuadrándolo en su sección 9.c, entre los delitos contra la libertad y la paz del Capítulo IV.

Un defecto que comparten la mayoría de las legislaciones citadas es que no son lo suficientemente minuciosas en su regulación del *cracking*, al limitarse muchas de ellas a la regulación del tipo básico sin conceder a esta conducta la autonomía necesaria respecto a otras, con los problemas interpretativos que esto puede ocasionar sobre todo en relación con la determinación del bien jurídico que se pretende proteger. Así, los defectos de

la legislación española se extienden a muchos de los CCPP pertenecientes a otros países del mundo, lo que refuerza mi convicción tanto en relación con la necesidad de crear un nuevo título en el CP para los delitos que afectan a la ciberseguridad como en lo concerniente a la adecuación de considerar la ciberseguridad como un bien jurídico protegido autónomo.

Y es que, a pesar de la extensa regulación de estos accesos ilícitos que realizan algunos países, como Croacia, Finlandia, Hungría, Malta, Portugal y Reino Unido, la mayoría de CCPP de la UE han optado por incluirlos entre los delitos contra la intimidad (es el caso de Alemania, Austria, Grecia y Polonia), contra el honor y otros derechos individuales (Dinamarca), contra la propiedad (Eslovaquia, Eslovenia, Estonia, Francia, Malta, República Checa y Luxemburgo)[195], contra el orden público (Holanda), de daños (Irlanda), contra la inviolabilidad del domicilio (Italia), contra la libertad y la paz (Suecia), o contra la seguridad (Letonia, Lituania y Rumanía), resultando esto problemático para la delimitación del bien jurídico protegido, y poniendo de manifiesto la necesidad de un bien jurídico protegido autónomo como la ciberseguridad que permita la unificación de criterios a nivel internacional.

Mucho más minoritaria resulta la opción de regular sistemáticamente los delitos informáticos (de hecho, solo países como Reino Unido, Portugal o Chipre han optado por la misma) o de dotarles de cierta autonomía mediante un título o capítulo propio y diferenciado (Bélgica, Bulgaria, Croacia, Finlandia o Hungría). Esto tiene como resultado que muy pocos países tipifiquen con el detalle necesario el *cracking*, siendo fundamental definir los conceptos esenciales relacionados con el mismo y regular más allá del tipo básico, y todo ello en un título o capítulo propio y diferenciado que permita evitar los errores que conlleva inevitablemente la amalgama actual de artículos, remisiones y bienes jurídicos protegidos[196].

[195] Almenar Pineda, *El delito de hacking*, p. 103.

[196] Almenar Pineda, *El delito de hacking*, p. 104.

2.4 Análisis de la regulación de los delitos que afectan a la ciberseguridad en el Derecho penal comparado

2.4.1 Reino Unido

Incluso teniendo en cuenta la influencia del Brexit[197] en las relaciones jurídicas entre la UE y el Reino Unido, este país continúa siendo de esencial importancia al liderar la clasificación mundial en materia de ciberseguridad[198]. No es posible encontrar en él una norma específica que regule la ciberseguridad, pero sí un conjunto de normas penales especiales[199] entre las que destaca, por encima de todas las demás, la Computer Misuse Act 1990 (CMA), ya que prevé de forma específica los accesos ilícitos a los sistemas informáticos. En efecto, tras la reforma efectuada por la Police and Justice Act 2006, su Sección 1 (1) prevé que incurrirá en este delito cualquier persona que, en ausencia de la debida autorización, y teniendo consciencia de ello, lleve a cabo utilizando un ordenador cualquier actividad orientada a acceder a un programa o a datos contenidos en un sistema informático, o a hacer posible dicho acceso. Aunque la redacción de la conducta típica es sorprendentemente tosca (o quizá se describe de manera tan genérica que transmite esa impresión, profundizando en esta tendencia la Sección 1 (2) a través de una desacertada y amplísima descripción del objeto material del delito explicando no cuál es, sino solo que el mismo no se limita a un *numerus*

[197] D. Borrajo Valiña, "La integración en la seguridad y defensa de la UE: las iniciativas post-Brexit y la futura articulación de la cooperación con el Reino Unido", *Revista Aranzadi Unión Europea*, no. 4, 2019, p. 71.

[198] L.G. Fernández Delgado (edit.), "Reino Unido lidera el nuevo ránking de ciberseguridad mundial, seguido de EE.UU. quedando España en un meritorio séptimo lugar", *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, vol. 28, no. 135, 2019, p. 140. Su posición en el Global Cybersecurity Index evidencia la capacidad del Reino Unido para la implementación y la actualización periódica de los elementos que componen su sistema de seguridad cibernética con objeto de adaptarlos a las necesidades cambiantes.

[199] D.I. Bainbridge, "Hacking. The Unauthorised Access of Computer Systems. The Legal Implications", *The Modern Law Review*, vol. 52, no. 2, 1989, p. 236. Esta manera de estructurar los delitos que afectan a la ciberseguridad tiene aspectos tanto positivos como negativos: es positiva la flexibilidad que proporciona al ordenamiento jurídico, pero, en ocasiones, puede resultar difícil saber qué norma aplicar a un caso concreto.

clausus), resulta fascinante comprobar la manera en que coincide con mi propuesta de *lege ferenda* para el delito de *cracking* en el CP español. Si se exceptúan la vulneración de medidas de seguridad y la extensión de la conducta típica al hecho de mantenerse en el conjunto o en una parte de un sistema de información contra la voluntad de quien tenga legítimo derecho a la exclusión del sujeto activo, es posible encontrar también en la legislación del Reino Unido la misma conducta, la exigencia de actuar sin autorización y el elemento subjetivo del delito, aunque no se exija el ánimo de lesionar la ciberseguridad y baste con actuar con consciencia respecto a las implicaciones que conlleva la acción. Pero es que coinciden, incluso, las consecuencias jurídicas del delito, siendo la pena máxima prevista para este delito en la Sección 1 (3) (c) la pena de prisión de dos años, lo cual hace posible, en el caso británico, solicitar la extradición del criminal.

Las Secciones 2 y 3 del mismo texto legal recogen los tipos agravados de este delito, consistiendo el primero en cometer el delito de *cracking* como medio para la comisión de un delito fin, siendo necesario no el mero intento de acceder a un sistema informático, como en el tipo básico, sino haber conseguido el acceso al mismo. La Sección 3, por su parte, castiga las modificaciones no autorizadas, estando pensada para, entre otros, el uso de virus.

La interceptación ilegal intencionada de las comunicaciones, incluyendo las enviadas o recibidas por medio de ordenadores, se recoge en la Sección 3 de la Investigatory Powers Act 2016 (IPA), estando previsto como castigo una pena máxima de dos años de prisión.

En cuanto a los datos personales, su protección se estructura sobre tres pilares: el RGPD, la Data Protection Act 2018 (DPA) y la Network and Information Systems Regulation 2018 (NISR)[200]. No obstante, la herramienta jurídica que ha permitido ir más allá del ámbito administrativo y criminalizar

[200] M.J. Taylor y T. Whitton, “Public Interest, Health Research and Data Protection Law: Establishing a Legitimate Trade-Off between Individual Control and Research Access to Health Data”, *Laws,* vol. 9, no. 1, 2020, p. 4. La Data Protection Act 2018 (DPA) cuenta entre sus objetivos la salvaguarda del interés público.

ciertos comportamientos en relación con los datos personales ha sido la DPA, en cuya Sección 170 se tipifica la obtención ilegal de datos personales.

Es importante destacar, en este sentido, la manera en que la jurisprudencia y la doctrina del Reino Unido entienden la información confidencial. A raíz del Caso *Oxford v Moss (1979) 68 Cr App Rep 183*, el acceso a datos, su lectura y su utilización no constituyen un delito perseguible mediante la Theft Act 1968, puesto que la información confidencial no encaja en la definición de propiedad de su Sección 4 a pesar de que la misma hace referencia a la propiedad intangible, y por lo tanto no puede considerarse como robada desde una perspectiva material. Conductas como esta encajan, más bien, en la Sección 1 (1) de la Computer Misuse Act 1990 (CMA) y, cuando se llevan a cabo como medio para la comisión de un delito fin, resulta de aplicación la Sección 2 (1) del mismo texto legal.

En último lugar, la Sección 3ZA (3) (f) de la mencionada Computer Misuse Act 1990 (CMA) tipifica la utilización consciente de un ordenador para un propósito prohibido que cause daños o cree un riesgo significativo de causar daños a la salud humana, protegiendo de manera específica los servicios sanitarios. La pena prevista en la Sección 3ZA (6), consistente en un máximo de 14 años de prisión, es elevada de por sí, pero el tipo agravado de las Secciones 3ZA (7) (a) y (b), previsto para los casos en los que esta conducta provoque daños o cree un riesgo significativo de causar daños serios a la salud humana o a la seguridad nacional, se castiga con una elevadísima pena de cadena perpetua en prisión[201].

2.4.2 Estados Unidos de América

[201] K. Stoddart, “UK cyber security and critical national infrastructure protection”, *International Affairs,* vol. 92, no. 5, 2016, p. 1105. En el Reino Unido, la NCA es la encargada de combatir los delitos más graves. Para adaptarse a los avances de la tecnología y poder perseguir, entre otros, los delitos que afectan a la ciberseguridad, la NCA incorpora en su seno la National Cyber Crime Unit (NCCU), que absorbió y fusionó las ya desaparecidas Police Central e-Crime Unit (PCeU) y Serious Organised Crime Agency (SOCA).

Incluso antes de convertirse en una de las partes contratantes del Convenio sobre la Ciberdelincuencia de Budapest[202] [203], los EE. UU. ya llevaban años combatiendo la delincuencia en la Red[204] [205]. No obstante, fue entonces cuando introdujeron en el ámbito de su derecho interno disposiciones orientadas a sancionar con penas de hasta 20 años de cárcel conductas de muy diversa naturaleza cometidas en el ciberespacio. Las herramientas jurídicas utilizadas fueron las leyes federales[206] [207], las cuales, en contraposición a las leyes estatales, son susceptibles de aplicación en todo el territorio de EE. UU[208]. Más específicamente, el Título 18 del USC es el principal CP del Gobierno federal de los EE. UU., pues recopila tanto los delitos federales como elementos de Derecho procesal penal. En su Parte I, dedicada a la tipificación de delitos, el Capítulo 47 contiene una § 1030 que tipifica la intromisión dolosa en un sistema informático[209]. Desde un punto de

[202] F. Wells, "Hacked off: How Germany and the United States are Dealing with the Continuous Threat of Cyber Attacks", *National Security Law Brief,* vol. 10, no. 1, 2020, p. 473. En ambos casos, EE. UU., con el objetivo de proteger su seguridad nacional, se ha caracterizado por perseguir de manera inmediata, rápida y agresiva mediante largas investigaciones a quienes acceden a sus redes informáticas gubernamentales.

[203] J.L. Contreras, L. DeNardis, y M. Teplinsky, "Mapping Today's Cybersecurity Landscape", *The American University Law Review,* vol. 62, no. 5, 2013, p. 1130. El aumento de las ciberamenazas hizo que ya en 2013 se reconociese que la ciberseguridad era fundamental para garantizar la seguridad nacional de EE. UU.

[204] M.E. O'Connell, "Cyber Security without Cyber War", *Journal of Conflict & Security Law,* vol. 17, no. 2, 2012, p. 209. Algunos autores afirman que la ciberseguridad debería regularse fuera del ámbito militar. No obstante, en EE. UU. muchos de los expertos más destacados en este ámbito trabajan para el ejército.

[205] Pérez Machío, *Derecho Penal Informático*, p. 151.

[206] B.K. Payne y L. Hadzhidimova, "Cyber Security and Criminal Justice Programs in the United States: Exploring the Intersections", *International Journal of Criminal Justice Sciences,* vol. 13, no. 2, 2018, p. 401.

[207] C.M. Dennis y D.A. Goldman, "Data Security Laws and the Cybersecurity Debate", *Journal of Internet Law,* vol. 17, no. 2, 2013, p. 10. Los autores desarrollan un listado de leyes federales sobre ciberseguridad.

[208] K.D. Ashley, "Introduction: Cybersecurity in Pittsburgh", *Pittsburgh Journal of Technology Law and Policy,* vol. 14, no. 2, 2014, p. 274. Esto resulta muy importante, porque los delitos que afectan a la ciberseguridad se cometen en todos los estados que componen los EE. UU. Así, el University of Pittsburgh Medical Center tuvo que acabar admitiendo que una sustracción de datos que, en principio, habían considerado sin importancia, había puesto en peligro en realidad la información personal de más de 27.000 de sus empleados, y que la información se había utilizado, posteriormente, para la comisión de multitud de delitos.

[209] Pérez Machío, *Derecho Penal Informático*, p. 152.

vista académico, el análisis de su estructura resulta fascinante, puesto que difiere por completo de la manera en que las leyes europeas prevén los delitos que afectan a la ciberseguridad, por lo general en artículos claramente separados en atención a criterios como el bien jurídico protegido. Esta § 1030 incluye delitos que afectan a la ciberseguridad tan distintos como el acceso ilícito a un sistema informático y la sustracción de datos en la § 1030 (a) (2) (C) como los daños informáticos apenas unas líneas después, en la § 1030 (a) (5) (A), (B) y (C). En el primer caso, la consecuencia jurídica del delito, en ausencia de antecedentes, es una pena de prisión máxima de 1 año, una pena de multa, o ambas, de acuerdo a la § 1030 (c) (2) (A). En el caso del delito tipificado en la § 1030 (a) (5) (B), la consecuencia jurídica prevista en la § 1030 (c) (4) (A) (i) (IV) es una pena de prisión máxima de 5 años, una pena de multa, o ambas, cuando se haya provocado un peligro para la seguridad o para la salud públicas[210].

En el Capítulo 119 del mismo texto legal, la § 2511 tipifica la interceptación de las comunicaciones electrónicas, telefónicas, radiofónicas e incluso orales, y la § 2512 fabricar, distribuir, poseer y publicitar dispositivos prohibidos idóneos para ello. Por último, dentro de su Capítulo 121, la § 2701 prevé la conducta consistente en acceder de forma ilícita a comunicaciones almacenadas electrónicamente, castigando el tipo básico con una pena máxima de 1 año de prisión, con una multa, o con ambas, en ausencia de antecedentes.

Además del Título 18 del USC, EE. UU. cuenta con leyes penales especiales de gran importancia a nivel federal, siendo la más destacada la a su vez muy criticable Ley Patriótica de 26 de octubre de 2001. Y la considero criticable porque, en su origen, se la consideró como legislación de emergencia creada tras los trágicos acontecimientos que tuvieron lugar el 11 de septiembre de 2001 en suelo estadounidense, ampliando las prerrogativas

[210] M. Erbschloe, *Threat Level Red. Cybersecurity Research Programs of the U.S. Government,* 1ª ed., Boca Raton, FL, CRC Press, 2017, p. 178. También en EE. UU. se reconoce la importancia de la salud pública y de los servicios de asistencia sanitaria, teniendo ambos la consideración de sectores industriales críticos.

de las autoridades para vigilar las comunicaciones de las personas e introduciendo penas hasta de cadena perpetua en caso de relación directa del sujeto activo con grupos terroristas[211].

Entre su articulado, resulta de especial interés lo siguiente: la Sección 216, que equipara las comunicaciones a través de Internet con las comunicaciones tradicionales tras reconocer el desarrollo que las primeras han experimentado y la necesidad de regularlas; la Sección 814, que establece las consecuencias jurídicas del *cracking* y prevé una pena de prisión de hasta 10 años, o 20 en el caso de los reincidentes, para quienes ataquen ordenadores protegidos de EE. UU. o de países extranjeros sin importar la cuantía del daño causado, y una pena de hasta 5 años de prisión para quienes ataquen otros ordenadores y ocasionen pérdidas por un valor superior a 5.000 dólares estadounidenses; y lo más importante, la tipificación del ciberterrorismo, que incluye una definición del *cracker* coincidente una vez más con mi propuesta de *lege ferenda*, y de acuerdo con la cual es un *cracker* quien, con intención de provocar un daño, causa cualquier deterioro a la disponibilidad o a la integridad de datos, programas o sistemas, sin importar la cuantía del daño causado[212]. Si bien no se hace referencia a la confidencialidad, esto puede atribuirse a una pobre técnica legislativa, que también puede percibirse en aspectos como la mención a datos, programas o sistemas, cuando los dos primeros forman parte del *software* de los sistemas informáticos, y protegiendo dichos sistemas estos quedan también protegidos.

Existen, además, dos aspectos profundamente criticables en relación con la Ley Patriótica: la carencia de capacidad persuasiva de su aumento punitivo, y la ausencia de proporcionalidad entre el delito cometido por el *cracker* y la consecuencia jurídica del mismo. La restricción de libertades individuales y de garantías, así como los excesivos poderes concedidos a las autoridades gubernamentales resultan aún más inquietantes si se tiene en

[211] Pérez Machío, *Derecho Penal Informático*, p. 153.
[212] Pérez Machío, *Derecho Penal Informático*, p. 154.

cuenta el actual carácter permanente de esta norma[213]. No ha sido la primera vez, ni será la última, en que utilizando objetivos indudablemente loables, como la protección de nuestro pueblo, se desarrolla una herramienta jurídica que, a medio plazo, resulta lesiva para sus intereses y, a largo plazo, puede llegar a utilizarse contra el mismo, como en una persecución de todas las personas cristianas que no se arrodillen ante una ley gentil injusta.

En último lugar, hay que reconocer la gran versatilidad de la que están dotados los sistemas legislativos anglosajones, puesto que en los mismos es posible legislar con gran rapidez en relación con las nuevas tecnologías. Es el caso de la Secure 5G and Beyond Act 2020, de 23 de marzo de 2020, que supone la creación de una norma que obliga a desarrollar una estrategia que garantice la seguridad de las comunicaciones inalámbricas llevadas a cabo mediante una tecnología específica: el tan controvertido y criticado 5G.

Además de la legislación, agencias como el FBI desarrollan profundos análisis en relación con los delitos que afectan a la ciberseguridad que resultan de sumo interés para obtener una perspectiva más amplia de la manera en que los mismos se desarrollan en EE. UU.

2.4.2.1 Conclusiones del Internet Crime Report 2019 del FBI

El FBI, a través del IC3, elabora anualmente el Internet Crime Report, un informe en el que se refleja su creciente actividad, que casi se ha duplicado en cinco años[214]. Sus conclusiones pueden dividirse en dos grupos: aquellas que hacen referencia a los ciberdelitos en general y aquellas en las que puede

[213] Pérez Machío, *Derecho Penal Informático*, p. 155.

[214] Federal Bureau of Investigation, *Internet Crime Report 2019,* Washington, D.C., Federal Bureau of Investigation, 2020, p. 5. En los cinco años previos a 2020, el IC3 recibió un total de 1.707.618 denuncias relacionadas con los ciberdelitos. La media fue de 340.000 denuncias anuales, distribuidas del siguiente modo: 288.012 en el año 2015, 298.728 en 2016, 301.580 en 2017, 351.937 en 2018 y 467.361 en 2019. Como puede apreciarse, el número de denuncias recibidas en 2019 casi duplicó a las recibidas en 2015. El coste económico correspondiente a la actividad delictiva de estos cinco años asciende a más de diez mil millones de dólares estadounidenses, triplicando la cifra del año 2019 (más de tres mil millones) a la de 2015 (que asciende a poco más de mil millones). Ante estas cifras, no resulta extraño que combatir la ciberdelincuencia sea una de las prioridades del FBI en su misión de proteger al pueblo estadounidense.

distinguirse información específica correspondiente a los delitos que afectan a la ciberseguridad. La mención de las primeras me parece igualmente importante porque, aunque reflejan datos sobre ciberdelitos en sentido general, es la única manera de analizar una información muy valiosa que, por desgracia, no puede ser más detallada y específica por las propias limitaciones del contenido del informe.

2.4.2.1.1 Resultados generales relativos a los ciberdelitos

En primer lugar, el análisis del rango de edad de las víctimas durante el año 2019 evidencia que la tendencia es ascendente hasta cierta edad, para después disminuir hasta llegar a los mayores de sesenta años, franja en la que el número se dispara de nuevo. En efecto, la cifra asciende a lo largo de las primeras tres franjas de edad: menores de 20 años (10.724 víctimas), personas entre 20 y 29 años (44.496) y personas entre 30 y 39 años (52.820). En las dos siguientes franjas de edad se aprecia un descenso muy ligero, con 51.864 víctimas en la franja de edad correspondiente a las personas de entre 40 y 49 años, y 50.608 en la franja de edad que corresponde a las personas de entre 50 y 59 años. El descenso se detiene abruptamente en la última de las franjas, dedicada a las personas de más de 60 años, siendo la cifra de víctimas de 68.013, casi veinte mil más que en la franja de edad inmediatamente anterior. Este último dato justifica la existencia de normas como la Elder Abuse Prevention and Prosecution Act 2017 (de nuevo, una herramienta jurídica nueva para reaccionar ante un problema específico), dedicada a la protección de los ancianos[215].

En segundo lugar, la clasificación de países con más víctimas en el año 2019 excluyendo a los EE. UU. está encabezada por el Reino Unido, con 93.796 víctimas. Canadá es el país siguiente, pero con una notabilísima diferencia de más de 90.000 víctimas (3.721), cifra que se estabiliza en este punto de la clasificación y continúa descendiendo más progresivamente en países como Australia (1.298 víctimas), Francia (1.243), Bélgica (1.031),

[215] Federal Bureau of Investigation, *Internet Crime Report 2019,* pp. 12 – 16.

Alemania (850), Suiza (438), Italia (428), España (358) y Rusia (349). Al ser el nivel de desarrollo tecnológico muy similar en todos estos países, la enorme diferencia en el número de víctimas en esta clasificación podría deberse no tanto a un mayor número de ciberataques cometidos en territorio del Reino Unido, puesto que resultaría desmesurado en especial en comparación con países como Rusia o Australia, sino a la gran capacidad que posee dicho país para la detección de esta clase de delitos y para su posterior clasificación.

En tercer y último lugar, los estados con más víctimas de ciberdelitos en EE. UU. en 2019 fueron California (con 50.132 víctimas), Florida (27.178), Texas (27.178) y Nueva York (21.371), y los que más pérdidas económicas sufrieron como consecuencia de los mismos fueron, a su vez, California, Nueva York, Florida y Ohio, destacando las pérdidas del estado de Nueva York, que ascendieron a una cifra de 573.624.151 dólares estadounidenses[216].

2.4.2.1.2 Resultados específicos relativos a los delitos que afectan a la ciberseguridad

De entre los delitos que afectan a la ciberseguridad, el más cometido durante el año 2019 en territorio de EE. UU., con diferencia, fue la estafa informática, modalidad delictiva que sufrieron un total de 114.702 víctimas. La sustracción de datos personales tuvo lugar en 38.218 ocasiones, siendo el segundo delito en esta clasificación, seguida por los daños informáticos, en relación con los cuales es necesario realizar una matización. Y es que si bien existen distintas maneras de llevar a cabo este delito, no todas fueron igual de utilizadas, y la amplitud con la que el Internet Crime Report expone las acciones típicas realizadas permite categorizar las distintas modalidades de daños informáticos dependiendo del modo utilizado para cometerlos. Así, destacó el uso de *malware* (2.373 delitos de daños informáticos cometidos a través del mismo) ligeramente por encima del *ransomware* (2.047), quedando

[216] Federal Bureau of Investigation, *Internet Crime Report 2019,* pp. 17 – 22.

los ataques DoS en tercer lugar (1.353). Por último, los ciberdelitos que lesionaron de manera específica los servicios sanitarios estadounidenses fueron 657, y creo esencial mencionarlos por la enorme importancia que el ámbito sanitario, siempre en relación con los delitos que afectan a la ciberseguridad, adquirirá en los siguientes capítulos de esta investigación.

En lo concerniente a las consecuencias económicas de estos delitos, la sustracción de datos personales encabezó la clasificación superando holgadamente a la estafa informática, con unas pérdidas anuales en 2019 de 120.102.501 dólares estadounidenses. La estafa informática, y más concretamente conductas como el *phishing*, ocuparon el segundo lugar con unas pérdidas de 57.836.379 dólares estadounidenses, tras el cual, esta vez de manera coincidente con la clasificación de ciberdelitos en base al número de víctimas, estuvieron los daños informáticos en sus distintas modalidades, las cuales alteraron su orden respecto a dicha clasificación. En efecto, el *ransomware* fue la modalidad que más pérdidas económicas ocasionó en 2019: 8.965.847 dólares estadounidenses, si bien el propio Internet Crime Report advierte de que esta cantidad no incluye aspectos como las pérdidas de archivos sufridas. Existe una particularidad en relación con el *ransomware* y es que, en ocasiones, las víctimas no especifican a los investigadores las pérdidas que han sufrido, disminuyendo de forma artificial la cantidad de pérdidas total resultante. Además, esta cifra es solo el resultado de las operaciones aritméticas realizadas con la información obtenida por el IC3, y no tiene en cuenta la recogida por agentes de campo del FBI. Continuando con los daños informáticos, los ataques DoS se situaron justo por debajo del *ransomware*, con un total de 7.598.198 dólares estadounidenses de pérdidas en 2019.

El *malware* fue la modalidad del delito de daños informáticos menos lesiva económicamente, con unas pérdidas por valor de 2.009.119 dólares estadounidenses. Cierran la clasificación los ciberdelitos que lesionaron de

manera específica los servicios sanitarios de EE. UU., cuyas pérdidas ascendieron a 1.128.838 dólares estadounidenses[217].

2.4.2.2 La importancia de la protección de los datos sanitarios en la jurisprudencia estadounidense

Además de las leyes federales y de los análisis llevados a cabo por agencias gubernamentales como el FBI, la jurisprudencia también arroja luz sobre la importancia de la adecuada protección de los datos sanitarios de distinta clase en EE. UU., poniendo de manifiesto que no solo deben protegerse mientras están almacenados incluso en lo que respecta a la formación en ciberseguridad de los empleados, sino que deben establecerse protocolos adecuados para su eliminación si se pretende respetar plenamente la legalidad.

2.4.2.2.1 Sorrell v. IMS Health Inc.

En el Caso *Sorrell v. IMS Health Inc., 564 U.S. 552 (2011),* el Tribunal Supremo de Justicia de los Estados Unidos se enfrentó a un caso en el que se contraponían la libertad de expresión y la intimidad, puesto que una ley del estado de Vermont que prohibía la venta, la revelación o el uso de la información de los registros de los medicamentos recetados por los facultativos para proteger su intimidad había sido considerada contraria a la Primera Enmienda a la Constitución de los EE. UU., que prohíbe la creación de cualquier ley que reduzca la libertad de expresión. Rechazando las alegaciones del estado de Vermont, el Tribunal Supremo determinó que la ley imponía restricciones de distintos tipos a la libertad de expresión que no estaban justificadas, y que no eran necesarias para garantizar la intimidad en el ámbito médico ni para mejorar el sistema sanitario público[218].

[217] Federal Bureau of Investigation, *Internet Crime Report 2019,* pp. 19 – 20.

[218] F.H. Cate y B.E. Cate, "The Supreme Court and information privacy"*, International Data Privacy Law,* vol. 2, no. 4, 2012, pp. 260 – 261. Entre los años 1970 y 2011, el

Personalmente, me adhiero al voto particular que sostuvo que los objetivos de la ley del estado de Vermont eran legítimas y apenas lesionaban a la Primera Enmienda, toda vez que el objetivo de que esta información estuviese disponible era hacer más eficientes las campañas de comercialización de productos farmacéuticos, algo que no solo afecta a la intimidad de los facultativos a causa de las previsibles campañas agresivas de las compañías farmacéuticas, sino a los tratamientos que reciben los pacientes, influenciados sin duda por las mismas. Considero que leyes como la Prescription Confidentiality Law 2007 del estado de Vermont son muy positivas no solo para defender la intimidad, sino también para mejorar el sistema sanitario público, puesto que permiten avanzar hacia un modelo de protección de la intimidad basado en el consentimiento explícito de las personas y en el bienestar del paciente[219].

2.4.2.2.2 CareFirst, Inc. v. Chantal Attias

En el Caso *CareFirst, Inc. v. Chantal Attias, no. 16-7108 (2017)*, la Corte de Apelaciones de los Estados Unidos para el Circuito del Distrito de Columbia consideró que no es necesario que con posterioridad a la sustracción de datos como resultado de un ciberataque estos se utilicen para cometer un delito fin, sino que cuando se trata de datos sensibles existe un riesgo de sufrir un daño sustancial por sí mismo, siendo el temor a ser víctima de un delito fin mediante la utilización de dichos datos sensibles suficientemente grave. Y es que la existencia de un riesgo de sufrir un perjuicio futuro es aceptable en casos en los que, como en este, resulta plausible determinar que los ciberdelincuentes tenían la intención y la

Tribunal Supremo de Justicia de los Estados Unidos llevó a cabo valoraciones significativas en relación con la intimidad en un total de 328 ocasiones.

[219] M.J. Taylor y J. Wilson, "Reasonable Expectations of Privacy and Disclosure of Health Data", *Medical Law Review,* vol. 27, no. 3, 2019, p. 460. Uno de los principales problemas en relación con la protección de datos sanitarios es el consentimiento implícito, en el que no se especifica con claridad la forma en que el paciente ha otorgado su consentimiento, dándolo en muchos casos por sentado. Es necesario avanzar hacia un modelo centrado en el paciente que permita compartir estos datos de manera más garantista.

capacidad de utilizar la información robada para delinquir. En febrero de 2018, el Tribunal Supremo de Justicia de los Estados Unidos se negó a la revisión de esta decisión, si bien hay que señalar que existe, en este sentido, una división entre las Cortes de Apelaciones de los Estados Unidos, puesto que algunas de ellas son favorables a esta línea jurisprudencial (Sexta, Séptima, Novena, y la correspondiente al Circuito del Distrito de Columbia), mientras que otras son contrarias a la misma (Primera, Tercera y Cuarta).

2.4.2.2.3 LabMD, Inc. v. Federal Trade Commission

En el último de los tres casos seleccionados, el Caso *LabMD, Inc. v. Federal Trade Commission, no. 16-16270 (2018),* la Corte de Apelaciones de los Estados Unidos para el Undécimo Circuito determinó que la Comisión Federal de Comercio estadounidense se había extralimitado en sus funciones al pretender una reforma del sistema de protección de datos del laboratorio médico LabMD, especializado en pruebas diagnósticas para la detección del cáncer. Este laboratorio guardaba información personal de sus pacientes, incluyendo datos sanitarios, y uno de sus empleados hizo un uso indebido de su red informática que fue advertida por una empresa llamada Tiversa, que aseguró que sus *hackers* podían acceder a la información correspondiente a más de nueve mil de sus pacientes. Se consideró, en consecuencia, que LabMD no había establecido las medidas de seguridad necesarias para proteger su red informática, y aunque esto era cierto, la Corte de Apelaciones de los Estados Unidos para el Undécimo Circuito revocó el deber para LabMD de implementar un programa de ciberseguridad adecuado por ser las exigencias demasiado difusas. A pesar de ello, no cabe duda de que LabMD no protegió de manera adecuada los datos personales de sus pacientes y se enfrentó a un largo proceso judicial, siendo posible sacar dos conclusiones: primera, lo importantes que son los datos sanitarios para la jurisprudencia estadounidense, capaz de condicionar la actividad de una empresa privada a su adecuada protección; segunda, el deber de establecer criterios específicos para valorar cuándo existe dicha protección, o que permitan alcanzarla,

puesto que, como demuestran casos como el de LabMD, empresa hundida tras este proceso judicial, constituye un craso error entorpecer la actividad de las empresas privadas que pretenden cumplir las normas.

Incluso teniendo esto en cuenta, la actividad de la Comisión Federal del Comercio estadounidense no ha sido siempre tan negativa, siendo muy beneficiosa su intervención en distintos casos que han permitido establecer requisitos más seguros para la tramitación de historias clínicas, como en el Caso *CBR Systems, Inc., no. C-4400 (2013)*; para deshacerse de información farmacéutica, como en el Caso *CVS Caremark Corporation, no. C-2459 (2009);* y para la formación de los empleados tanto en la gestión de datos sanitarios como en ciberseguridad, como en el Caso *Eli Lilly and Company, no. 012 3214 (2002)*[220].

2.4.2.3 Particularidades de la legislación de Washington D.C.

Washington D.C. merece una mención destacada por ser la capital de EE. UU. pero, al tener la consideración de distrito federal, y no de estado, carece de una ley estatal que regule de manera específica los delitos que afectan a la ciberseguridad. Aunque es una lástima que esto impida analizar sus particularidades, es lógico y responde al espíritu práctico que caracteriza al *Common Law* adoptado por influencia de Inglaterra[221] considerar que la legislación federal regula suficientemente esta materia, desarrollando leyes estatales solo cuando resulta realmente necesario[222]. Tampoco existe ninguna referencia a los delitos que afectan a la ciberseguridad en el Título 22 del Código del Distrito de Columbia, dedicado a los delitos y las penas. La

[220] Kosseff, *Cybersecurity Law,* pp. 18 – 20.

[221] C.A. Tschider, *International Cybersecurity and Privacy Law in Practice,* 1ª ed., Alphen aan den Rijn, Kluwer Law International B.V., 2018, p. 87. Ya he mencionado en este mismo capítulo el hecho de que la posibilidad de crear leyes penales especiales dota a los sistemas legislativos anglosajones de una gran versatilidad, pero también permite evitar las duplicidades y las redundancias en un ordenamiento jurídico.

[222] A. Lazari, "De ciberataques y ciberleviatanes: cartografía de la governance en el prisma del derecho europeo y comparado", en G. Fernández Arribas (edit.), *Ciberataques y ciberseguridad en la escena internacional,* 1ª ed., Cizur Menor, Navarra, Aranzadi, 2019, pp. 181 – 182.

principal referencia en este sentido se encuentra en el Título 28 del mismo texto legal, cuyo Capítulo 38 está dedicado a la protección de los consumidores. Aunque se trata de una norma claramente ajena al Derecho penal, su Subcapítulo II impone unos requisitos de seguridad a las personas que manejan datos sobre personas residentes en Washington D.C. (§ [28-3852.01]), así como el deber de informar a los afectados en caso de que se vulneren las medidas de seguridad (§ 28-3852). La § 28-3851 incluye la información genética, el perfil de ADN y la información médica dentro de la categoría de información personal, refiriéndose en el caso de la última a cualquier información sobre un tratamiento o un diagnóstico llevado a cabo por un profesional en los ámbitos dental, médico o de la salud mental. El aspecto positivo de la existencia de estas previsiones legales es que permiten al afectado conocer cualquier incidente relacionado con sus datos, lo que le faculta para activar los mecanismos de la justicia amparándose en la ley federal ya analizada[223].

2.4.3 Canadá

No hay particularidades reseñables en la manera en que el CP de Canadá recoge delitos que afectan a la ciberseguridad como el acceso ilícito o los daños informáticos. Dentro de su Parte IX, relativa a los delitos contra la propiedad, la Sección 342.1 (1) tipifica, bajo el genérico título de uso no autorizado de un ordenador, cuatro conductas: primera, obtener, directa o indirectamente, cualquier servicio informático de manera fraudulenta y sin contar con respaldo legal (dos requisitos que se extienden a las otras tres conductas); segunda, interceptar, directa o indirectamente, cualquier función de un sistema informático mediante aparatos electromagnéticos, acústicos, mecánicos o de otra clase; tercera, utilizar, directa o indirectamente, un sistema informático para incurrir en las dos primeras conductas mencionadas, o para cometer el delito de daños informáticos previsto en la Sección 430 (1.1); y cuarta, la utilización, posesión, tráfico o puesta a disposición de un

[223] Kosseff, *Cybersecurity Law,* pp. 375 – 376.

tercero de una contraseña informática que permita llevar a cabo cualquiera de las tres conductas anteriores.

Dentro de esta Parte IX, la Sección 342.2 (1) tipifica los actos preparatorios para cometer los delitos de las Secciones 342.1 (1) y 430 (1.1), y más específicamente la creación, posesión, venta, puesta a la venta, importación, obtención para su uso, distribución o puesta a disposición de un tercero de un dispositivo diseñado o adaptado principalmente para cometerlos, siempre que sea en ausencia de justificación legal y que el sujeto activo tenga conocimiento de que dicho dispositivo ha sido utilizado o va a ser utilizado para ello.

La Parte XI, sobre actos deliberados y prohibidos en relación con ciertas propiedades, recoge los daños informáticos en su Sección 430 (1.1), cuyo título hace referencia de manera concreta los daños contra los datos informáticos. Las conductas previstas son cuatro, y todas requieren que el sujeto activo actúe deliberadamente: primera, destruir o alterar datos informáticos; segunda, inutilizar datos informáticos; tercera, obstruir, interrumpir o interferir en el legítimo uso de datos informáticos; y cuarta, obstruir, interrumpir o interferir en la actividad de una persona que está haciendo un uso legítimo de datos informáticos, o denegarle el acceso a los mismos a una persona autorizada para ello. Al ser el objeto material del delito los datos informáticos, los daños sufridos en un sistema informático deberían encuadrarse en los tipos de la Sección 430 (1) (a) y sucesivos, que castigan no solo las conductas consistentes en destruir o dañar la propiedad, sino todas las incluidas en la Sección 430 (1.1), solo que en sentido genérico, incluyendo, por tanto, los daños en los sistemas informáticos siempre que no recaigan específicamente sobre datos.

No cabe duda de que Canadá ha empezado a adaptarse a los retos que plantea una sociedad cada vez más digitalizada, pero su estrategia parece centrarse más en mitigar el impacto de la ciberdelincuencia que en detenerla. Para ello, se ha fijado en las políticas de países como Australia o

Nueva Zelanda[224]. Aunque esto puede resultar positivo, considero que no tiene por qué conllevar dejar en un segundo plano la tipificación de delitos que afectan a la ciberseguridad en el CP canadiense, siendo la estrategia más recomendable el equilibrio entre el desarrollo de políticas orientadas a mitigar su impacto y la creación de tipos delictivos que permitan perseguirlos cuando la prevención no sea suficiente, especialmente en los casos más graves que requieran la introducción de tipos agravados y en relación con los cuales la mitigación de sus efectos no baste para garantizar los intereses de las víctimas.

2.4.4 Australia

Las estadísticas demuestran que en Australia, a nivel federal, ha habido un incremento constante durante la última década en la persecución de las conductas recogidas en la Parte 10.7 de su CP, dedicada a los delitos informáticos[225] [226]. Esta Parte se encuentra dentro del Capítulo 10 (relativo a la infraestructura nacional), Volumen 2 de dicho texto legal.

Aunque Australia tiene ciertas particularidades en relación con los datos sanitarios con las que estoy en desacuerdo por lo poco garantistas que son con los pacientes, como la imposibilidad de reclamar sus propias historias clínicas por considerar que estos no poseen un derecho de propiedad sobre

[224] J. Popham et al., "Exploring police-reported cybercrime in Canada: variation and correlates", *Policing: An International Journal,* vol. 43, no. 1, 2020, p. 45. En Australia, el Cyber Issue Reporting System del ACSC sustituyó al Australian Cybercrime Online Reporting Network (o ACORN) en 2019. Nueva Zelanda permite informar sobre ciberdelitos a través de un sencillo e intuitivo formulario en la página web del CERT NZ. A mi juicio, estas herramientas al servicio del pueblo no resultan útiles para el mismo si no están respaldadas por una adecuada legislación en el ámbito penal que permita la persecución de los ciberdelitos denunciados.

[225] G. Urbas, *Cybercrime Legislation, Cases and Commentary,* 1ª ed., Chatswood, NSW, LexisNexis Butterworths, 2015, pp. 298 – 299. No obstante, la jurisprudencia a nivel federal en Australia en relación con los delitos informáticos de la Parte 10.7 de su CP se encuentra todavía en una etapa embrionaria.

[226] R. Broadhurst, "Cybercrime in Australia", en A. Deckert y R. Sarre (eds.), *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice*, Londres, Palgrave Macmillan, 2017, p. 222.

ellas ni sobre ninguno de los datos contenidos en las mismas[227] [228], la estructura en tres divisiones de estos delitos dentro de la Parte 10.7 es muy adecuada, sobre todo por su claridad. Hay que tener en cuenta, en el caso australiano, que sus estados y territorios elaboran y administran la mayor parte de la legislación penal, pese a lo cual existe una parte de la misma que el Gobierno federal se encarga de elaborar y de administrar, y cuya pieza clave es el CP de Australia. Su Parte 10.7 contiene tres divisiones: la 476, que hace las veces de título preliminar e incluye definiciones y aspectos técnicos que facilitan la interpretación de los otros dos; la 477, que recoge los delitos informáticos graves; y la 478, que incluye los que no es posible incardinar en la División 477.

Dentro de la División 477, la Sección 477.1 (1) tipifica el acceso, modificación o alteración no autorizados cuando la intención sea cometer un delito grave, es decir, un delito castigado con una pena de prisión de 5 años o superior, o de cadena perpetua. Las primeras dos conductas, correspondientes a las Secciones 477.1 (1) (a) (i) y 477.1 (1) (a) (ii), afectan a los datos contenidos en un ordenador, mientras que la tercera, contenida en la Sección 477.1 (1) (a) (iii), a las comunicaciones electrónicas emitidas desde o recibidas en un ordenador. En cualquiera de las tres, el sujeto activo debe ser consciente de que no está autorizado para llevar a cabo la acción, siendo este un requisito típico indispensable. El delito fin que el sujeto activo

[227] J. Brebner, "*Breen v. Williams:* A lost opportunity or a welcome conservatism?", *Deakin Law Review,* vol. 3, no. 2, 1996, pp. 248 – 249. En el Caso *Breen v. Williams*, la Corte Suprema de Australia decidió que un facultativo no estaba obligado a proporcionar acceso a su historia clínica a una paciente, no considerándola propietaria de la misma, puesto que el contrato entre ambos regulaba el tratamiento que el primero debía proporcionar y que la segunda debía recibir, pero no detalles específicos como la propiedad de los datos que se derivarían del mismo, propiedad que, en opinión de la Corte Suprema, no correspondía a la paciente.

[228] D.J. Carter y S. Hartridge, "Mandatory data breach notification requirements for medical practice", *The Medical Journal of Australia,* vol. 209, no. 5, 2018, pp. 204 – 205. Afortunadamente, y aunque no despoja de validez al Caso *Breen v. Williams*, la Privacy Amendment (Notifiable Data Breaches) Act 2017 obliga a los facultativos australianos a proteger activamente los datos de sus pacientes e, incluso, a garantizar las medidas de protección que sean necesarias en el ámbito de la ciberseguridad. Además, igual que sucede en el caso de Washington D.C., la obligación de informar a los pacientes sobre cualquier incidente relacionado con sus datos permitirá que estos busquen el amparo del Derecho penal cuando sea oportuno.

pretenda cometer tiene, en este caso, una gran importancia, puesto que la Sección 477.1 (6), que recoge las consecuencias jurídicas de este delito, determina que la pena por cometerlo no podrá ser superior a la pena que corresponda al delito fin.

La Sección 477.2 (1) castiga con 10 años de prisión la modificación no autorizada de datos informáticos con el objetivo de llevar a cabo ciertas alteraciones. De nuevo, el sujeto activo debe ser consciente de que la modificación no está autorizada, y debe actuar sin importarle que la modificación altere la posibilidad de acceder a los datos contenidos en cualquier ordenador, o la fiabilidad, la seguridad o el funcionamiento de dicha información.

Por último, la Sección 477.3 (1) prevé una pena de 10 años de prisión para la conducta consistente en alterar sin autorización una comunicación electrónica emitida desde o recibida en un ordenador con conocimiento de que dicha alteración no ha sido autorizada.

La División 478 está dedicada a otros delitos informáticos: el acceso o la modificación no autorizada de datos de acceso restringido (Sección 478.1 (1), castigado con 2 años de prisión, siempre que los datos estén protegidos dentro del sistema informático); la alteración no autorizada de datos contenidos en determinados sistemas informáticos (Sección 478.2, castigado con 2 años de prisión); la posesión o el control sobre datos cuando la intención del sujeto activo sea la de cometer o facilitar la comisión de uno de los delitos informáticos de la División 477 (Sección 478.3 (1), castigado con 3 años de prisión); y la producción, suministro u obtención de datos cuando la intención del sujeto activo sea la antes mencionada (Sección 478.4 (1), castigado también con una pena de 3 años de prisión).

El análisis comparativo en base a indicadores objetivos que evalúa la manera en que el Reino Unido, EE. UU. y Australia han hecho frente al desafío de la ciberseguridad evidencia que si bien Australia no alcanza el

nivel de EE. UU., sí le saca una ligera ventaja al Reino Unido, especialmente en lo concerniente a la creación de políticas de seguridad[229].

2.4.5 Nueva Zelanda

Al contrario de lo que sucede en Australia, el Crimes Act 1961 de Nueva Zelanda no divide los delitos informáticos dependiendo de su gravedad, sino que les dedica un apartado general dentro de su Parte 10, relativa a los delitos contra la propiedad. No obstante, al igual que en el Criminal Code Act 1995 australiano, los delitos que recoge pertenecen, además de a la categoría de los ciberdelitos, específicamente a la de los delitos que afectan a la ciberseguridad[230]. La Sección 249 (1) tipifica el acceso a un sistema informático con fines delictivos, previendo una pena de hasta 7 años de prisión para la persona que, tras acceder directa o indirectamente a un sistema informático de manera fraudulenta y sin contar con respaldo legal, consigue un beneficio o perjudica a un tercero. La Sección 249 (2) castiga con una pena de hasta 5 años de prisión dicho acceso cuando no se consigue un beneficio ni se perjudica a un tercero, pero se lleva a cabo con el propósito de lograr lo uno o lo otro.

La Sección 250 (1) castiga con una pena de hasta 10 años de prisión a quien voluntaria o imprudentemente y de manera intencionada destruye, daña, o altera cualquier sistema informático con conocimiento de que su

[229] A. Dedeke y K. Masterson, "Contrasting cybersecurity implementation frameworks (CIF) from three countries", *Information and Computer Security,* vol. 27, no. 3, 2019, p. 387. EE. UU. encabeza la clasificación con 99 puntos, seguido de Australia con 66 y del Reino Unido en tercer lugar, con 63 puntos. Australia destaca en aspectos como la elaboración de planes para la gestión de riesgos en el ámbito de la seguridad, pero tiene carencias en otros, como demuestran la poca consistencia entre dichos planes y su ejecución o sus dificultades para analizar las amenazas y recopilar información suficiente sobre las mismas.

[230] J. Burton, "Small states and cyber security: The case of New Zealand", *Political Science,* vol. 65, no. 2, 2013, p. 216. A pesar de su relativa cercanía respecto a Australia, Nueva Zelanda ha disfrutado durante años de una posición y de un aislamiento geográficos que han beneficiado a su población en lo que se refiere a la delincuencia. Hoy en día, ni su posición ni su aislamiento impiden la comisión de delitos que afectan a la ciberseguridad, lo que ha obligado a su Gobierno a equilibrar la seguridad y la intimidad.

acción puede resultar peligrosa para la vida de un tercero. Algo menos severa es la pena de la Sección 250 (2), que consiste en hasta 7 años de prisión para quien comete una de las tres conductas siguientes voluntaria o imprudentemente y sin autorización: primera, dañar, borrar, modificar, alterar o cambiar de otro modo cualquier dato o *software* contenido en un sistema informático; segunda, provocar que suceda cualquiera de los delitos anteriores; y tercera, hacer que cualquier ordenador pase a estar inoperativo o que deniegue el servicio a uno de los usuarios autorizados.

Las Secciones 251 (1) y 251 (2) penalizan los actos preparatorios para la comisión de los delitos de las secciones anteriores, castigando con una pena de hasta 2 años de prisión la creación, venta, distribución o posesión de *software* adecuado para este objetivo.

Hay que destacar, por último, la Sección 252 (1), que tipifica el delito de *cracking*[231]. Nueva Zelanda castiga con una pena de hasta 2 años de prisión a quien accede directa o indirectamente, de manera intencionada y en ausencia de autorización a cualquier sistema informático, sin importar si el sujeto activo actúa de manera consciente o imprudente en lo que respecta a la ausencia de autorización. La Sección 252 (2) incluye un matiz que, aunque innecesario en nuestro ordenamiento jurídico por evidente, hace pensar que se han podido intentar encuadrar conductas en este tipo delictivo de forma inadecuada. Así, se excluye del mismo el acceso a un sistema informático por parte de una persona autorizada que, sin embargo, accede para un propósito distinto a aquel para el que dispone de autorización.

Además del contenido del Crimes Act 1961, Nueva Zelanda cuenta con una elaborada estrategia de ciberseguridad basada en la mejora de cinco áreas prioritarias entre los años 2019 y 2023. La quinta está directamente relacionada con el Derecho penal, puesto que consiste en combatir la ciberdelincuencia de manera proactiva. Con este objetivo, se barajan

[231] S.V.A. Richardson y N. Gilmour, “Cyber Crime and National Security: A New Zealand Perspective”, *The European Review of Organised Crime,* vol. 2, no. 2, 2015, p. 52. A pesar de que conductas como esta se han generalizado a nivel mundial, la primera norma de Nueva Zelanda sobre ciberdelitos data de 2003.

iniciativas como la ratificación del Convenio sobre la Ciberdelincuencia de Budapest mientras se protege la seguridad de los neozelandeses sin comprometer su intimidad[232].

2.4.6 Suiza

En el caso de Suiza, los incidentes relacionados con ciber espionaje y ciberdelitos sufridos sobre todo desde 2007 fueron los que empujaron a su Gobierno no solo a ratificar el Convenio sobre la Ciberdelincuencia de Budapest en 2012, sino a tipificar con detalle en su CP ciertos delitos que afectan a la ciberseguridad: el artículo 143 regula la obtención no autorizada de datos; el 143 bis el acceso sin autorización a un sistema de procesamiento de datos; el 144 bis los daños informáticos; y, por último, el artículo 147 la estafa informática.

Aunque el CP suizo incluye estos artículos que permiten hacer frente a los delitos que afectan a la ciberseguridad, en la práctica se han perseguido muy pocos casos en los que haya sido posible aplicarlos. Esto se debe a la complejidad de la estructura del sistema legal helvético, que hace que no resulte sencillo aplicar con rigor las leyes federales y las cantonales, y en el que existe un intrincado Derecho procesal penal que dificulta el proceso.

En cualquier caso, además de su CP, Suiza cuenta desde 2003 con la CYCO, una oficina central para denunciar delitos relacionados con Internet fruto de la colaboración entre la Confederación y la mayoría de cantones que cuenta con tres áreas de responsabilidad: primera, la monitorización, o la búsqueda sistemática de contenido delictivo; segunda, el análisis de casos; y tercera, su resolución. Todo ciudadano suizo puede denunciar actividades

[232] Department of the Prime Minister and Cabinet, *New Zealand's cyber security strategy 2019,* Wellington, Department of the Prime Minister and Cabinet, 2019, pp. 10 – 15. Para combatir proactivamente la ciberdelincuencia, el Gobierno de Nueva Zelanda prevé actuaciones como el apoyo a las personas afectadas por la misma, la mejora en el sistema que hace posible denunciarla, elaborar normas adaptadas a la realidad que aumente la eficacia en su persecución y aumentar la inversión para apoyar los esfuerzos internacionales orientados a luchar contra ella en origen, antes de que afecte a ciudadanos neozelandeses.

sospechosas de constituir un delito mediante un formulario destinado al efecto. Con el tiempo, la CYCO ha ido haciéndose cargo de cada vez más operaciones y deberes policiales, como la coordinación de investigaciones nacionales e internacionales o el intercambio de datos policiales, alejándose del trabajo puramente analítico de sus inicios[233].

2.4.7 Federación de Rusia

La Federación de Rusia no es un Estado parte del Convenio sobre la Ciberdelincuencia de Budapest, ya que después de analizarlo sus autoridades consideraron que su art. 32 b) permitía unas injerencias incompatibles con su soberanía nacional[234], y por lo tanto era contrario a ciertos principios fundamentales del Derecho internacional[235]. Existe en este país una pugna entre la voluntad de adherirse al Derecho penal internacional[236] [237] y la de conservar ciertas particularidades claramente incompatibles con el mismo[238]. Con independencia de su resultado, tanto la

[233] M.D. Cavelty, *Cybersecurity in Switzerland,* 1ª ed., Cham, Springer, 2014, pp. 16 – 17. El CP helvético entró en vigor en el año 1942. Hasta entonces, el Derecho penal había sido una competencia cantonal.

[234] G. Esakov, "International Criminal Law in Russia: Missed Crimes Waiting for a Revival", *Journal of International Criminal Justice,* vol. 15, no. 2, 2017, p. 392. La Federación Rusa tiene un problema principalmente terminológico, ya que muchas de las expresiones legales que se utilizan en el Derecho penal internacional no se contemplan en su Derecho penal interno, si bien esto está cambiando poco a poco.

[235] Baumard, *Cybersecurity in France*, pp. 34 – 35.

[236] R.V. Veresha, "Preventive measures against computer related crimes: Approaching an individual", *Informatologia,* vol. 51, no. 3-4, 2018, p. 197. Para la adopción de decisiones en relación con la ciberdelincuencia, la Federación Rusa utiliza, inevitablemente, datos de países como EE. UU. o Noruega.

[237] A.I. Korobeev, R.I. Dremlyuga, y Y.O. Kuchina, "Cybercrimes in the Russian Federation: Criminological and Criminal Law Analysis of the Situation", *Russian Journal of Criminology,* vol. 13, no. 3, 2019, p. 416.

[238] F. Daucé et al., "From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia", *Laboratorium: Russian Review of Social Research,* vol. 11, no. 3, 2019, p. 67. La existencia de vigilantes que juzgan ciertos contenidos de Internet en base a un criterio ideológico, y no tras una evaluación objetiva de su adecuación a los límites del Derecho penal, es claramente incompatible con la relativa libertad que la Red ofrece, al menos de momento, a los ciudadanos de, por ejemplo, la UE. No obstante, esta lamentable tendencia ya ha empezado a extenderse también a países como España, donde se está otorgando poder a personas con perfiles ideológicos concretos para descalificar contenidos atendiendo a criterios subjetivos.

Federación Rusa como los países de su entorno[239] siguen teniendo que hacer frente a los delitos que afectan a la ciberseguridad[240], por lo que es posible analizar la manera en que esta los prevé y castiga a través del contenido de su CP.

La Parte Especial del CP de la Federación Rusa, dentro de su Sección IX, dedicada a los delitos contra la seguridad y el orden públicos, contiene un Capítulo 28 que recoge los delitos en la esfera de los sistemas informáticos. Su articulado se caracteriza por cierto caos que induce a la confusión en la tipificación de las conductas, siendo esto muy evidente en el art. 272. Este artículo pretende tipificar el acceso ilegal a la información contenida en redes y sistemas informáticos que está legalmente protegida, pero esta acción solo puede considerarse típica cuando se consigue mediante la destrucción, el bloqueo, la modificación o la copia de dicha información, o bien mediante la interrupción de la actividad de las redes o sistemas informáticos. Esta redacción del tipo hace difícil determinar si lo que se pretende es castigar el mero acceso, o también ciertas conductas en las que el objeto material del delito son los datos informáticos, incluyendo aquellas que conducen a su destrucción. Una lectura conjunta del artículo me lleva a decantarme por lo segundo, pero reitero mi opinión de que supone un error tipificar en un único artículo al menos dos conductas de distinta naturaleza que merecerían una tipificación individualizada y un reproche penal acorde a la gravedad de cada una, máxime cuando también forma parte del tipo la interrupción de la actividad de las redes o sistemas informáticos. Las penas previstas para el delito del art. 172 son una multa de hasta 200 rublos rusos, la imposición de trabajos correctivos durante un periodo de seis a doce meses, o la privación de libertad por un periodo de hasta dos años.

[239] I. Proshchyn y V. Shypovskyi, “Cyber security in the national security & defence sector of Ukraine: today´s challenges and ways to avoid possible threats”, *Social Development & Security,* vol. 10, no. 1, 2020, p. 7.

[240] I.R. Begishev, Z.I. Khisamova, y S.G. Nikitin, “The organization of hacking community: Criminological and criminal law aspects”, *Russian Journal of Criminology,* vol. 14, no. 1, 2020, p. 96. Incluso en la Federación Rusa se plantean aspectos como la diferencia entre la actividad del *hacker* y la del *cracker*.

El art. 273 castiga la creación, el uso y la diseminación de virus informáticos lesivos. Si bien no es tan caótico en su redacción como el art. 272, adolece de un problema distinto: su obsolescencia respecto a la realidad tecnológica actual. Y es que, como expondré en el capítulo tercero de esta investigación, el art. 264.1 del CP español permite castigar los daños informáticos no solo cuando sean el resultado de un virus, sino también del aprovechamiento de las vulnerabilidades existentes a través de ataques DoS o DDoS. Si el legislador ruso pretendía tipificar los daños informáticos, hubiese debido tener en cuenta los últimos avances tecnológicos o, en última instancia, llevar a cabo una redacción menos específica que no acotase este delito al ámbito de los virus informáticos. El art. 273 necesita, en consecuencia, una profunda revisión para adaptarlo a los últimos avances de la tecnología informática. De acuerdo a su redacción actual, se prevé para el mismo una pena de prisión de hasta 3 años, a la que hay que añadir una multa de hasta 200 rublos rusos.

Por último, el art. 274 es, sin duda, el peor de los tres artículos de este Capítulo 28. Dedicado a la violación de las normas de uso de las redes o sistemas informáticos, lleva implícita una remisión a la legislación extrapenal de una amplitud tal que supone un notable riesgo para la seguridad jurídica. Si bien el tipo especifica que este delito solo puede llevarlo a cabo una persona que tenga acceso a redes y sistemas informáticos y que su conducta debe haber tenido como consecuencia la destrucción, el bloqueo o la modificación de datos legalmente protegidos causando un daño sustancial, no se especifica cuáles son esas normas que deben violarse, a qué redes y sistemas informáticos debe tener acceso el sujeto activo (si a las que va a perjudicar, o a cualquiera), cuáles son los datos legalmente protegidos o qué se puede considerar un daño sustancial. Si su comisión hace posible, como en la actual redacción del artículo, la imposición de una pena tan grave como 2 años de prisión, es necesario que el legislador ruso actualice este artículo introduciendo la descripción de una conducta típica que evite la remisión a normas extrapenales, especificando a qué redes y sistemas informáticos

debe tener acceso el sujeto activo, y determinando qué datos están legalmente protegidos y en qué consiste un daño sustancial.

Aunque la Duma Estatal no ha desarrollado una legislación como la de la UE en relación con la ciberseguridad, la política rusa en este ámbito se estructura sobre sus respuestas a casos específicos, más que en normas emanadas del Kremlin. Así, un análisis de los documentos policiales Doctrine of Information Security of the Russian Federation y Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020 evidencia que la política rusa en materia de ciberseguridad se basará en la protección de sus infraestructuras críticas[241], en aumentar la competitividad de Rusia en el mercado de la tecnología de la información, en la cooperación internacional como medio para impedir los ciberataques y, sobre todo, en la existencia de un poder ejecutivo centralizado que regulará en este ámbito de acuerdo a las necesidades del país[242].

2.5 Aspectos del Derecho penal comparado susceptibles de ser tenidos en cuenta en el Derecho penal español

Después de analizar los delitos que afectan a la ciberseguridad en el Derecho penal de, entre otros, Reino Unido, EE. UU., Canadá, Australia, Nueva Zelanda, Suiza y la Federación de Rusia, considero que existen ciertos aspectos que sería positivo y posible trasladar al Derecho penal español, empezando por el hecho de que resulta imposible limitarse a los países mencionados e ignorar los aciertos de países que forman parte de la UE (motivo por el cual resultaba esencial estructurar así este análisis de derecho comparado), suponiendo esta unión entre lo extracomunitario y lo comunitario

[241] I.R. Begishev, Z.I. Khisamova, y G.I. Mazitova, “Criminal legal ensuring of security of critical information infrastructure of the Russian Federation”, *Revista Gênero & Direito,* vol. 8, no. 6, 2019, p. 283. Hay que destacar, en el ámbito de la protección de las infraestructuras críticas, la Ley Federal no. 187-FZ, de 26 de julio de 2017, relativa a la seguridad de las infraestructuras críticas de información de la Federación Rusa.

[242] Rhodes y Litt, *The ABA Cybersecurity Handbook,* pp. 110 – 111.

el elemento que dota de su fuerza a esta propuesta, que no es sino el reflejo de la suma del ingenio legal de naciones destinadas a colaborar.

Primero, la iniciativa danesa de destinar fondos para la investigación en nuevas tecnologías, incluyendo entre las mismas la ciberseguridad. A esto hay que añadir la creación y financiación de una unidad de ciberseguridad asignada a cada uno de los sectores críticos para la sociedad, como el sanitario, permitiendo desarrollar una estrategia específica adaptada a sus vulnerabilidades y combatir más eficazmente las ciberamenazas.

Segundo, la decisión de países como Bélgica de dotar de autonomía a los delitos informáticos mediante un título o capítulo propio y diferenciado, que permitiría tipificar minuciosamente y con el detalle necesario el delito de *cracking*, yendo más allá del tipo básico y delimitando la ciberseguridad como bien jurídico protegido autónomo, lo que solucionaría las carencias existentes en este sentido en la actual redacción del CP español.

Tercero, la manera en que se tipifica el delito de *cracking* en el Reino Unido después de la reforma introducida por la Police and Justice Act 2006. La Sección 1 (1) de la Computer Misuse Act 1990 (CMA) no menciona la vulneración de medidas de seguridad ni extiende la conducta típica al hecho de mantenerse en el conjunto o en una parte de un sistema de información contra la voluntad de quien tenga legítimo derecho a la exclusión del sujeto activo, pero sí incluye aspectos que coinciden con mi propuesta de *lege ferenda* para este delito, como la descripción de la conducta típica, la exigencia de actuar en ausencia de autorización y, sobre todo, el elemento subjetivo del delito, si bien no se menciona de manera específica la ciberseguridad, sino la consciencia respecto a las implicaciones que conlleva la acción. La Sección 1 (3) (c) del mismo texto legal prevé las consecuencias jurídicas de este delito, una pena de prisión máxima de dos años, coincidiendo de nuevo con mi propuesta para el CP español. Atendiendo a la distinguida posición que ocupa el Reino Unido en las clasificaciones sobre ciberseguridad, considero muy positivo que nuestro ordenamiento jurídico guarde similitudes con el suyo en lo relativo al delito de *cracking*.

Cuarto, no incurrir en los mismos errores que países como EE. UU. o la Federación Rusa. En relación con el primero, la sistematización de los delitos que afectan a la ciberseguridad es mucho más adecuada en el actual CP español que en el Título 18 del USC, principal CP del Gobierno federal de los EE. UU., que recopila tanto los delitos federales como elementos de Derecho procesal penal. Aunque soy partidario de agruparlos, no me parece clara la tipificación que se lleva a cabo en la Parte I, Capítulo 47 de dicho texto legal, en cuya § 1030, dedicada a la intromisión dolosa en un sistema informático, se incluyen con apenas unas líneas de separación delitos que afectan a la ciberseguridad tan distintos como el acceso ilícito a un sistema informático y la sustracción de datos como los daños informáticos. Incluso agrupados, es necesario establecer una adecuada distinción entre estos delitos que respete sus particularidades y permita tipificarlos con el nivel de detalle necesario. En cuanto a la Federación Rusa, el legislador español debe evitar incurrir en errores notorios del CP ruso como la tipificación de dos conductas de distinta naturaleza en un único artículo o la remisión injustificada a normas extrapenales, debiendo actualizar el texto legal en base a la realidad tecnológica del momento y ser muy específico para garantizar la seguridad jurídica.

Quinto, trasladar la gran versatilidad[243] [244] del sistema jurídico-penal anglosajón al español, el cual, a su vez, está vinculado a la tradición jurídica europea continental. Aunque sea imposible desde un punto de vista técnico hacerlo a través de leyes penales especiales por las características de la legislación penal española, sí al menos dotar al legislador de una mayor

[243] M. Kaplan, "Sex Offenses and the Problem of Prevention", en L. Alexander y K. Kessler Ferzan (eds.), *The Palgrave Handbook of Applied Ethics and the Criminal Law,* 1ª ed., Londres, Palgrave Macmillan, 2019, p. 721. Esta versatilidad se extiende a propuestas tan controvertidas y necesitadas de un análisis ético-legal como la posibilidad de que la policía acceda periódicamente al ordenador de una persona para evitar su ingreso en prisión, en un intento de imponer siempre la medida de seguridad menos restrictiva posible.

[244] R.D. Bachman y R. K. Schutt, *The Practice of Research in Criminology and Criminal Justice,* 7ª ed., Thousand Oaks, CA, SAGE Publications, 2020, p. 178. Desde un punto de vista ético, una mayor versatilidad de la legislación en este ámbito sería indudablemente beneficiosa para la sociedad española.

libertad para adaptar progresivamente los delitos que afectan a la ciberseguridad a los desafíos que impone la tecnología informática más avanzada[245], pero sin olvidar jamás la enorme importancia del principio de legalidad consagrado en el Derecho penal español.

[245] S. Vasiliev, “The Crises and Critiques of International Criminal Justice”, en K.J. Heller et al. (eds.), *The Oxford Handbook of International Criminal Law,* Oxford, Inglaterra, Oxford University Press, 2020, p. 630.

CAPÍTULO III

LA CIBERSEGURIDAD EN EL DERECHO PENAL ESPAÑOL

3.1 El principio de *ultima ratio* como límite entre el Derecho administrativo y el Derecho penal

Desde el 25 de mayo 2018, dos años después de su entrada en vigor, se aplica de forma plena en España el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, también llamado Reglamento General de Protección de Datos o RGPD. La nueva LOPD-GDD, que entró en vigor el 7 de diciembre de 2018, transpuso al ordenamiento jurídico español sus disposiciones, al tiempo que ampliaba algunos de sus preceptos indeterminados. Ante la existencia de estas dos normas de Derecho administrativo en pleno funcionamiento, cabe plantearse el papel del Derecho penal en relación con la protección de datos[246]. No obstante, un rápido vistazo a las mismas evidencia la necesidad de ir más allá de las meras sanciones administrativas para protegerlos como es debido, máxime teniendo en cuenta su importancia a todos los niveles.

El principio de intervención mínima o *ultima ratio* establece[247] el uso limitado o restringido que, en la práctica, debe hacerse del Derecho penal, de manera que constituya únicamente un recurso extremo ocasionalmente operativo, y solo cuando resulte estrictamente necesario. Se busca con ello, de acuerdo con un postulado utilitarista, garantizar la seguridad con el menor

[246] E. Morón Lerma, *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red,* 2ª ed., Cizur Menor, Navarra, Aranzadi, 2002, p. 171. Como puede observarse por la fecha de publicación de esta obra, el debate entre los límites entre el Derecho administrativo y el Derecho penal en este ámbito es antiguo.

[247] M.A. Boldova Pasamar, "Los principios del derecho penal", en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho penal, Parte General. Introducción y teoría jurídica del delito,* Granada, Comares, 2016, p. 45. También deben tenerse en cuenta los criterios de necesidad y oportunidad.

coste posible para la libertad, lo que implica acudir al CP solo cuando sea la única manera de asegurar la convivencia pacífica, libre y segura de una comunidad mediante la protección de sus bienes jurídicos más importantes. En los casos en los que es posible conseguir el mismo o superior efecto para la protección de los bienes jurídicos con una reacción menos grave, no está justificada que aquella sea más grave. Solo debe acudirse al Derecho penal, teniendo en cuenta su carácter subsidiario, cuando las demás formas de resolución del conflicto derivado de la infracción de una norma jurídica demuestren su insuficiencia o su ineficacia. Únicamente ante el fracaso de otras sanciones con menor poder inhibitorio, como las previstas en el Derecho administrativo, se acudiría a lo establecido en el Derecho penal, a causa de su mayor potencial intimidatorio.

Este principio de *ultima ratio*, que tantas reflexiones ha despertado en la doctrina, tanto a nivel nacional [248] [249] [250] [251] como internacional [252], obliga a

[248] C.M. Romeo Casabona, "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet", *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento,* no. 2, 2002, p. 125. Es necesaria una reflexión en cada caso sobre si recurrir a la tipificación penal está o no justificado teniendo en cuenta los principios de *ultima ratio* y de intervención mínima, sobre todo en lo concerniente a los accesos ilegítimos sin el propósito de producir ningún daño determinado. Si es posible satisfacer las necesidades de tutela jurídica mediante normas extrapenales, no debería abusarse del recurso a los instrumentos punitivos. En cualquier caso, incluso si se decide que la intervención del Derecho penal es necesaria, sería recomendable, so riesgo de fracasar, la adopción de bloques de medidas y regulaciones jurídicas adicionales en otros ámbitos como el Derecho internacional o el Derecho procesal o, en su caso, abordar la compleja tarea de revisar la eficiencia de las que ya existen como medio para conseguir una *optima ratio* a la intervención del Derecho penal.

[249] R. Carnevali Rodríguez, "Derecho penal como *ultima ratio*. Hacia una política criminal racional", *Ius et Praxis,* vol. 14, no. 1, 2008, p. 13. El Derecho penal debe ser el último instrumento al que recurra la sociedad para proteger determinados bienes jurídicos, siempre en ausencia de otras formas de control menos lesivas.

[250] C. Conde-Pumpido Tourón, "El derecho penal como última ratio: principio de intervención mínima", *Estudios de derecho judicial,* no. 48, 2003, p. 45. Se remarca el lógico deber de mínima intervención.

[251] F. Palazzo, "Principio de última ratio e hipertrofia del derecho penal", en L.A. Arroyo Zapatero e I. Berdugo Gómez de la Torre (dirs.), *Homenaje al Dr. Marino Barbero Santos: In Memoriam (Vol. 1)*, Cuenca, Ediciones de la Universidad de Castilla – La Mancha / Ediciones Universidad de Salamanca, 2001, pp. 433 – 438.

[252] M. Kettunen, *Legitimizing European Criminal Law: Justification and Restrictions,* 1ª ed., Cham, Springer, 2020, p. 63. Es importante que el poder legislativo consiga establecer una coherencia interna en el tratamiento que prevé para los distintos tipos de delito. A este deber se le ha llamado, en ocasiones, dimensión interna del principio de

preguntarse si el Derecho penal es necesario para la protección de la intimidad y de los datos de carácter personal. Sin desmerecer su aplicación en la valoración de los límites de la intervención del Derecho penal, la respuesta es, a mi juicio, afirmativa. Me baso, para ello, en tres argumentos.

Primero, tras los más de dos años desde la fecha en que comenzó a ser obligatorio aplicar de forma plena el Reglamento, la ciberdelincuencia, incluyendo la relativa a la sustracción de datos, continúa siendo uno de los principales problemas de la sociedad, hasta el punto de que se espera[253] que en 2021 la economía mundial sufra pérdidas por valor de 6 billones de dólares estadounidenses a causa de la misma. Este argumento podría, tal vez, aplicarse también al Convenio de Budapest, pero, dejando de lado el Derecho administrativo, hechos como que los ataques de *ransomware* sigan creciendo exponencialmente, hasta el punto de que tenga lugar uno cada doce segundos solo en EE. UU., o el ciberataque masivo sufrido por Australia en pleno junio de 2020, que afectó a su sector sanitario, evidencian la necesidad del legislador estatal de continuar trabajando en el ordenamiento jurídico interno para pulir las disposiciones del tratado internacional. Atendiendo solo a las cifras en relación con el *ransomware*, en relación con el cual ninguna sanción prevé el Derecho administrativo, la tendencia al alza de los ciberdelitos conlleva la necesidad de una adecuada respuesta del Derecho penal. Existe, en efecto, una profusa legislación extrapenal en relación con la ciberseguridad, y es precisamente su existencia lo que hace posible determinar que ciertas conductas no solo continúan cometiéndose, sino que, además, aumentan en frecuencia[254]. Es por esto que no creo que acudir al

ultima ratio, de acuerdo al cual las diferentes previsiones penales deben formar un todo coherente que enfatice la proporcionalidad en el tratamiento de distintos tipos de conducta.

[253] S. Wertheim, “Tips for Fighting off Cybercrime in 2020”, *The CPA Journal,* vol. 90, no. 3, 2020, p. 64.

[254] L. Ayala, *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention,* 1ª ed., Nueva York, NY, Apress Media LLC, 2016, pp. 9 - 73. En el ámbito sanitario, no se trata solo de la cantidad, sino de la variedad cada vez mayor de modalidades de ciberataque. Así, el *phishing*, el *pharming*, los ciberataques indirectos, el *scareware*, el *ransomware*, las memorias USB infectadas y los accesos ilícitos suponen un problema para los profesionales que pretenden proporcionar asistencia médica de calidad.

Derecho penal sea negativo, al cumplirse, en verdad, el principio de *ultima ratio,* siempre teniendo en cuenta que el mismo supone acudir al Derecho penal como último recurso, no dejar de utilizarlo incluso cuando la realidad pone de manifiesto que su intervención, respetando sus demás principios, es necesaria.

En segundo lugar, están las sanciones (que no penas) previstas por el Derecho administrativo, que son siempre de tipo pecuniario. El art. 83 del Reglamento (UE) 2016/679, al que nos remite la LOPD-GDD en materia sancionadora, prevé cuantiosas multas administrativas de un máximo de varios millones de euros, o del equivalente a un porcentaje de su volumen de negocio total global del ejercicio financiero anterior cuando se trate de una empresa, debiendo optarse por la que suponga una mayor cuantía. Estas sanciones cumplen sin duda su objetivo desde un punto de vista administrativo[255] y animan a cumplir lo dispuesto en el Reglamento y la LOPD-GDD[256]. No obstante, es muy importante valorar dos elementos: por un lado, que una pena basada en el abono de una cantidad de dinero, por elevada que sea, puede no resultar un problema para una gran multinacional; por otro, el valor de los datos, que se compara hoy en día con el del petróleo por ser enormemente codiciados en el mercado. Teniendo en cuenta lo anterior, no es difícil prever un escenario en el que las empresas de mayor nivel económico sopesen el cumplimiento o no de las normas atendiendo a los beneficios que podrían obtener al incumplirlas. La protección necesaria en este ámbito trasciende, por lo tanto, la esfera del Derecho administrativo.

[255] J. Shires, "Cybersecurity Governance in the GCC", en R. Ellis y V. Mohan (eds.), *Rewired: Cybersecurity Governance,* Hoboken, NJ, Wiley, 2019, p. 28. Para algunos autores, la regulación de la ciberseguridad corresponde exclusivamente al ámbito administrativo. No obstante, en la práctica esto no es suficiente.

[256] J. Bell et al., "Balancing Data Subjects' Rights and Public Interest Research: Examining the Interplay between UK Law, EU Human Rights Law and the GDPR", *European Data Protection Law Review,* vol. 5, no. 1, 2019, p. 43. Desde el punto de vista del Derecho administrativo, el Reglamento (UE) 2016/679 es una herramienta extrapenal idónea para la protección de los datos personales, pero necesita la intervención del Derecho penal para una defensa total de los mismos mediante la persecución de ciertas conductas.

En tercer lugar, el más importante de los problemas: en el Derecho administrativo, las sanciones están previstas para quienes, debiendo proteger los datos, incumplen o cumplen de manera insuficiente este deber. En el Derecho penal, en cambio, se persiguen, entre otras, las conductas orientadas a la obtención de los datos custodiados por un tercero. Aunque en ambos casos la cuestión gira en torno a la protección de los datos, el espíritu que subyace en las prohibiciones de cada una de estas ramas del derecho es muy distinto.

Basándome en los tres argumentos anteriores[257], considero que, en este caso, no hay que temer utilizar de manera abusiva el Derecho penal, so riesgo de cargar sobre el Derecho administrativo un peso excesivo y de incurrir en lo que ya se ha denominado administrativización (horrendo neologismo no admitido aún de manera formal en español) de determinadas ramificaciones del Derecho penal. No cabe duda de que, siempre que no se solapen[258], y siempre que esto no resulte incompatible con el respeto al principio *non bis in idem*[259]*,* ambos pueden no solo coexistir, sino incluso complementarse[260] a causa de la dualidad de objetivos antes señalada,. Hay que tener en cuenta, por último, que el desarrollo en el ordenamiento jurídico estatal de las bases dispuestas por el Convenio de Budapest supone no solo una adaptación acorde a su influencia mundial[261], sino el cumplimiento de una

[257] J.M. Gau, *Statistics for Criminology and Criminal Justice,* 3ª ed., Thousand Oaks, CA, SAGE Publications, 2019, p. 256. Solo se pretende la intervención del Derecho penal para regular lo que en el ámbito administrativo resulta ineficaz, insuficiente, o directamente no está regulado por ser otros sus objetivos.

[258] E. Davara Fernández de Marcos y L. Davara Fernández de Marcos, *Delitos informáticos,* 1ª ed., Cizur Menor, Navarra, Aranzadi, 2017, pp. 45 – 46. Es importante tener en cuenta que existen leyes relacionadas con la ciberseguridad en el ámbito administrativo que ya prevén sanciones por determinadas conductas.

[259] M. Salat Paisal, *La relación entre Derecho penal y Derecho administrativo sancionador. Una propuesta basada en la idea de la prisión como ultima ratio*, 1ª ed., Valencia, Tirant lo Blanch, 2021, pp. 15 – 16.

[260] N. Pastor Muñoz, *Riesgo permitido y principio de legalidad: la remisión a los estándares sociales de conducta en la construcción de la norma jurídico-penal*, 1ª ed., Barcelona, Atelier, 2019, pp. 77 – 82.

[261] F. Siracusano, "The European Investigation Order for Evidence Gathering Abroad", en T. Rafaraci y R. Belfiore (eds.), *EU Criminal Justice: Fundamental Rights, Transnational Proceedings and the European Public Prosecutor´s Office,* Cham, Springer, 2019, p. 91. Pp. 85 – 101. El Convenio de Budapest introdujo importantes

inexcusable obligación internacional. Y es que hay bienes jurídicos protegidos por la CE que no son sino la encarnación de derechos fundamentales, siendo necesaria, ante amenazas graves, la intervención del Derecho penal. De manera que, siempre que se haga atendiendo al debido detalle[262] y tras un análisis previo que evidencie el respeto por principios como el de *ultima ratio*, la intervención del Derecho penal resulta adecuada en este ámbito.

3.2 La importancia del principio de precaución en el desarrollo de los delitos contra la ciberseguridad

Ya hace años que se discute el papel del Derecho penal en la llamada sociedad del riesgo, que recibe este nombre por la profunda influencia que el desarrollo científico y tecnológico, así como los riesgos que se derivan del mismo, tienen sobre ella. No obstante, muchas veces es difícil concretar la naturaleza y magnitud de dichos riesgos, o la posibilidad de que deriven en un resultado que lesione o haga peligrar bienes jurídico-penalmente protegidos. Es por esto que mientras por un lado se denuncian las insuficiencias del Derecho penal tradicional para enfrentarse a ciertas situaciones nuevas, su necesidad de adaptación a las mismas, e incluso de reconocer lo muy poco que puede hacer de manera efectiva en algunos ámbitos, por otro se cuestiona la validez de un sistema legal que pretende regular y perseguir todos los riesgos, incluso los menores, hasta sus más

novedades no solo en Estados miembros del Consejo de Europa, sino en otros como EE. UU.

[262] L. Tosoni, "Rethinking Privacy in the Council of Europe´s Convention on Cybercrime", *Computer Law & Security Review,* vol. 34, no. 6, 2018, p. 1200. El uso del Derecho penal para la protección de datos solo es posible si las normas se formulan con un nivel de detalle adecuado, muy distinto al que requiere el Derecho administrativo. Para ilustrar esta idea, se pone como ejemplo el art. 32 del Reglamento (UE) 2016/679, cuyas medidas de seguridad administrativas chocarían frontalmente con el principio de legalidad (*nullum crimen, nulla poena sine praevia lege*) de pretenderse su traslado directo al ámbito del Derecho penal.

íntimos detalles, tolerando la licitud de los grandes peligros al no poder reducirlos a un mínimo técnico[263].

Se hace imperativo, por lo tanto, encontrar un medio que contribuya a regular eficazmente el marco del riesgo permitido y del riesgo punible[264], también en el ámbito de la ciberseguridad. El principio de precaución[265] [266] es la herramienta idónea en este sentido, toda vez que toma como punto de partida la concatenación de dos presupuestos: la posibilidad de que una conducta humana cause daños colectivos vinculados a situaciones catastróficas que afecten a un conjunto de seres vivos, y la ausencia de evidencia científica (o incertidumbre) respecto a la existencia del daño que se teme y que se pretende evitar[267].

---

[263] C.M. Romeo Casabona, "Aportaciones del principio de precaución al Derecho Penal", en C.M. Romeo Casabona (edit.), *Principio de precaución, Biotecnología y Derecho*, Granada, Comares, 2004, p. 385.

[264] Romeo Casabona, *Principio de precaución, Biotecnología y Derecho,* p. 386.

[265] S. Escobar Vélez, "El traslado del principio de precaución al Derecho penal en España", *Nuevo Foro Penal,* no. 75, 2010, pp. 18 - 22. Se cita a C.M. Romeo Casabona para arrojar luz sobre el origen de este principio de precaución o principio de cautela, que se remonta a la legislación medioambiental de Alemania en la década de los setenta, bajo la denominación *Vorsorgeprinzip*. A partir de ahí, se expandió de forma paulatina a otros instrumentos jurídicos internacionales en la década de los ochenta hasta que, en junio de 1992, este principio se formuló por primera vez de manera más detallada en el principio decimoquinto de la Declaración de Río sobre el Medio Ambiente y el Desarrollo. De acuerdo con el mismo, en sentido genérico, ante un peligro de daño grave o irreversible, los Estados no deberían postergar la adopción de medidas eficaces, incluso teniendo en cuenta la posible falta de certeza científica absoluta. Con el tiempo, este principio se trasladó al Derecho penal español por vía jurisprudencial, si bien es importante señalar que solamente en el ámbito de los delitos contra la salud pública. Su aplicación a los delitos que afectan a la ciberseguridad resulta, por lo tanto (atendiendo a que esta subcategoría de ciberdelitos también es nueva), arriesgada, y requiere un trato cauto y muy meticuloso que probablemente conduzca a su no utilización.

[266] A. Galán Muñoz, "La problemática utilización del principio de precaución como referente de la política criminal del moderno derecho penal. ¿Hacia un derecho penal del miedo a lo desconocido o hacia uno realmente preventivo?", *Revista de estudios de la justicia,* no. 22, 2015, p. 113. Existe el peligro de que este principio se use de forma desmedida y abusiva, e incluso hay quienes rechazan completamente que se utilice en el ámbito penal por entender que supone la caída de los pilares más relevantes de la dogmática clásica. Solo el respeto hacia ciertos criterios y garantías desarrollados por la misma, como el principio de *ultima ratio*, al que he dedicado la apertura de este tercer capítulo, pueden impedir la creación de un Derecho penal desmedido y poco respetuoso con los derechos de las personas. En consecuencia, es necesario velar por la adecuada utilización del principio de precaución en el ámbito del Derecho penal.

[267] Romeo Casabona, *Principio de precaución, Biotecnología y Derecho,* p. 390.

Hay que partir de la base de que no debe perseguirse ni la seguridad absoluta ni el riesgo cero, sino que hay que determinar si el Derecho penal puede dar acogida o no al principio de precaución y, si es así, bajo qué condiciones y con qué limitaciones[268]. Y es que en el Derecho penal tradicional, la prevención se basó de forma inexcusable en la idea de la previsión o de la previsibilidad, en las certidumbres más o menos precisas de la ciencia. La utilización del principio de precaución supone un cambio de paradigma, un tránsito de un modelo de previsión en el que se conocen el riesgo y los nexos causales, a uno de incertidumbre del riesgo en el que el daño no se puede calcular, ni tampoco el posible nexo causal entre uno y otro[269]. Esto no impide su aplicación en el ámbito del Derecho penal, pero sí la restringen notablemente, al existir principios como el de mínima intervención y el de subsidiariedad, que deben ser siempre respetados. En consecuencia, aunque es posible interpretar y resolver algunos delitos conforme al principio de precaución[270], e incluso conociendo las gravísimas consecuencias y riesgos de ciertas conductas respecto a las que el Derecho penal no ha ofrecido oportuna respuesta[271], no pueden prohibirse ciertas acciones por mucho que no sea posible demostrar su carácter inofensivo, puesto que, de otro modo, podrían paralizarse muchas actividades de gran trascendencia económica[272].

---

[268] C.M. Romeo Casabona et al., "Informe sobre los intentos de adaptación del Derecho Penal al desarrollo social y tecnológico: líneas de investigación y conclusiones", ", en C.M. Romeo Casabona y F. Guanarteme Sánchez Lázaro (eds.), *La adaptación del derecho penal al desarrollo social y tecnológico,* Granada, Comares, 2010, p. 515. La seguridad absoluta y el riesgo cero son solo una utopía en ciertas actividades.

[269] Romeo Casabona et al., *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 516 – 517.

[270] Romeo Casabona et al., *La adaptación del derecho penal al desarrollo social y tecnológico,* p. 517.

[271] E. Sola Reche, "Principio de precaución y tipicidad penal", en C.M. Romeo Casabona (edit.), *Principio de precaución, Biotecnología y Derecho*, Granada, Comares, 2004, p. 490. Por lo general, en casos como el de la intoxicación masiva ocurrida por el síndrome del aceite tóxico de colza, es difícil determinar quién merece ser castigado, incluso cuando hay autoridades con responsabilidades públicas sobre la materia.

[272] C.M. Romeo Casabona, "Conocimiento científico y causalidad en el Derecho Penal", en C.M. Romeo Casabona y F. Guanarteme Sánchez Lázaro (eds.), *La adaptación del derecho penal al desarrollo social y tecnológico,* Granada, Comares, 2010, p. 132.

No existe en el Derecho penal español vigente figura delictiva alguna que constituya una encarnación indiscutible del principio de precaución. A pesar de ello, algunos tipos penales dan cabida al mismo de manera indirecta pero evidente mediante normas extrapenales que completan la descripción de la conducta típica, lo que permite considerarlas como un trasunto en mayor o menor medida del mencionado principio. Es innegable su utilidad político-criminal para configurar nuevos delitos de peligrosidad (peligro abstracto) y, especialmente, de acción peligrosa (peligro abstracto-concreto), así como para tipificar delitos imprudentes de resultado con un alcance más limitado y preciso[273], toda vez que demostrar una relación de causalidad de forma garantista siempre plantea dificultades. No obstante, es necesario plantear la cuestión de si el mismo debe aplicarse en el ámbito específico de los delitos contra la ciberseguridad y, si la respuesta es afirmativa, en qué grado, especialmente teniendo en cuenta el imparable desarrollo de la tecnología y el hecho de que, en el futuro, se podría usar, incluso, en relación con las decisiones automatizadas[274].

Basándome en la idea de que la necesidad de seguridad de las redes informáticas y la prevención delictiva son compatibles con una amplia libertad en las mismas[275], y en la certeza de que seguridad y libertad son compatibles, creo que el principio de seguridad resulta importante para encontrar un equilibrio entre el deber del Derecho penal de adaptarse al desarrollo tecnológico y la regulación excesiva y sin sentido del mismo. Para ello, no

---

Carece de sentido pretender perseguir toda innovación tecnológica, pero un alto grado de permisividad conlleva el deber ineludible de vigilar las innovaciones.

[273] Romeo Casabona, *Principio de precaución, Biotecnología y Derecho,* p. 419.

[274] J. Mazur, "Automated Decision – Making and the Precautionary Principle in EU Law", *Baltic Journal of European Studies,* vol. 9, no. 4, 2019, pp. 14 – 15. Cuando estas decisiones automatizadas supongan un riesgo serio para la salud pública o exista un elevado nivel de impredecibilidad en su aplicación a las políticas para la protección de la salud, también será posible aplicar el principio de precaución a las mismas.

[275] Romeo Casabona, *La adaptación del derecho penal al desarrollo social y tecnológico,* p. 330. Para garantizar el deseable objetivo de que imperen las actitudes y los comportamientos responsables y respetuosos en Internet, es necesario crear un entramado jurídico diversificado que se adapte a las nuevas realidades y necesidades sociales que se derivan de las TIC, aunque no necesariamente debe ser nuevo.

hay que olvidar que debe aplicarse en base a la razón[276], de manera proporcional, y que es importante recordar su simpleza[277] original para alejarlo de construcciones teóricas complejas que impidan determinar su aplicabilidad a ciertos tipos de delito en particular.

No existe, en la actualidad, una tecnología en el ámbito de la ciberseguridad que cumpla los dos requisitos necesarios para la intervención del principio de precaución, a saber: riesgo para muchos e incertidumbre. Es decir, que conlleve la posibilidad de que una conducta humana cause daños colectivos relacionados con situaciones catastróficas que afecten a un conjunto de seres vivos, o que cree una ausencia de evidencia científica respecto a la demostración de un nexo causal, esto es, de una relación de causalidad entre el daño que se teme y se pretende evitar y, si llega a producirse, la acción correspondiente. Y esto por dos motivos: primero, que, como explicaré de manera extensa en el apartado siguiente, el Derecho penal español ha sabido adaptarse a la actualidad tecnológica de manera notable, siendo muy limitadas, en consecuencia, las conductas atípicas, y mucho menos las idóneas para cumplir los requisitos antes mencionados; segundo, que, en la actualidad, tampoco hay una tecnología en el ámbito de la ciberseguridad que los cumpla, de manera que si no existe esta nueva tecnología, no puede tampoco someterse a una valoración en relación con los mismos, por lo que prever una respuesta en el ámbito penal resulta imposible. Hay que introducir, en este sentido, una diferenciación importante entre la utilización de la tecnología que nos parece éticamente reprobable y la que merece el reproche del Derecho penal. Así, el hecho de que millones de usuarios en todo el mundo entreguen *motu proprio* sus datos a gigantescas bases de datos controladas por empresas privadas con dudosas intenciones es increíblemente preocupante desde una perspectiva ética, ya

[276] A. Christiansen, "Rationality, Expected Utility Theory and the Precautionary Principle", *Ethics, Policy & Environment,* vol. 22, no, 1, 2019, p. 18. La idea de que el principio de precaución exige grandes sacrificios para garantizar la seguridad se ha exagerado, teniendo en cuenta que debe aplicarse con proporcionalidad.

[277] H.O. Stefánsson, "On the Limits of the Precautionary Principle", *Risk Analysis,* vol. 39, no. 6, 2019, p. 1204. No solo eso, sino que es suficientemente difuso como para encajar en decisiones contradictorias.

que considero que, con el paso de los años, esta información será utilizada contra los intereses de los propios usuarios y, de cumplirse la peor de mis previsiones, cimentará la construcción de una tiranía política mundial sustentada sobre la tecnología.

No obstante, las elaboradas técnicas de ingeniería social utilizadas para que las personas lleven a cabo esta acción de forma voluntaria convierten en inútil cualquier propuesta del Derecho penal de intervenir e impedir la catástrofe futura. No es ético, pero sí es legal. En consecuencia, solo queda presenciar estas conductas carentes de ética basadas en maniobras de ingeniería social y psicología de masas que hacen que los usuarios se pongan voluntariamente en torno al cuello las sogas con la que, simbólicamente, serán ahorcados en el futuro. Y todo ello, como digo, es legal, pese a su ausencia de ética[278] y a las cotas de incertidumbre tecnológica que le son inherentes de manera inevitable.

La inexistencia, en la actualidad, de una tecnología en el ámbito de la ciberseguridad que reúna las características necesarias para la utilización del principio de precaución no garantiza su inexistencia futura. Esto obliga al legislador penal a permanecer vigilante en relación con cualquier posible salto tecnológico pero, incluso en este caso, y salvo que se trate de un avance tecnológico que introduzca un nuevo paradigma, la adecuada intervención del Derecho penal se basará más, como así ha sido hasta ahora, en un poder legislativo con capacidad de adaptación rápida a los cambios que en el principio de precaución. Así, la relación entre el Derecho penal y el principio de precaución en lo que se refiere a los delitos contra la ciberseguridad debería basarse en tres puntos fundamentales.

---

[278] A. Cortina, “Fundamentos filosóficos del principio de precaución”, en C.M. Romeo Casabona (edit.), *Principio de precaución, Biotecnología y Derecho*, Granada, Comares, 2004, p. 15. Las decisiones sobre tecnologías de riesgo no pueden ser tomadas únicamente por los expertos, las empresas que financian las investigaciones y los políticos, sino que el pueblo también debe poder opinar y participar en las mismas. Esta loable afirmación, que comparto, no deja de ser cierta por mucho que la ingeniería social y la psicología de masas empujen a las personas a tomar decisiones que, en ocasiones, son negativas para sus intereses. Y es que corresponde a los académicos dar un paso al frente y luchar por la verdad, aunque esto haya ido sucediendo cada vez menos hasta llegar al actual estado de las cosas, en el que no sucede en absoluto.

Primero, la vigilancia del desarrollo de la tecnología como medio para prever la introducción de un nuevo paradigma con características idóneas para la aplicación del principio de precaución. Es importante, en este sentido, no solo identificar los bienes jurídicos susceptibles de ser lesionados, sino también valorar la posibilidad de que otras ramas del derecho sancionen la conducta antes de recurrir al Derecho penal, con objeto de que prevalezcan los principios de protección de bienes jurídicos, de intervención mínima o *ultima ratio* y de subsidiariedad como límite a la proclividad expansiva de este principio[279].

Teniendo en cuenta lo anterior, debe realizarse, para valorar objetivamente si una conducta es peligrosa, un análisis *ex ante* de previsibilidad objetiva basado en el saber ontológico (o circunstancias del caso concreto cognoscibles por el juez y el autor) y en el saber nomológico (o experiencia común de la época sobre los cursos causales). No concuerdo con la idea de que el resultado de la valoración, para ser tenido en cuenta, deba reflejar siempre como no absolutamente improbable la producción de la lesión de un bien jurídico. Ahora bien, dicho juicio podría traducirse en una respuesta extrapenal, que iría desde la recomendación de no iniciar la actividad (o, en los casos más extremos, su prohibición, adoptada por la autoridad competente) hasta una moratoria sobre la misma de distinta duración, mientras no se dispongan de conocimientos técnicos más fiables[280].

Segundo, una vigilancia doblemente atenta en relación con la verdadera amenaza: el desarrollo tecnológico menor (es decir, aquel que, sin introducir un nuevo paradigma, tiene lugar con el paso del tiempo de manera constante), que también es el más habitual. Tanto el *hardware* como el *software* se actualizan de manera progresiva, de forma que, junto a los incidentes de ciberseguridad reales en relación con los cuales informen los CERT y aquellos que lleguen a sede judicial, hacen necesaria una actualización jurídico-penal rápida mediante una adaptación de los tipos

[279] Romeo Casabona, *Principio de precaución, Biotecnología y Derecho,* p. 421.

[280] Romeo Casabona, *Principio de precaución, Biotecnología y Derecho,* pp. 405 – 406.

delictivos existentes o, solo cuando sea estrictamente necesario, la creación de otros nuevos. En este segundo caso, la capacidad del poder legislativo de adaptar las normas penales al desarrollo tecnológico, incluyendo aspectos como la brevedad del plazo para completar la adaptación, es lo que distinguirá un ordenamiento jurídico actualizado y con capacidad de solvencia de uno obsoleto e inservible.

Tercero, no entreverar las características de los dos puntos anteriores para, amparándose en el principio de precaución y en la necesidad de proteger a las personas, introducir previsiones en el ámbito penal en relación con conductas total o parcialmente inocuas, ignorando los principios de protección de bienes jurídicos, de intervención mínima o *ultima ratio* y de subsidiariedad o, en sentido contrario, postergar innecesariamente la actualización del CP en relación con conductas demostradamente lesivas para ciertos bienes jurídicos protegidos basándose en construcciones teóricas o discusiones doctrinales que vayan más allá de lo razonable. A cada desarrollo tecnológico le corresponde su orden.

3.3 Derecho penal sustantivo

3.3.1 Construcción de los perfiles de los delitos que afectan a la ciberseguridad

La doctrina ha realizado, en este ámbito, clasificaciones muy distintas[281] [282] [283] [284] basadas en criterios dispares, refiriéndose casi siempre a la ciberdelincuencia en su conjunto o a un grupo de delitos en particular. No obstante, no ha habido un intento de desarrollar un *numerus clausus* que permita categorizar los delitos que afectan a la ciberseguridad y distinguirlos como pertenecientes a un grupo propio y distinto dentro de la categoría más amplia de los ciberdelitos, en la que se incardinan tanto tipos delictivos encuadrables dentro del primero como otros que, con base en sus características, no pertenecen al mismo[285].

---

[281] M. Robles Carrillo, "Las fuerzas armadas ante el reto de la ciberseguridad", en S. Olarte Encabo (dir.), *Estudios sobre derecho militar y defensa,* Cizur Menor, Navarra, Aranzadi, 2015, p. 440. La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, incluye la definición de seguridad en su preámbulo, afirmando que constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones. Del mismo modo, reconoce que la regulación vigente a tal efecto se articula en un modelo tradicional y homologable con los países de nuestro entorno que, aunque se ha demostrado válido hasta ahora, no lo es más, puesto que en el mundo actual, y en el entorno más previsible para el futuro, los actores y circunstancias que ponen en peligro los niveles de seguridad se encuentran sujetos a constante mutación, y es responsabilidad de los poderes públicos dotarse de la normativa, procedimientos y recursos que le permitan responder eficazmente a estos desafíos a la seguridad. El modelo tradicional de seguridad, en consecuencia, no permite abordar los retos y amenazas actuales y futuros y es necesario el establecimiento de una articulación diferente. Esto es trasladable, siempre teniendo en cuenta sus principios, al Derecho penal, en relación con el cual el avance de la tecnología hace necesaria una constante reflexión intelectual para garantizar su actualización.

[282] Instituto Nacional de Ciberseguridad de España / Agencia Estatal Boletín Oficial del Estado, *Código de Derecho de la Ciberseguridad: edición actualizada a 4 de mayo de 2022,* Madrid, Instituto Nacional de Ciberseguridad de España / Agencia Estatal Boletín Oficial del Estado, 2022, pp. 863 – 892. En este caso, la categoría que se utiliza para la selección de los delitos es la ciberdelincuencia, en sentido general.

[283] Fernández Bermejo y Martínez Atienza, *Ciberseguridad, Ciberespacio y Ciberdelincuencia*, pp. 156 – 158. Se habla de tipos penales informáticos, una categoría que resulta demasiado extensa y poco concreta.

[284] V. Moret Millás, "El marco jurídico de la ciberseguridad en España", en F. Pérez Bes (coord.), *El derecho de Internet*, Barcelona, Atelier, 2016, pp. 268 – 269. Al menos, se realiza una selección más exhaustiva y se enumeran solo los delitos con una relación más directa con la ciberseguridad, aunque en sentido amplio.

[285] A. Rallo Lombarte et al*., Robo de identidad y protección de datos,* Cizur Menor, Navarra, Aranzadi, 2010, p. 33. Ya hace años se preveía la necesidad de ofrecer garantías en relación con la identidad electrónica, así como de establecer normas protectoras para las personas físicas que utilizasen las nuevas tecnologías. No obstante, este delito no encaja en la definición propuesta, no siendo un delito que afecte a la ciberseguridad, toda vez que, en ausencia de cualquiera de las conductas descritas a continuación, y al igual que en el caso de la falsedad en documentos públicos o privados,

Para crear esta subcategoría propia y distinta para los delitos que afectan a la ciberseguridad, resulta condición indispensable, en primer lugar, contar con un criterio, como el que desarrollé en el capítulo primero de esta investigación, y según el cual son delitos que afectan a la ciberseguridad aquellos que lesionan de cualquier manera la seguridad de una red o sistema informáticos, afectando así a su disponibilidad, a su integridad o a su confidencialidad. Así, los tipos delictivos pertenecientes a esta subcategoría de los ciberdelitos son los que recogen conductas idóneas para este resultado, debiendo rechazar la integración en la misma de aquellos otros que, por sus características, no lo hacen. Su elemento distintivo es la lesión de la ciberseguridad, aunque en la mayoría de los casos este característico acceso no autorizado, considerado como elemento nuclear del tipo, sea solo un medio para la comisión de un delito fin susceptible de lesionar bienes jurídicos distintos.

A partir de lo anterior pueden sacarse tres conclusiones: primera, que el hecho de que muchos de los delitos pertenecientes a la categoría de los ciberdelitos no pertenezcan, a su vez, a la subcategoría de los delitos que afectan a la ciberseguridad, no significa que no deban ser perseguidos, correspondiendo a las autoridades competentes dicha persecución en una red informática que, a pesar de haber sufrido la comisión de un delito en su seno, gozará, en lo concerniente a sí misma, de la cualidad de segura (sirva como ejemplo el hecho de que el BCSC nada tiene que decir en relación con un caso de *grooming* o engaño pederasta por Internet, pero sí debe ponerlo en conocimiento de las autoridades competentes para su persecución); segunda, que la especificidad del criterio desarrollado conlleva que los tipos delictivos que integran los delitos que afectan a la ciberseguridad se encuentren dispersos[286]; y tercera, que lo anterior se debe a que, junto a los

en ausencia de una acción que afecte al art. 197 bis 1, la conducta afecta solo al contenido del sistema informático, al cual puede haberse accedido de manera legítima y sin traspasar ninguna medida de ciberseguridad establecida para evitarlo.

[286] Barrio Andrés, *Ciberdelitos*, p. 55. Hay que tener en cuenta que en el Derecho penal español partimos de la base de una importante dispersión normativa no en materia de delitos que afectan a la ciberseguridad, sino de la categoría más amplia de ciberdelitos, ya que los distintos preceptos se encuentran diseminados a lo largo del articulado del

delitos que afectan a la ciberseguridad como tales, en relación con los cuales no cabe ninguna duda de su pertenencia a esta subcategoría, es posible encontrar en el articulado del CP preceptos que contienen uno o varios elementos característicos de los mismos y que sin embargo, analizados en su conjunto, no contienen más que estos elementos meramente residuales.

Así, el art. 197 bis 1 del CP, pese a su incorrecta ubicación actual entre los delitos de descubrimiento y revelación de secretos, pertenece a dicha subcategoría y puede considerarse en su totalidad un delito contra la ciberseguridad, pero no sucede lo mismo con el art. 270.6 del CP, el cual, a pesar de recoger una conducta encuadrable dentro de los delitos que afectan a la ciberseguridad, no tiene relación alguna con los mismos más allá de este apartado sexto al pertenecer al art. 270 del CP, dedicado a los delitos relativos a la propiedad intelectual, los cuales, en su actual configuración, no pueden considerarse en su conjunto como parte de la mencionada subcategoría de delitos que afectan a la ciberseguridad. La diferencia la marcan detalles muy sutiles, pero siempre objetivos.

Continuando con la creación de una subcategoría propia y distinta para los delitos que afectan a la ciberseguridad, en segundo lugar no hay que olvidar que, tal y como he expuesto en el capítulo primero de esta investigación, la legislación penal internacional y de la UE tienen una enorme influencia en este ámbito, de manera que se convierte en especialmente importante analizar cómo se han trasladado las mismas al ordenamiento jurídico español con objeto de detectar los artículos resultantes. Actualmente, las conductas que se describen en los arts. 3, 4, 5 y 6 de la Directiva 2013/40/UE han sido transpuestas casi literalmente[287] en los arts. del CP español 197 bis 1 (acceso ilegal), 197 bis 2 (interceptación ilegal, protegiendo no solo las comunicaciones entre personas, sino las llevadas a cabo entre sistemas de información), 264.1 (interferencia en los datos) y 264 bis 1

CP dependiendo de los bienes jurídicos a los cuales se encuentran vinculados. En opinión de Barrio Andrés, no existe vínculo común alguno entre los ciberdelitos en el CP español.

[287] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 723.

(interferencia en los sistemas). Como de costumbre, se puede apreciar una mayor tendencia punitiva en el texto legal español, como en el caso del art. 197 bis 1 del CP, que sanciona la facilitación del acceso ilegal, lo que no ocurre en la Directiva. El artículo 197 bis 2, por su parte, no exige la utilización de medios técnicos en la interceptación para poder proceder a la sanción. Por último, y más importante, en los dos casos anteriores no se tiene en cuenta el principio de insignificancia recogido en la Directiva, de acuerdo con el cual hubiese sido posible para el legislador español no sancionar aquellos casos de menor gravedad[288].

El art. 264.1 también va más allá de lo dispuesto en la Directiva al sancionar no solo la interferencia en los datos, sino también en programas informáticos o documentos electrónicos. El art. 264 bis 1, por su parte, añade como conductas a sancionar las de su letra c), relativas a la destrucción, daño, inutilización, eliminación o sustitución de sistemas informáticos, telemáticos o de almacenamiento de información electrónica. La Directiva de 2013 exigía una serie de medidas en su art. 7 relativas a los instrumentos utilizados para cometer las infracciones descritas. Estas medidas, que ya se adoptaban en el art. 248.2 b), que castiga las estafas, o en el art. 400, relativo a las falsedades, se extendieron tanto al art. 197 ter como al art. 264 ter, con una redacción idéntica, que suponía una transcripción casi literal de la normativa de la UE. De nuevo, se dejó fuera el principio de insignificancia[289].

El art. 9 de la Directiva 2013/40/UE, en sus apartados 1 y 2, exige un marco penal que se respeta tanto en lo relativo a los accesos (arts. 197 bis 1 y 197 bis 2 del CP) como en lo concerniente a los daños (arts. 264.1 y 264 bis 1 del mismo texto legal), así como en lo que corresponde a los actos preparatorios (arts. 197 ter y 264 ter del CP). Se cumple, también, lo establecido por su art. 9.3, que obliga a llegar a una pena máxima de al menos tres años de privación de libertad en determinados supuestos, como sucede

[288] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* pp. 238 – 239.

[289] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 239.

en los arts. 264.2 y 264 bis 2 del CP (llegándose a prever una pena de hasta ocho años de prisión, en el caso de este último). El art. 9.4 de la Directiva, que contiene asimismo exigencias agravatorias, también se ha trasladado al ordenamiento estatal a través de arts. del CP como el 264.2.4, relativo a hechos que afecten a sistemas informáticos de una infraestructura crítica. La previsión del art. 9.5 de la Directiva sobre el uso ilícito de datos de carácter personal para interferir ilegalmente en los sistemas de información o en los datos (arts. 4 y 5 de la norma de la UE) se refleja adecuadamente en los arts. 264.3 y 264 bis 3 del CP[290].

No cabe duda de que, tras la reforma introducida por la LO 5/2010, de 22 de junio, la LO 1/2015, de 30 de marzo, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal, ha supuesto la culminación de la adaptación de nuestra legislación a la de la UE, poniendo a España a la vanguardia en lo que se refiere al nivel punitivo[291]. No obstante, el legislador español, quien hasta ahora, por las temáticas abordadas, había sido capaz de realizar la transposición de la legislación europea respetando la sistemática tradicional del CP recurriendo a fórmulas como, por ejemplo, la introducción de artículos bis, no es tan fiel como debería serlo a la esencia de las normas comunitarias. Es necesario, para conseguir una fidelidad mayor, no solo intentar acomodar las redacciones legales, sino, una vez comprendido el objetivo comunitario, abordarlas desde ese entendimiento.

Además, otro aspecto controvertido es la valoración de hasta qué punto puede la actuación de la UE quebrar el principio de proporcionalidad de las normas penales en el derecho interno, sobre todo al vincular una pena específica a un supuesto de hecho determinado[292]. Así, el tipo básico de

---

[290] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 239.

[291] N.J. De la Mata Barranco, *Derecho penal europeo y legislación española: las reformas del Código Penal*, 1ª ed., Valencia, Tirant lo Blanch, 2015, p. 97. Esta adaptación quizá haya sido excesiva en algunos puntos.

[292] N.J. De la Mata Barranco, *El principio de proporcionalidad penal*, 1ª ed., Valencia, Tirant lo Blanch, 2007, p. 128. El principio de proporcionalidad vincula al legislador en sus decisiones de incriminación *ex novo* de un determinado comportamiento y de modificación de los elementos positivos de cada tipo de injusto, en la previsión o concreción de causas de justificación o de disminución de la culpabilidad específicas y

daños previsto en el art. 263 del CP se castiga con una pena de multa de seis a veinticuatro meses, mientras que si los daños recaen sobre un elemento informático el art. 264 del mismo texto legal prevé la imposición de una pena de prisión de seis meses a tres años. Lo mismo sucede con la exigencia de determinados máximos penales que han llevado al legislador español a prever penas de hasta ocho años de prisión como castigo para actos claramente menos graves que las lesiones agravadas, cuya pena es menor (si bien, en este caso, fue el propio legislador estatal el que incurrió en un exceso, puesto que la Directiva de 2013 exigía un máximo de cinco años de prisión).

Por último, también resulta discutible la obligación de sancionar ciertas conductas, como la tenencia de instrumentos, no existiendo paralelo en este sentido en otros campos delictivos. Resulta indudable, en cualquier caso, que el Derecho penal informático refleja las políticas de la UE en este ámbito, y estas se sustentan en la armonización legislativa y en la exigencia y concreción de sanciones desde una perspectiva expansiva y sancionadora. Su influencia en los ordenamientos penales estatales resulta decisiva para su configuración[293].

En tercer y último lugar, una vez puesta de manifiesto la influencia de la legislación internacional y de la UE, considero necesario realizar un análisis individualizado de los delitos que cumplen con los criterios expuestos y, por lo tanto, resultan adecuados para integrar la subcategoría propia y distinta de los delitos que afectan a la ciberseguridad. Este análisis, aunque omnicomprensivo, resultará desigual a causa del rigor que requiere, toda vez que en el mismo expondré, junto a artículos del CP español que analizaré en profundidad por considerarlos delitos que afectan a la ciberseguridad en su totalidad, otros artículos aislados que, si bien, por sí mismos, reúnen los requisitos necesarios para integrarse en esta subcategoría, en ocasiones se

---

en la determinación abstracta de la pena que corresponde a cada comportamiento considerado como punible.

[293] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* pp. 240 – 241.

encuadran dentro de artículos que no guardan relación en absoluto con esta clase de delitos teniendo, por lo tanto, un interés menor, si bien posibilitarán otro tipo de reflexiones en el apartado dedicado a la propuesta de *lege ferenda*. Será en este apartado en el que abordaré, una vez concluido el análisis crítico de *lege lata*, aspectos como la necesidad, o no, de desarrollar un delito genérico contra la ciberseguridad.

3.3.2 Los delitos que afectan a la ciberseguridad en el Código Penal

3.3.2.1 Ciberseguridad en los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

3.3.2.1.1 Apoderamiento de secretos documentales

La rúbrica "Del descubrimiento y revelación de secretos" recoge en el Capítulo I del Título X del CP varios delitos cuyo objetivo común es que determinados hechos solo sean conocidos por las personas a las que estos conciernen, quienes no desean que otros accedan a información o datos solo conocidos por ellas o por un reducido círculo (teniendo, por tanto, la consideración de secretos). Al mismo tiempo, se protege el derecho de las personas a controlar la información o los hechos que afecten a su vida privada y, por extensión, a su intimidad[294]. Si bien el descubrimiento y la revelación de los mencionados secretos y hechos íntimos constituyen el núcleo de estos tipos delictivos[295], solo resultan de interés para esta investigación aquellos en

[294] C.M. Romeo Casabona, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho Penal, Parte Especial*, 2ª ed., Granada, Comares, 2022, p. 267. Es importante destacar que algunos de los delitos que afectan a la intimidad, al deber de secreto y a la inviolabilidad del domicilio se localizan en títulos distintos del CP. Es el caso de los delitos de infidelidad en la custodia de documentos y la violación de secretos (arts. 413 a 418) y de los atentados contra la inviolabilidad del domicilio y las demás garantías de la intimidad (arts. 534 a 536), que también serán objeto de análisis por su relación con la ciberseguridad.

[295] F. Muñoz Conde, *Derecho Penal, Parte Especial*, 23ª ed., Valencia, Tirant lo Blanch, 2021, p. 273.

torno a los que se hayan establecido medidas de ciberseguridad con objeto de protegerlos, no importando los que carecen de protección.

La propia Fiscalía General del Estado ha definido las medidas de seguridad como aquellas que se hayan establecido con la finalidad de impedir el acceso al sistema, sin importar su solidez, complejidad o robustez, ni tampoco si han sido establecidas por el administrador, por el usuario o por el instalador del sistema, siempre que cumplan el requisito de mantenerse operativas por quien está legitimado para evitar el acceso de terceros.

La conducta consistente en el mero apoderamiento de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales para descubrir los secretos o vulnerar la intimidad de otro[296] en ausencia de su consentimiento, recogida en el inciso primero del art. 197.1 del CP, constituye un ejemplo de ausencia de las protecciones debidas en relación con la información, puesto que incluso cuando los datos reservados se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado y sea de aplicación el apartado 2 del art. 197 del CP[297], seguirá tratándose de información no protegida por barrera de seguridad informática alguna, y que no goza del amparo, en consecuencia, de medidas de ciberseguridad. Hay que aclarar que, si bien la acción típica consiste en apoderarse de los objetos materiales recogidos en el tipo delictivo[298] [299], se ha ido adaptando el mismo

[296] J. Barja de Quiroga López, M. A. Encinar del Pozo, y M.ª A. Villegas García, *Código Penal. Comentado, con jurisprudencia sistematizada y concordancias,* 8ª ed., Madrid, Francis Lefebvre, 2021, p. 697. El sujeto pasivo del delito, de acuerdo a la STS de 14 de octubre de 2011, debe ser, además del titular del bien jurídico protegido, también el titular del objeto material del delito, pues se utiliza el posesivo *sus*, tanto cuando se hace referencia a los papeles como en relación con la interceptación de las telecomunicaciones.

[297] Muñoz Conde, *Derecho Penal, Parte Especial*, p. 275.

[298] M.ª A. Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal,* 1ª ed., Barcelona, Atelier, 2018, p. 71. Este libro tiene una gran influencia en este capítulo.

[299] M.ª A. Rueda Martín, *Protección penal de la intimidad personal e informática: los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código penal*, 1ª ed., Barcelona, Atelier, 2004, p. 43. El art. 26 del CP define lo que se entiende por documento en el ámbito jurídico-penal.

al avance de la tecnología[300], aceptándose en la actualidad como conducta típica el apoderamiento de elementos como los antiguos disquetes y CD-ROM o sus equivalentes actuales, siempre que el elemento cumpla el requisito de contener retazos de la intimidad de otra persona[301] [302].

En efecto, se ha producido un proceso de espiritualización de los objetos susceptibles de apoderamiento, hasta el punto de que, tal y como establecen sentencias como la STS 538/2021, de 17 de junio[303], basta la aprehensión virtual o digital del documento, sin importar que con posterioridad nunca se llegue a tener el mismo en formato físico[304].

Al no verse afectada la seguridad física ni lógica de las redes o sistemas informáticos, ni la disponibilidad, la integridad ni la confidencialidad de los datos contenidos en los mismos, esta modalidad delictiva debe ser tenida en cuenta únicamente como reflejo de una gestión obsoleta de la seguridad informática y como evidencia de la aceptación por parte del legislador de la existencia de un nivel inexistente de la misma en ausencia de unas medidas adecuadas orientadas a su protección y, por extensión, a la protección de la intimidad y de los datos reservados de carácter personal amparados tras las mismas.

3.3.2.1.2 Interceptación de comunicaciones

El art. 197.1 del CP castiga, en su inciso segundo, a quien para descubrir los secretos o vulnerar la intimidad de otro sin su consentimiento

---

[300] C.M. Romeo Casabona, "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de la red", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* no. 10, 2006, p. 15. El sentido de su apoderamiento se ha espiritualizado progresivamente.

[301] A. Juanes Peces, "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Capítulo I. Del descubrimiento y revelación de secretos", en C. Conde-Pumpido Tourón (dir.), *Comentarios al Código Penal, Tomo 2*, Barcelona, Bosch, 2007, p. 1541. La acción típica puede consistir, incluso, en el conocimiento de un contenido sin necesidad de apoderarse materialmente de su soporte.

[302] Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos,* p. 78.

[303] ECLI:ES:TS:2021:2451.

[304] Romeo Casabona, *Derecho Penal, Parte Especial*, pp. 269 - 270.

intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación (es decir, ondas radioeléctricas, vía satélite o cualquier otro tipo de comunicación telemática o a distancia que se desarrolle a medida que avance la tecnología[305]). Este último inciso ofrece ciertas dudas por su amplitud. Aunque, por lógica, debería vincularse solo con las señales de comunicación conocidas o por descubrir con las que las mencionadas en el tipo compartan ciertas características tecnológicas, esta expresión tan genérica refleja el intento del legislador de prevenir problemas de tipicidad y lagunas de punición provocados por los avances de la tecnología en detrimento de la seguridad jurídica[306]. Y es que mediante la simple inclusión del adjetivo "semejantes" hubiese podido asegurarse de no sacrificarla. Hay que destacar dos elementos: primero, que la captación de las comunicaciones orales solamente puede considerarse típica si se utilizan artificios técnicos (como micrófonos) para ello[307]; segundo, que la interceptación relativa a las telecomunicaciones abarcaría conductas como el acceso al correo electrónico del sujeto pasivo después de vulnerar medidas de ciberseguridad como la clave de acceso establecida para protegerla[308]. Un aspecto criticable es que la pena abstracta prevista por el legislador tanto para el apoderamiento de secretos documentales como para la interceptación de comunicaciones es la misma (prisión de uno a cuatro años y multa de doce a veinticuatro meses), incluso cuando en el primer caso la intimidad y los datos reservados de carácter personal, entendidos como bienes jurídicos a proteger, se encuentran directamente expuestos sin protección alguna, y en el caso de la interceptación de comunicaciones se acepta la posible existencia de medidas de ciberseguridad como las claves de acceso y, en

[305] Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos,* pp. 93 – 94.

[306] Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos,* p. 97.

[307] A. Serrano Gómez et al., *Curso de Derecho Penal. Parte Especial*, 6ª ed., Madrid, Dykinson, 2021, p. 216. La consumación del delito sucede en el momento de la interceptación de la conversación. Cuando solo se hayan instalado o preparado los aparatos, pero sin llegar a conectarlos, se tratará de una tentativa.

[308] Muñoz Conde, *Derecho Penal, Parte Especial*, p. 276.

determinados casos, solo se lesionará uno de los dos anteriores después de haber rebasado la barrera de la seguridad informática.

3.3.2.1.3 Descubrimiento del secreto recogido en archivos o registros

La crítica relativa a la pena abstracta que afecta al apoderamiento de secretos documentales y a la interceptación de comunicaciones puede extenderse a este delito contenido en el art. 197, párrafo segundo, del CP, que castiga con las mismas penas tipificadas en el párrafo primero a quien, en ausencia de autorización, se apodere, utilice o modifique en perjuicio de terceros datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, así como a quien acceda por cualquier medio[309] a los mismos y a quien los altere o utilice en perjuicio de su titular en ausencia de autorización. El objeto sobre el que recaen las distintas acciones tipificadas son los datos reservados de carácter personal o familiar de otro registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado[310]. Por "reservados" hay que entender aquellos datos personales de acceso limitado para terceros ajenos al fichero, aunque no sean íntimos en sentido estricto, siempre que cumplan el requisito de no estar al alcance de terceras personas ajenas a su tratamiento autorizado, y quedando excluidas, en consecuencia, las fuentes accesibles al público y cualesquiera otros datos para cuyo acceso o conocimiento no se requiera la autorización o el consentimiento del interesado[311]. Esta limitación en el acceso es esencial para entender este delito, puesto que da lugar a tratar dos conductas típicas relacionadas con la ciberseguridad: primera, el acceso excediéndose de la autorización (art. 197.2, primer inciso), en el que el autor

[309] J. Gómez Navajas, *La protección de los datos personales: un análisis desde la perspectiva del Derecho Penal*, 1ª ed., Navarra, Civitas, 2005, p. 147. El acceso a los datos "por cualquier medio" es una expresión que se utiliza tanto en este art. 197.2, inciso segundo, del CP, como en el art. 278 del mismo texto legal.

[310] Muñoz Conde, *Derecho Penal, Parte Especial*, p. 277.

[311] Romeo Casabona, *Derecho Penal, Parte Especial*, p. 273.

está legitimado para acceder al fichero, pero se excede de dicha autorización y se apodera o modifica datos más allá de sus funciones legítimas o para fines ajenos a su competencia o autorización; segunda, el acceso no autorizado (art. 197.2, segundo inciso), en el que el sujeto activo es un *extraneus* (aunque no siempre) que accede a los datos por cualquier medio, es decir, venciendo los mecanismos físicos o lógicos de seguridad, o mediante engaños, o de cualquier otro modo, siendo suficiente, al contrario que en el inciso anterior, la mera captación intelectual de los datos, incluso en ausencia de apoderamiento, aprehensión física, reproducción o copia de los mismos. Hay que señalar, además, la existencia de conductas alternativas como la modificación o la alteración de los datos afectando a su integridad, de modo que no reflejen la realidad de la que daban constancia o no sean ya útiles u operativos para el fin al que estaban destinados[312].

El matiz que relaciona este art. 197.2 con la ciberseguridad es muy sutil: cuando se trate de accesos indebidos, debe tratarse siempre de un acceso por cualquier medio siempre que pueda considerarse ilícito, incluyendo esto la inhabilitación de las medidas de ciberseguridad establecidas al efecto. En el capítulo cuarto de esta investigación, por su orientación hacia la protección de la actividad, sobre todo, de los hospitales y de los centros sanitarios, adquirirá gran importancia una de las cualificaciones aplicables a estos delitos recogidos en los párrafos primero y segundo: la prevista en el art. 197.5, relativa al carácter sensible de los datos, que obliga a la imposición de la pena prevista en su mitad superior cuando los datos afectados revelen, entre otros, el estado de salud del sujeto pasivo[313].

Aunque no siempre es posible compartir o desentrañar claramente el sentido político-criminal del abundante conglomerado que conforman estos tipos agravados[314], no cabe duda del fundamento y la legitimidad político-criminal de la protección que el art. 197.5 del CP proporciona a los datos sensibles, al ser una medida jurídica orientada a la protección reforzada del

[312] Romeo Casabona, *Derecho Penal, Parte Especial*, p. 275.
[313] Muñoz Conde, *Derecho Penal, Parte Especial*, p. 278.
[314] Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos,* p. 145.

así llamado núcleo duro de la intimidad[315]. Se incardinan en dicho núcleo, entre otros, los datos referidos a la salud[316], tratándose de datos sensibles o hipersensibles cuyo conocimiento o utilización por parte de terceros hace más vulnerable a su titular, sobre todo en ausencia de su consentimiento. Al tratarse de datos muy sensibles, procede establecer garantías reforzadas orientadas a asegurar de manera efectiva dicha protección, como la prohibición del acceso a los mismos o de su tratamiento en archivos automatizados cuando no exista dicho consentimiento, o la limitación del acceso o de su utilización en los demás casos. A pesar de la importancia de estos datos, quedan fuera del ámbito penal conductas como la creación de ficheros con el objetivo único de almacenar algunos de ellos[317].

3.3.2.1.4 Actual configuración del delito de intrusión en un sistema de información

3.3.2.1.4.1 Inadecuada ubicación entre los delitos de descubrimiento y revelación de secretos

Actualmente, los delitos de descubrimiento y revelación de secretos[318] están regulados bajo una rúbrica con esta denominación en el Capítulo I,

---

[315] Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal,* p. 146.

[316] P. Nicolás Jiménez, *La protección jurídica de los datos genéticos de carácter personal,* 1ª ed., Granada, Comares, 2006. También de la misma autora, "La protección de los datos genéticos de carácter personal en Derecho penal español: un caso práctico", en E.J. Armaza Armaza, J. Mendoza Valdez, I. De Miguel Beriain y A. Urruela Mora (coords.), *Temas de Derecho penal: libro homenaje a Luis Guillermo Cornejo Cuadros,* Arequipa, Adrus, 2008, p. 189. Más recientemente, destacan artículos como "Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos", *Revista de Derecho y Genoma Humano: Genética, Biotecnología y Medicina Avanzada*, no. extra, 2019, p. 129. Los datos genéticos son un excelente ejemplo de datos especialmente protegidos.

[317] Romeo Casabona, *Derecho Penal, Parte Especial*, pp. 279 – 280.

[318] M. Mínguez Rosique, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Sección 1. Descubrimiento y revelación de secretos", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, p. 1178. La técnica legislativa empleada en estos delitos resulta deficiente, puesto que el resultado es una regulación tan enrevesada que incluso su

Título X, Libro II del CP. Su evolución histórica fue lenta, produciéndose, por lo general, con retraso en comparación con otros delitos o instituciones jurídico-penales del mismo[319]. Los pasos orientados a su actualización fueron aislados, surgiendo con el paso del tiempo una crítica doctrinal unánime en su pretensión de revisarlos y actualizarlos. Antes del CP de 1995, estos delitos, aunque figuraban también en un mismo título del CP de 1973, estaban estructurados de manera diferente, puesto que aparecían agrupados junto con otros delitos de muy diversa factura[320].

En 1994, después de que la realidad demostrase la vulnerabilidad existente frente al acceso intencionado o fortuito de las comunicaciones realizadas a través de unas nuevas tecnologías en constante innovación y desarrollo, y a pesar de la inminente reforma total del CP de 1973 que tendría lugar un año después, el legislador introdujo el art. 497 bis para ampliar la cobertura penal de las comunicaciones personales por medios técnicos, ampliando para ello el objeto material del delito a las telecomunicaciones o a cualquier telecomunicación. Solo un año después, en el CP de 1995, los variados delitos antes agrupados fueron separados y reagrupados atendiendo a los bienes jurídicos realmente implicados. Además, una

interpretación plantea problemas. Los preceptos adolecen de un importante déficit de precisión y claridad y, sobre todo, resulta problemática la desafortunada ubicación de preceptos como el art. 197 bis 1 del CP.

319 Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal,* pp. 15 – 16. Ya era posible encontrar los delitos de descubrimiento y revelación de secretos en el CP de 1822, más específicamente en su art. 718, Capítulo I, Título II, dedicado a las calumnias, los libelos infamatorios, las injurias y la revelación de secretos confiados. En años posteriores, su regulación se llevó a cabo englobándolos dentro de los delitos contra la libertad y la seguridad. Así lo reflejan los distintos CP: el de 1848 (en su Título XIII, Capítulo VII, arts. 412 – 414), el de 1850 (en su Título XIII, Capítulo VII, arts. 422 – 424), el de 1870 (en su Título XII, Capítulo VII, arts. 512 – 514), el de 1928 (Título XIII, Capítulo IV, arts. 683 – 686), el de 1932 (Título XIII, Capítulo VI, art. 490) y, por último, el de 1973 (Título XIII, Capítulo VI, arts. 497 – 499). El objeto material del delito supuso la principal variación en las conductas tipificadas como delito dependiendo de la época. Hay que recalcar que, en lo que concierne a la intimidad personal, el CP de 1973 solo tipificaba conductas referidas al secreto de las comunicaciones (arts. 192, 497, 498, 360, 367 y 368) y la inviolabilidad del domicilio (arts. 191, 490 y sucesivos), dependiendo la protección penal de la imagen de la protección del derecho al honor mediante las calumnias (art. 453) y las injurias (art. 457).

320 Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos,* p. 21.

importante novedad fue la protección no solo de la intimidad, sino de los datos de carácter personal. Hay que destacar que la rúbrica que actualmente identifica al mencionado Capítulo I ha permanecido prácticamente inalterada desde el siglo XIX hasta la actualidad, si bien continúa haciendo alusión a la acción punible en lugar de al bien jurídico protegido: la intimidad. Ésta, por su parte, preside la denominación actual del Título X[321].

Las modificaciones posteriores del CP en este ámbito respondieron a la necesidad de adaptarlo a la normativa internacional[322]. No obstante, la forma en la que el legislador español abordó esta tarea fue objeto de importantes críticas por parte de la doctrina, que consideró que se había arruinado la claridad sistemática de la redacción de 1995, y señaló los futuros problemas que plantearían aspectos como la incriminación de actos preparatorios, difíciles de delimitar en la esfera del desvalor de lo injusto. En definitiva, se trató de una valoración desoladora que evidenciaba el desprecio del legislador a valores tan innegociables como la seguridad jurídica. El análisis doctrinal de los nuevos preceptos fue también negativo, y se criticó la ausencia, una vez más, de la Sección Penal de la Comisión General de Codificación, que tampoco intervino en el desarrollo del CP de 1995, así como la intervención en su lugar de grupos de expertos escogidos *ad hoc* por el Ministro de Justicia. Las críticas se extendieron también al legislador comunitario, a quien se achacó, junto al legislador nacional, la culpa por la falta de un criterio sistemático claro, así como el caos al que se enfrentan los intérpretes cuando intentan realizar un análisis de manera organizada[323]. Hay que destacar, pues, esta idea fundamental: la ordenación actual de estos delitos resulta caótica, al menos en lo que respecta al art. 197 y sucesivos del

[321] Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos,* pp. 22 – 24.

[322] F. Almenar Pineda, *El delito de hacking,* 1ª ed., Cizur Menor, Navarra, Aranzadi, 2018, p. 69. En efecto, el preámbulo de la LO 5/2010 hacía referencia a la cumplimentación de la Decisión Marco 2005/222/JAI, y la LO 1/2015 contaba entre sus objetivos el de ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea a través de la transposición al derecho español de la Directiva 2013/40/UE.

[323] Almenar Pineda, *El delito de hacking,* pp. 78 – 79.

CP, siendo necesaria una reestructuración de los mismos de acuerdo a un criterio adecuado y solvente.

Qué mejor prueba del caos mencionado que el hecho de que, a pesar de la pretensión de recoger estos delitos en el Capítulo I (dedicado al descubrimiento y revelación de secretos) del Título X (delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio) del Libro II del CP, no todos los delitos que afectan a la intimidad y al deber de secreto figuran en él, encontrándose dispersos en distintas partes de dicho texto legal. Es el caso de los arts. 413 y sucesivos, dedicados a la infidelidad en la custodia de documentos y a la violación de secretos cuando son cometidos por funcionarios públicos.

Aunque la regulación de estos delitos en el CP de 1995 supuso una novedad necesaria y, en líneas generales, acertada, persisten en la actualidad aspectos censurables o dudosos en relación con la misma, como la redacción del tipo relativo a los comportamientos de apoderamiento del art. 197.1, primer inciso, que responde a concepciones ya superadas; resulta confuso el tipo básico relativo a la protección de datos reservados de carácter personal del art. 197.2, sobre todo en lo concerniente al contenido de cada uno de los dos tipos introducidos y a la manera en que se relacionan entre sí; también resulta dudosa la tipificación de conductas como la modificación o alteración de datos reservados, por sobrepasar el ámbito de la intimidad; son notables las lagunas terminológicas entre el CP y la antigua LOPD, que fomentan aún más la confusión existente; y, sobre todo, hay que destacar la configuración de tipos agravados en cadena, que se traducen en penas muy elevadas y un marco punitivo demasiado amplio. Por tanto, no solo el caos, sino también el permanente riesgo de obsolescencia son ideas fundamentales en relación con la vulneración de la intimidad por medios tecnológicos, ya que la continua aparición de nuevas formas de delinquir pone en riesgo la eficacia del instrumento penal.

Aunque la redacción de los artículos analizados, cuya mayor parte se introdujo con el CP de 1995, supone una indudable mejora respecto al

contenido del CP del año 1973, y a pesar de las modificaciones introducidas por la LO 1/2015, se han perpetuado muchos de los defectos que fueron señalados[324] hace ya casi veinte años. Sigue sin haber armonía terminológica y conceptual entre el CP y el RGPD, incluso a pesar de la novedad de este último, continúa abusándose de los tipos agravados en cadena o cascada hasta niveles que, en ocasiones, pueden ocasionar confusión en su interpretación y, sobre todo, sigue sin existir un tipo específico que prevea los accesos ilegítimos sin importar el propósito del autor.

Y es que, en lo que respecta de manera específica al 197 bis, el acceso no autorizado a datos o programas informáticos fue una de las mayores novedades de la LO 5/2010, que introdujo su contenido numerándolo nada menos que como art. 197.3 del CP. La LO 1/2015 no tardó en modificar su redacción y su ubicación, adaptando la legislación penal española al art. 2 de la ya mencionada Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, y al Convenio sobre la Ciberdelincuencia de Budapest, de 23 de noviembre de 2001, que en su art. 2 incluía un delito de similar factura. No obstante, el legislador cometió, una vez más, un error en lo concerniente a su ubicación, toda vez que la misma plantea numerosos problemas interpretativos, y hubiera sido conveniente una más atenta reflexión en este sentido[325]. Ya he comentado que considero este art. 197 bis del CP solo como un eslabón en la cadena que conduce a la creación de un delito autónomo de intrusión en un sistema de información, puesto que, en su ubicación actual, a mi juicio inadecuada, su utilidad se ve limitada por su alejamiento respecto de la protección de dichos sistemas y su vínculo exclusivo con los dos bienes jurídicos mencionados: la intimidad y los datos reservados de carácter personal[326].

---

[324] C.M. Romeo Casabona, “La protección penal de la intimidad y de los datos personales en sistemas informáticos y en redes telemáticas (Internet)”, *Estudios jurídicos. Ministerio Fiscal,* 2001, pp. 309 – 310.

[325] Romeo Casabona, *Derecho Penal, Parte Especial*, pp. 282 – 283.

[326] S. Cámara Arroyo et al., *Cibercriminalidad*, 1ª ed., Madrid, Dykinson, 2019, pp. 198 – 199.

3.3.2.1.4.2 Más allá de la intimidad y de los datos reservados de carácter personal como bienes jurídicos protegidos

El bien jurídico protegido[327] fue la novedad más destacada que incorporó el legislador en su reforma de 1995 del CP en relación con los delitos de descubrimiento y revelación de secretos. A raíz de ésta, se introdujeron otras novedades relativas a su sistematización. Fue la primera vez que la intimidad figuró de manera explícita en una rúbrica del CP como bien jurídico protegido. Con anterioridad, solo se había hecho alusión a la intimidad en el art. 497 bis del texto refundido del CP del año 1973. Tras la reforma, la intimidad se convirtió en el elemento común y en el eje rector e identificador de buena parte de estos delitos.

De este modo, el legislador, notablemente influenciado por el art. 18 de la CE de 1978, que proclamaba la intimidad como derecho fundamental, reconoció, aunque de manera tardía, su peso específico como bien jurídico objeto de protección penal[328].

Con independencia de la influencia de otros textos legales sobre el CP, delimitar un bien jurídico protegido como la intimidad resulta complejo toda vez que, a juicio de la doctrina[329], es un concepto impreciso y en constante evolución. Se trata de la intimidad personal o familiar entendida en sentido amplio (incluyendo, por lo tanto, la propia imagen). A este bien jurídico hay que añadir los datos reservados de carácter personal o familiar, cuyo concepto y contenido también evolucionan de manera continua. Ya hace más de diez años, la doctrina[330] planteó la posibilidad, en atención a la expansión de la comunicación por vías telemáticas, de reflexionar sobre la oportunidad

---

[327] C.M. Romeo Casabona, "Los datos de carácter personal como bienes jurídicos penalmente protegidos", en C.M. Romeo Casabona (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Granada, Comares, 2006, pp. 167 – 190. El CP de 1944 fue reformado en varias ocasiones con el paso del tiempo, como evidencian las publicaciones del texto revisado de 1963 y del texto refundido de 1973, haciéndose en este último referencia a la intimidad por primera vez en su art. 497 bis.

[328] Romeo Casabona, *El cibercrimen*, p. 167.

[329] Romeo Casabona, *El cibercrimen*, p. 169.

[330] Romeo Casabona, *El cibercrimen*, p. 170.

de establecer una protección más amplia y específica de las mismas con objeto de garantizar que pudiesen llevarse a cabo pacíficamente. ¿Podría ser la ciberseguridad un bien jurídico autónomo que mereciese ser protegido junto a la intimidad y los datos reservados de carácter personal o familiar?

La única manera de responder a esta pregunta es un análisis de cada uno de los bienes jurídicos protegidos admitidos como tales, tratando de trasladar después sus características a la ciberseguridad para determinar si esta reúne los requisitos necesarios.

El concepto del derecho a la intimidad data del año 1891, cuando comenzó a protegerse el reducto vital privado en el que se desenvuelven algunas de las actividades más vinculadas a la naturaleza del ser humano[331]; desde sus creencias hasta atributos como los relativos a su salud. La persona tenía, gracias al mismo, derecho a excluir a los demás de las distintas manifestaciones de ese ámbito vital, tanto en relación con sus actividades como en lo referente a objetos físicos, como las bases de datos. Así, el derecho a la intimidad garantizaba el derecho de toda persona a ser dejada en paz[332]. Nadie, a excepción de quien contase con la debida autorización, podía penetrar en ese reducto personal llamado intimidad. He aquí la definición perfecta, en mi opinión, del derecho a la intimidad, porque blinda a la persona frente a las injerencias externas y permite que construya su vida de manera autónoma, libre y plena. Esto adquiere especial importancia en tiempos como los nuestros, en los que el Estado se muestra más y más

[331] F. Ruiz Marco, *Los delitos contra la intimidad: especial referencia a los ataques cometidos a través de la informática,* 1ª ed., Madrid, Colex, 2001, pp. 45 – 46. En 1891, los juristas estadounidenses Samuel Warren y Louis Brandeis acuñaron la definición del derecho a la intimidad: derecho de toda persona a ser dejada en paz. En 1967, Alan Westin añadió que es la capacidad de individuos, grupos o instituciones para decidir por sí mismos cuándo, cómo y hasta qué punto desean comunicar información propia a los demás.

[332] S. Warren y L. Brandeis, "The Right to Privacy", *Harvard Law Review,* vol. IV, no. 5, 1890, pp. 193 - 220, citado en C.M. Romeo Casabona, "Los datos de carácter personal como bienes jurídicos penalmente protegidos", en C.M. Romeo Casabona (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Granada, Comares, 2006, p. 173. En la página 219 de su artículo, Warren y Brandeis sostuvieron que, indudablemente, sería deseable la protección adicional del Derecho penal para garantizar la intimidad de las personas. Para ello hicieron referencia, incluso, a un pequeño bosquejo legal.

omnipresente e intruso a causa de su progresiva y cada vez más desmedida tendencia al escrutinio, la dominación y el control.

La evolución de la intimidad como bien jurídico protegido es, sin embargo, un hecho para la doctrina[333], que la considera inmersa en un constante e inacabado proceso evolutivo. No resultaría posible, por lo tanto, construir un retrato definitivo de la misma. Y es que, en las últimas décadas, la preocupación por la protección jurídica de la intimidad ha aumentado a causa de la multiplicación y mayor potencialidad de los procedimientos con capacidad para vulnerarla, como los medios técnicos de captación y transmisión de la imagen y del sonido, o los de acumulación y procesamiento de la información en general y de los datos de carácter personal en particular. Siendo el desarrollo tecnológico en este ámbito relativamente reciente, no existió la necesidad de delimitar el concepto del objeto de tutela hasta hace pocos años, cuando se hizo evidente la importancia de tratar de establecer un procedimiento de protección adecuado. Además, el reducto de la esfera íntima se ha visto reducido a causa de la manera en que la sociedad moderna concibe las relaciones sociales y del mayor intervencionismo estatal orientado, en teoría, a prestar sus servicios de la forma más eficaz posible[334]. En el derecho español, el art. 18 de la CE de 1978 constituye la base del reconocimiento de la intimidad como derecho fundamental, posteriormente apuntalada por las decisiones del TC que enumeraré a continuación, que fueron jalonando una sucesión de hitos decisivos en relación con su contenido y extensión. Al principio, se configuró como un derecho garantista o de defensa muy cercano a la definición tradicional, de manera que la intimidad se consideraba como un reducto restringido de la persona vedado al acceso por parte de otros. El ejercicio del derecho fundamental implicaba una vertiente exclusivamente negativa, pudiendo exigir su titular la no injerencia en su vida privada, y nada más[335].

[333] Romeo Casabona, *El cibercrimen*, p. 170.
[334] Romeo Casabona, *El cibercrimen*, p. 171.
[335] Romeo Casabona, *El cibercrimen*, p. 173.

Diecisiete años separan la STC 73/1982, de 2 de diciembre, de la STC 134/1999, de 15 de julio[336], en la cual se avanzó frente a la perspectiva tradicional representada por la primera y se reconoció que la intimidad también abarcaba un poder de control sobre la publicación de la información relativa a la persona y su familia. Es necesario matizar que, en ambos casos, el contenido del derecho fundamental se relacionó con el conocimiento de espacios de la vida privada de la persona, mientras que la concepción estadounidense de 1891 se traducía en facultades de decisión y de acción del individuo en la esfera privada que podían permanecer ajenas a cualquier intromisión o limitación por parte de terceros[337]. Así, desde esta perspectiva más amplia, se puede entender por intimidad aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento o desarrollo quedan reservados a su titular o sobre las que ejerce alguna forma de control cuando se ven implicados terceros, entendiendo por tales tanto los particulares como los poderes públicos. Por lo tanto, el derecho a la intimidad conlleva también el reconocimiento de una reserva o control sobre terceros. Cuando el sujeto pasivo no disponga de ningún mecanismo legítimo de control sobre terceros, la manifestación de la personalidad afectada habrá salido de su esfera íntima y, en ese caso, su protección solo será posible en tanto en cuanto afecte a la propia imagen o al honor, por encontrarse ambos muy vinculados con la misma[338].

Hay que distinguir, por último, la intimidad de la privacidad, puesto que la segunda abarca un conjunto más amplio de facetas de la personalidad que, consideradas aisladamente, no tienen un significado intrínseco, pero que, enlazadas entre sí de manera coherente, permiten construir un retrato de la personalidad del individuo que este tiene derecho a mantener reservado. El legislador español ha excluido esta manifestación[339].

---

[336] ECLI:ES:TC:1999:134.

[337] Romeo Casabona, *El cibercrimen*, p. 174.

[338] Romeo Casabona, *El cibercrimen*, p. 175.

[339] Romeo Casabona, *El cibercrimen*, p. 176.

A partir de lo anterior, y a pesar de su carácter relativo y difuso, resulta posible perfilar la intimidad como bien jurídico-penalmente protegido a través de tres cauces: la intimidad como reducto de la manifestación de la personalidad en la vida privada, en su manifestación de confidencialidad compartida y en relación con el procesamiento y comunicación de datos a través de las modernas tecnologías de la información y de la comunicación. El primero[340] se refiere al ámbito de la intimidad reservado directa y exclusivamente a la esfera del propio interesado o de su familia, si bien la intimidad familiar no ha merecido, como tal, una consideración penal explícita: su protección se alcanza a través del reconocimiento de la titularidad individual del derecho a la intimidad personal de cada miembro de la familia. Así, es la persona la que, dentro de ciertos límites, decide sobre la extensión del ámbito protegido. Se tratar de proteger tanto ciertas manifestaciones del secreto por ser las mismas reservadas, como de establecer una restricción frente a medios de captación artificial que intervengan aquello que, sin ser específicamente secreto, forma parte de la intimidad, como las conversaciones. Se protege el espacio físico o continente del ejercicio o disfrute de la intimidad, incluso cuando su creación ha requerido artificios técnicos. Aunque se incluyen las modernas tecnologías de comunicación y de almacenamiento del sonido y de la imagen, domina la concepción tradicional de la intimidad, de manera que se pretende proteger frente a injerencias indebidas, no consentidas, los reductos de la intimidad exclusivos o compartidos con un número reducido de personas. La intimidad se concibe, como bien jurídico protegido, como presupuesto para el disfrute de otros bienes jurídicos protegidos.

El segundo[341] de los tres cauces mencionados es la intimidad en su manifestación de confidencialidad compartida, ámbito en el que se encuadran los aspectos de la intimidad que, por imperativo legal, o por la naturaleza de las relaciones sociales o entre particulares permiten el acceso a terceros, obligándolos, no obstante, a un deber de respetar la confidencialidad. Esto

[340] Romeo Casabona, *El cibercrimen*, p. 177.

[341] Romeo Casabona, *El cibercrimen*, p. 178.

conlleva que ciertos trabajadores, profesionales y autoridades y funcionarios públicos deben cumplir con un deber de secreto, pudiendo exigírselo la persona afectada en caso contrario para lograr la protección efectiva de esta manifestación de la intimidad. Hay que destacar el caso de los profesionales sanitarios, para quienes la confidencialidad supone uno de los pilares fundamentales de la relación médico-paciente.

El tercero[342] y último de los cauces es la intimidad en relación con el procesamiento y comunicación de datos a través de las modernas tecnologías de la información y de la comunicación, en el cual, aunque es posible encontrar alguno de los aspectos de los anteriores, el alcance de la intimidad se centra en la obligación del afectado de aportar información personal privada o reservada que puede revestir un carácter íntimo. También se encuadra en esta categoría el archivo o procesamiento por terceros de esta clase de información, incluso cuando no ha sido suministrada por el afectado, si bien en estos casos se le reconoce una cierta capacidad de control y disposición sobre la misma. Entender la naturaleza de estos datos de carácter personal resulta esencial, toda vez que presentan unas características muy diferentes de las de la intimidad, de manera que fueron objeto de un continuo desarrollo legislativo y doctrinal por parte del TC que se tradujo en el reconocimiento de un derecho fundamental distinto a la intimidad y, a su vez, en la posibilidad de configurar un bien jurídico autónomo de la intimidad en el ámbito penal.

En cuanto a los datos de carácter personal reservados, el art. 18.4 de la CE sostiene que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos, así como el pleno ejercicio de sus derechos. Se reconoce así la capacidad de la informática para vulnerar de forma especial el derecho fundamental a la intimidad y, al mismo tiempo, su potencialidad para afectar a otros derechos cuyo ejercicio también debe garantizarse plenamente[343]. Este art. 18.4 de la CE adquirirá

[342] Romeo Casabona, *El cibercrimen*, pp. 178 – 179.

[343] Romeo Casabona, *El cibercrimen*, p. 179.

posteriormente en esta investigación una importancia trascendental en relación con la ciberseguridad.

Del conjunto de dicho artículo, el TC extrajo el derecho fundamental a la protección de datos personales, sean o no objeto de tratamiento informático o automatizado. No puede entenderse la consideración de los datos personales como bien jurídico penalmente protegido sin un análisis previo desde una perspectiva constitucional. El punto de partida es la idea de que el derecho a la intimidad, por sí mismo, no es suficiente para proteger algunas de sus manifestaciones vinculadas con las nuevas tecnologías y con el tratamiento de datos personales a través de las mismas[344]. En consecuencia, es a través de la libertad informática, el haz de facultades positivas en relación con el control de sus propios datos personales, como el individuo ve reconocida una mayor capacidad de control sobre la información que le concierne. Construida a partir del derecho a la autodeterminación informativa, quedan amparados por el derecho a la libertad informática aquellos datos personales sometidos a procesamiento por sistemas informáticos, tengan o no carácter íntimo[345]. La jurisprudencia vinculó por primera vez la libertad informática con el art. 18.4 de la CE en la STC 254/1993, de 20 de julio, y después en las SsTC 143/1994, de 9 de mayo, 233/1999, de 13 de diciembre, y 2929/2000, de 30 de noviembre. Por su parte, el TS también aceptó esta vinculación en la STS de 18 de febrero de 1999, remarcando la influencia de este artículo de la CE sobre la misma en su STS 553/2015, de 6 de octubre[346]. Las sentencias más importantes, no obstante, son aquellas en que se eleva la protección de los datos de carácter personal a la máxima categoría jurídica y se proclama el nuevo derecho fundamental orientado a su protección. Así,

[344] Romeo Casabona, *El cibercrimen*, p. 180.

[345] Romeo Casabona, *El cibercrimen*, pp. 180 – 182. La identidad informática, pese a ser un interés objeto de tutela que también puede englobarse dentro del derecho a la libertad informática, tiene un sentido más preciso. Es el derecho a que los datos de un individuo reflejen efectiva y realmente la información que le concierne de forma veraz y exacta. De aquí se deriva un derecho a exigir que se rectifiquen o cancelen aquellos datos personales que, ya sea por accidente o de manera intencionada, se han introducido o modificado incorrectamente, puesto que los mismos no corresponden de forma veraz al perfil del afectado.

[346] ECLI:ES:TS:2015:4054.

en el fundamento jurídico séptimo de la STC 290/2000, de 30 de noviembre, se materializa ese reconocimiento de manera explícita, refiriéndose a este derecho tanto como derecho fundamental a la protección de datos personales frente a la informática como libertad informática, remitiendo, en este último caso, a la STC 254/1993[347].

El TC también detalla el contenido de este derecho fundamental en el fundamento jurídico séptimo de su sentencia 292/2000, de 30 de noviembre, definiéndolo como un poder de disposición y de control sobre los datos personales que faculta al individuo para decidir cuáles de esos datos desea proporcionar a un tercero, ya se trate del Estado o de un particular. También le otorga poder de decisión sobre qué datos puede recabar ese tercero, para averiguar quién posee sus datos personales y para qué, y para oponerse a su posesión o uso. Se trata, por lo tanto, de un poder de disposición y control sobre los datos personales que se concreta jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, así como su posterior almacenamiento y tratamiento y su uso o sus posibles por parte de un tercero, se trate del Estado o de un particular. No se limita al titular del fichero, sino que alcanza también a los posibles cesionarios, a quienes es posible requerirles que rectifiquen o cancelen los datos obtenidos a través del primero[348].

Aunque la libertad informática mantiene su razón de ser, solo es así en relación con determinados datos personales. Hay que acudir al derecho fundamental a la protección de los datos personales para la defensa no solo de datos personales procesados o almacenados por sistemas informáticos, sino para la protección de cualesquiera otros datos personales. Su objeto de protección no se reduce a los datos íntimos, sino que abarca cualquier tipo de dato personal, íntimo o no, cuyo conocimiento o empleo por parte de

[347] A. Galán Muñoz, "¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación", en A. Galán Muñoz (coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*, 1ª ed., Valencia, Tirant lo Blanch, 2014, pp. 210 – 211.

[348] Romeo Casabona, *El cibercrimen*, p. 183.

terceros pueda afectar a los derechos de la persona, sin importar si son o no derechos fundamentales. Así, su objeto no es únicamente la intimidad individual, sino los datos de carácter personal en sentido más amplio alcanzando, incluso, a ciertos datos personales públicos que no por el hecho de ser accesibles al conocimiento de cualquiera escapan al poder de disposición del afectado. En definitiva, esto se traduce en la protección de todos los datos que identifiquen o permitan la identificación de la persona y puedan servir para confeccionar un perfil de cualquier índole, e incluso de los datos que sirvan para cualquier otra utilidad y que, con el tratamiento adecuado, constituyan una amenaza para el individuo.

El ejercicio de este derecho se sustenta sobre un conjunto de facultades positivas en relación con la disposición y control sobre los datos personales que va más allá de la protección de la intimidad, puesto que se concretan en el derecho a consentir y a conocer su posesión y su uso por parte de terceros, así como a estar informado sobre los mismos y a oponerse a su uso. A través de los derechos de rectificación y de cancelación, que forman parte de las mencionadas facultades positivas, el individuo puede garantizar también la exactitud y pertinencia de sus datos, lo cual demuestra el contenido práctico de las mismas.

El TC, por lo tanto, desgajó la protección de los datos personales de la noción de intimidad, aunque ello no implicó una desconexión absoluta entre ambos derechos, toda vez que su estrecha relación resulta innegable. Del mismo modo, garantizó esta protección para datos que no fuesen íntimos y para los que no estuviesen sometidos a un procesamiento informático[349]. Esto contrasta con la ciberseguridad, la cual, por su propia definición, busca únicamente la seguridad de datos que, siendo íntimos o no, hayan sido informatizados.

La lectura constitucional de los datos de carácter personal facilita la delimitación de un bien jurídico protegido en relación con los mismos. El bien jurídico son los datos personales, pero es esencial introducir una matización:

[349] Romeo Casabona, *El cibercrimen*, pp. 184 – 185.

el Derecho penal no les otorga la misma amplitud que el TC, sino que selecciona solo los aspectos más relevantes que merezcan protección penal de acuerdo con el criterio político-criminal que el legislador adopte en un momento determinado. En consecuencia, resulta imperativo especificar que, en la versión del CP de 1995, el legislador estableció como bien jurídico protegido los datos reservados de carácter personal o familiar de otro. Idéntica expresión se recoge en el actual art. 197.2 del CP, pese a las modificaciones introducidas por la LO 1/2015, de 30 de marzo, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal. Como consecuencia de los principios de mínima intervención y *ultima ratio* del Derecho penal, no se pretende proteger todos los datos personales, sino únicamente aquellos reservados, que pertenezcan a un tercero, y que tengan carácter personal o familiar. Quedan excluidos del amparo del Derecho penal los datos públicos, los datos propios, y aquellos que carezcan del citado carácter personal o familiar. Aunque el Título X del CP recoge, entre otros, los delitos contra la intimidad[350] [351], dando relevancia a la intimidad como bien jurídico genérico, el tipo delictivo del art. 197.2 se refiere a datos reservados, no íntimos, de manera que pueden perseguirse a través del mismo conductas que atenten contra datos que tengan el carácter de reservados sin necesidad de que puedan catalogarse también como íntimos[352].

Solo tras un análisis en profundidad de los bienes jurídicos protegidos por los arts. 197 y sucesivos del CP, es decir, la intimidad y los datos reservados de carácter personal, es posible entender que, específicamente en el art. 197 bis 1 del mismo texto legal, la naturaleza y el contenido del bien jurídico protegido no solo están desdibujados, sino que resultan discutibles. Y es que el tipo se refiere al acceso a sistemas de información, pero no

[350] G. E. Aboso, "Delitos contra la intimidad y la privacidad: acceso indebido a comunicaciones electrónicas, datos sensibles y sistemas informáticos", *Revista de Derecho Penal y Criminología,* no. 7, 2017, p. 3.

[351] E. Orts Berenguer y M. Roig Torres, *Delitos informáticos y delitos comunes cometidos a través de la informática,* Valencia, Tirant lo Blanch, 2001, p. 13. Las nuevas tecnologías informáticas están dotadas de una extraordinaria capacidad lesiva que no ha pasado desapercibida para el legislador en el ámbito penal.

[352] Romeo Casabona, *El cibercrimen*, pp. 186 – 187.

especifica que deban ser reservados. Así, su ubicación parece errónea, puesto que el bien jurídico va más allá del que se pretende proteger en estos delitos. De hecho, la pérdida de nitidez de los sistemas de información que se pretenden proteger no hace sino reforzar la idea de que el bien jurídico protegido es, en realidad, la seguridad de los sistemas informáticos. La Decisión Marco 2005/222/JAI se refiere a ataques contra los sistemas de información, y también lo hace la LO 1/2015[353], lo que debilita la consideración de que la intimidad o los datos personales son los bienes jurídicos protegidos y refuerza la tesis que defiende que el auténtico bien jurídico protegido por este delito es, en realidad, la seguridad de los sistemas. En este mismo sentido se pronuncia la STS 494/2020, de 8 de octubre[354].

De la misma opinión es la Fiscalía General del Estado española, que en su Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos[355] [356], sostiene, en relación con el delito del art. 197 bis 1, que su reubicación sistemática deja constancia de que el bien jurídico protegido en el mismo no es directamente la intimidad personal, sino la seguridad de los sistemas de información en cuanto medida de protección del ámbito de privacidad reservado a la posibilidad de conocimiento público y, sobre el tipo penal del art. 197 bis 2, que su ubicación junto al acceso ilegal a sistemas informáticos es coherente con la voluntad del legislador de separar la tipificación y sanción de las conductas que tutelan la privacidad protegiendo la seguridad de los sistemas de aquellas otras en la que el bien jurídico protegido es directamente

[353] Romeo Casabona, *Derecho Penal, Parte Especial*, p. 283.

[354] ECLI:ES:TS:2020:3215.

[355] Fiscalía General del Estado, *Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos*, Madrid, Fiscalía General del Estado, 2017, p. 33.

[356] C. Obispo Triana, "Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos", *Revista Aranzadi Doctrinal*, no. 10, 2017, p. 183. Según la página tercera de la Circular 3/2017, se tipifica de forma separada y diferenciada el mero acceso a los sistemas informáticos.

la intimidad de las personas. No cabe duda de que la ubicación de este delito no es, en absoluto, adecuada, toda vez que una interpretación objetiva de la voluntad de la ley podría conllevar una restricción sobre su alcance, quedando excluidos del tipo accesos con capacidad para poner en peligro bienes jurídicos de diferente naturaleza[357].

Se hace imperativo, en consecuencia, su traslado a un título independiente que incorpore, donde resulte apropiado, otros delitos relacionados con las TIC cuya ubicación también sea desacertada por razones similares. Por último, me adhiero a la línea de pensamiento que desecha el concepto de domicilio informático[358], el cual, quizá, pudo haber tenido sentido en una fase muy anterior del desarrollo de la tecnología informática, pero que ha quedado completamente obsoleto y resulta inadecuado para referirse a avances como la computación en la nube, que se basan en una independencia casi total entre los dispositivos propios y la ubicación de la información. Resultaría muy difícil de justificar desde la perspectiva del Derecho penal la protección de un supuesto domicilio informático en relación con tecnologías que son independientes en gran medida del sujeto afectado por el delito.

3.3.2.1.4.3 La actual redacción del tipo delictivo del artículo 197 bis 1 del Código Penal

El delito del art. 197 bis 1 del CP tiene como objeto material un sistema de información. De acuerdo al art. 1, párrafo a, de la Decisión Marco 2005/222/JAI, entra dentro de dicha categoría 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 estos últimos para su funcionamiento, utilización, protección y mantenimiento. Dentro del tipo objetivo, la conducta

[357] Romeo Casabona, *Derecho Penal, Parte Especial*, p. 284.
[358] Romeo Casabona, *Derecho Penal, Parte Especial*, p. 283.

típica es doble y presenta un carácter alternativo, siendo suficiente la realización de una u otra: la primera es el acceso[359] al conjunto o a una parte[360] de un sistema de información o la facilitación de dicho acceso a un tercero, quien deberá lograr acceder para que se consume del delito; la segunda consiste en mantenerse en un sistema de información o en parte del mismo en contra de la voluntad de quien ostente el legítimo derecho a la exclusión, siendo una conducta omisiva que sucede cuando o bien el sujeto activo se introduce en el sistema de manera casual, o bien accede de manera legítima, pero la autorización otorgada le es retirada con posterioridad[361]. Si además de denegar el permiso para permanecer en el sistema de información o en parte del mismo quien ostente el legítimo derecho a la exclusión adopta medidas adicionales, como la modificación de las claves que hacen posible el acceso, cualquier nueva entrada debería incardinarse dentro de la primera de las dos modalidades típicas analizadas[362].

En cuanto al acceso al conjunto o a una parte de un sistema de información, no será necesario que el ciberdelincuente llegue a tener el dominio efectivo de alguno de los anteriores para poder considerar consumado este delito, sino que bastará con que tenga contacto con los datos o con el *software* contenidos en ellos. Existen, no obstante, partes del sistema que no contienen datos ni programas, pero a cuyas BIOS se puede acceder: es decir, el ciberdelincuente puede acceder también al *firmware* preinstalado

[359] Almenar Pineda, *El delito de hacking,* pp. 172 – 173. La amplitud que posee el término *acceso* permite que tengan cabida conductas típicas muy distintas, incluyendo tanto los accesos realizados utilizando la red interna de una empresa como los remotos a través de Internet. No obstante, es importante introducir un matiz fundamental en este sentido: la diferencia entre identificación y autenticación. De acuerdo al IBM Knowledge Center, la identificación es la capacidad de identificar de forma exclusiva a un usuario de un sistema o de una aplicación que se está ejecutando en el sistema, mientras que la autenticación es la capacidad de demostrar que un usuario o una aplicación es realmente quien asegura ser. Cuando un usuario se conecta a un sistema especificando su ID de usuario y contraseña, el sistema utiliza dicho ID de usuario para identificarle, pero la autenticación solo se produce en el momento de la conexión, cuando el sistema comprueba que la contraseña proporcionada es correcta por corresponder a dicho ID de usuario.

[360] F. Almenar Pineda, *Ciberdelincuencia. Teoría y práctica*, 1ª ed., Porto, Juruá Editorial, 2018, p. 151.

[361] Romeo Casabona, *Derecho Penal, Parte Especial*, pp. 284 – 285.

[362] Muñoz Conde, *Derecho Penal, Parte Especial*, p. 282.

en todo aparato digital que inicia y determina la manera en que debe funcionar un elemento en particular del mismo. Eso, en lo que concierne al *software*.

El *hardware* solo podrá considerarse parte de un sistema de información si trata de forma automatizada datos informáticos (como el ordenador que ejecuta el procesamiento) o si, como mínimo, está conectado con otros componentes que realicen dicho tratamiento (como un sistema de almacenamiento ideado para guardar datos que todavía está vacío, pero que ya se encuentra conectado al ordenador que los trata), de manera que no será posible que sufran accesos ilícitos los elementos físicos que no cumplan al menos una de estas dos características[363] [364].

[363] A. Galán Muñoz, *Los ciberdelitos en el ordenamiento español*, 1ª ed., Barcelona, Editorial UOC, 2019, pp. 109 – 116. Galán Muñoz cuestiona también la delimitación del bien jurídico protegido por el art. 197 bis 1 del CP en su actual ubicación para analizar después su posible desvinculación completa de la intimidad y su vinculación en exclusiva a otro bien jurídico distinto: la seguridad de los sistemas informáticos. Comparte esta opinión (si bien, siguiendo a Carrasco Andrino, extiende el bien jurídico también a la seguridad de las redes, y no solo de los sistemas informáticos) F. Morales Prats, "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en G. Quintero Olivares (dir.), *Comentarios a la Parte Especial del Derecho* Penal, 10ª ed., Cizur Menor, Navarra, Aranzadi, 2016, p. 471. También se muestra a favor de considerar como bien jurídico protegido la seguridad de los sistemas informáticos, en cuanto presupuesto imprescindible para que la informática pueda desempeñar su crucial papel en nuestra sociedad, como en la protección de infraestructuras críticas, C. Tomás-Valiente Lanuza, "Artículo 197 bis", en M. Gómez Tomillo (dir.), *Comentarios prácticos al Código Penal. Tomo II. Los delitos contra las personas. Artículos 138 – 233*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, pp. 674 – 675. Menciona directamente como bien jurídico la ciberseguridad de los sistemas y de las redes informáticos J. López-Muñoz, *Cibercriminalidad e investigación tecnológica*, 1ª ed., Madrid, Dykinson, 2020, p. 59. Al igual que sucede con Galán Muñoz, también está a favor de considerar el bien jurídico de este delito la seguridad de los sistemas informáticos C. Bolea Bardón, "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en M. Corcoy Bidasolo y S. Mir Puig (dirs.), *Comentarios al Código Penal. Reforma LO 1/2015 y LO 2/2015*, 1ª ed., Valencia, Tirant lo Blanch, 2015, p. 746. J.E. Sáinz-Cantero Caparrós, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I)", en L. Morillas Cueva (dir.), *Sistema de Derecho Penal. Parte Especial*, 4ª ed., Madrid, Dykinson, 2021, pp. 361 – 362, destaca que para Castelló Nicas el bien jurídico tutelado es no solo la seguridad del medio informático, sino también la confidencialidad de la información que los sistemas de información contienen. En último lugar, una corriente minoritaria: el bien jurídico protegido por este art. 197 bis 1 es la seguridad en el tráfico informático para C. Suárez-Mira Rodríguez, A. Judel Prieto, y J.R. Piñol Rodríguez, *Manual de Derecho Penal. Parte Especial. Tomo II,* 8ª ed., Cizur Menor, Navarra, Aranzadi, 2020, p. 299.

[364] M.D.M. Carrasco Andrino y M.D.M. Moya Fuentes, "La ciberdelincuencia dentro de la estrategia de seguridad nacional. Especial referencia a las conductas de introducción en el sistema informático", en J.M. Canales Aliende y A. Romero Tarín (eds.), *La seguridad de los Estados en el contexto de las incertidumbres: una visión poliédrica*, 1ª

El art. 3 de la Directiva 2013/40/UE no exigía que se castigase la conducta consistente en facilitar a otro del acceso al conjunto o a una parte de un sistema de información, aspecto que evitaba reiteraciones al contar nuestro ordenamiento jurídico-penal con herramientas suficientes para apreciar las diferentes formas de participación en el delito gracias a los arts. 28 y siguientes del CP. Al incluir esta modalidad comisiva, se convierte en delito autónomo la conducta del facilitador del acceso con objeto de garantizar que sea castigado como autor, sin importar si dicho acceso facilitado a un tercero llega o no a producirse[365]. Esta facilitación del acceso debe ir más allá del mero favorecimiento, debiendo suponer el otorgamiento de la posibilidad de acceder directamente y sin más al sistema, por ejemplo, inhabilitando de forma efectiva las medidas de seguridad, debiendo ser el objetivo de quien lleva a cabo esta conducta que un tercero complete con posterioridad un acceso ilícito. Esto, con independencia de que, finalmente, el acceso llegue o no a realizarse[366].

Solo son punibles los hechos que suponen la vulneración de las medidas de seguridad establecidas para impedir el acceso[367] [368] [369], o la

ed., Cizur Menor, Navarra, Aranzadi, 2021, p. 299. En un punto intermedio, por componerse tanto de *software* como de *hardware*, está el rúter que hace posible la conexión wifi, y que al estar conectado con los distintos dispositivos electrónicos se puede considerar parte del sistema informático. Solo es posible acceder al mismo tras vulnerar su contraseña, momento en el cual el ciberdelincuente tendrá acceso, al menos, a los datos no codificados que están siendo enviados y recibidos.

[365] Galán Muñoz, *Los ciberdelitos en el ordenamiento español*, p. 119.

[366] Galán Muñoz, *Los ciberdelitos en el ordenamiento español*, pp. 120 – 121.

[367] L. Hernández Díaz, *Los accesos ilícitos a sistemas informáticos: normativa internacional y regulación en el ordenamiento penal español*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2019, p. 283. Hernández Díaz destaca el hecho de que aunque el artículo 197 bis 1 exige la vulneración de las medidas de seguridad establecidas para impedir el acceso, en ningún momento se especifica en qué deben consistir. Coincido con su afirmación de que, a través de la deducción, es posible llegar a la conclusión de que no se trata solo de medidas de carácter lógico, como las contraseñas, sino también de carácter físico, siempre que su objetivo sea la protección de los sistemas de información frente a los accesos de terceros no autorizados.

[368] E. Velasco Núñez, *Delitos tecnológicos. Cuestiones penales y procesales*, 1ª ed., Madrid, Wolters Kluwer, 2021, p. 246. No importa la modalidad de ataque ni el método de intrusión empleados, toda vez que el art. 197 bis 1 del CP prevé todas las intrusiones que se realicen por cualquier medio o procedimiento.

[369] M.ª T. Castiñeira Palou y A. Estrada i Cuadras, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en J.M. Silva Sánchez (dir.),

facilitación a un tercero de dicha vulneración, la cual, a su vez, debe ser efectiva. No entran dentro del ámbito punitivo los accesos llevados a cabo sin vulnerar medidas de seguridad de estas características, incluso en ausencia de la autorización debida, o los accesos a sistemas que carecen de esta clase de protección. Tampoco los accesos disponiendo de autorización, que debe haber sido otorgada por la persona física o jurídica que sea titular del sistema de información al que se ha accedido, o por otra delegada de aquélla, e incluso, de acuerdo con el art. 1, párrafo d, de la Decisión Marco 2005/222/JAI, por la ley. Resulta necesario, con carácter adicional, haber accedido sin autorización, lo que considero redundante cuando el precepto exige ya la vulneración de medidas de seguridad. No entraré a valorar en profundidad aspectos como este, ya que lo haré en el apartado dedicado a la propuesta de *lege ferenda*, pero, junto a la ausencia de la necesidad de obrar con intención de perjudicar al sujeto pasivo o a un tercero y de lesionar realmente el bien jurídico protegido (aunque sí es necesario el dolo), se ha llamado a esta conducta *hacking* blanco o intrusión blanca. Hay mucho que discutir en relación con ella, como la idea de que en esta estructura típica se produce un adelantamiento de la intervención del Derecho penal que pone en entredicho el principio de lesividad[370].

Profundizando en las medidas de seguridad a las que hace referencia el tipo delictivo, es necesario que el ciberdelincuente las vulnere para acceder al sistema informático, si bien deben cumplir el requisito de haber sido establecidas para impedir el acceso y la permanencia típicos. Este matiz es importante, ya que existen distintas clases de medidas de seguridad en el ámbito de la informática, pero para el tipo solo son relevantes las interpuestas para evitar la realización de las conductas prohibidas. Al contrario que en el delito de allanamiento de morada (lo cual nos aleja más y más de la teoría del domicilio informático), no basta una declaración más o menos expresa de

Lecciones de Derecho Penal, Parte Especial, 7ª ed., Barcelona, Atelier, 2021, p. 170. La vulneración de las medidas de seguridad establecidas para impedir la intrusión es destacada, una vez más, como la parte esencial de la conducta típica de este artículo.

[370] Romeo Casabona, *Derecho Penal, Parte Especial*, pp. 285 – 286.

negación de acceso, sino que son necesarias unas medidas de seguridad independientes, en todo caso, de la autorización. Según la SAP de Girona 358/2015, de 22 de junio[371], las contraseñas pueden considerarse como tal, puesto que mediante las mismas se controla el acceso y la permanencia en el sistema. No serían admisibles como tal las medidas burdas, es decir, aquellas que no exijan un nivel técnico elevado para su vulneración; muy al contrario, las claves, para ser idóneas para impedir el acceso y la permanencia no deseados, deben estar dotadas de cierto grado de complejidad[372], siendo preferibles las compuestas por caracteres alfanuméricos propuestas por el sistema. Por último, la SAP de Vizcaya 90307/2014, de 23 de julio[373], sostiene que cuando se ha intentado sin éxito utilizar una contraseña para acceder a un sistema informático procede estimar ejecutados los hechos solo en grado de tentativa, atendiendo al escaso peligro que dicha acción representa para un sistema informático que, se entiende, se encuentra debidamente protegido gracias a la eficacia de su contraseña.

3.3.2.1.5 Interceptación de transmisiones no públicas de datos informáticos

Al delito del art. 197 bis 2, gracias al cual la legislación penal española cumple con lo dispuesto en el art. 6 de la Directiva 2013/40/CE, se le pueden atribuir muchas de las puntualizaciones dedicadas al art. 197 bis 1 en el subapartado anterior. En cuanto al objeto material, en este caso son solo los datos informáticos, si bien deben ser de carácter personal. La acción típica

[371] ECLI:ES:APGI:2015:940.

[372] M.ª P. Serrano Ferrer, *Derecho penal y nuevas tecnologías*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021, pp. 25 – 28. Serrano Ferrer se muestra favorable a la idea de que el art. 197 bis 1 trasciende a la intimidad y a los datos reservados de carácter personal y marca un nuevo espacio de protección con un bien jurídico diferenciado: la seguridad o la intangibilidad de los sistemas informáticos; idea avalada, a su juicio, por la normativa internacional y comparada. Así, el delito de intrusión se comportaría como una figura de lesión, pues su consumación viene determinada por el acceso a o la permanencia en un sistema.

[373] ECLI:ES:APBI:2014:1696.

consiste en la interceptación de transmisiones no públicas de datos informáticos que se produzca desde, hacia o dentro de un sistema de información. Tanto las expresiones elegidas (debería haberse hecho referencia a la interceptación de transmisiones no personales o automatizadas, en lugar no públicas) como el hecho de que las mismas dejan en segundo plano la intimidad como objeto de protección en beneficio de la seguridad de los sistemas informáticos evidencian, una vez más, que la ubicación elegida para este delito es inadecuada. Este delito solo puede cometerse utilizando artificios o instrumentos técnicos y sin contar con la debida autorización para llevar a cabo la interceptación, si bien no es necesaria la vulneración de ninguna medida de seguridad[374], motivo por el cual su vinculación con la seguridad de las redes y sistemas de información resulta más remota, aspecto que supone una diferencia esencial respecto al art. 197 bis 1, toda vez que no puede considerarse que la ciberseguridad sea el elemento nuclear del tipo.

3.3.2.2 Ciberseguridad en los delitos contra el patrimonio y contra el orden socioeconómico

Una vez analizados aquellos delitos contra la intimidad y el derecho a la propia imagen que son, a su vez, una herramienta para garantizar la ciberseguridad, es necesario, con objeto de desarrollar una visión de conjunto de la manera en que determinados artículos del CP español protegen también la seguridad física o lógica de las redes y sistemas informáticos, analizar otra clase de delitos. Esto nos obliga a alejarnos de la intimidad y de los datos de carácter personal reservados como bienes jurídicos protegidos y a analizar la forma en que las medidas de seguridad informatizadas pueden vulnerarse por parte de sujetos que, en su afán de hacerse con bienes de diversa naturaleza con valor patrimonial, consiguen sortear las medidas de ciberseguridad establecidas para protegerlos, lesionando la propiedad y, en su caso, la posesión de los mismos cuando, tras vulnerarlas, logran su

[374] Romeo Casabona, *Derecho Penal, Parte Especial*, pp. 286 – 287.

objetivo final. Idénticas consideraciones merecerán distintos tipos delictivos incluidos en el CP, que analizaré de manera ordenada utilizando como criterio su localización en el mismo.

3.3.2.2.1 Robo con fuerza en las cosas

El progreso tecnológico obliga a replantear delitos clásicos del CP como el robo con fuerza en las cosas[375], en cuyo articulado tienen cabida algunas conductas relacionadas con el descubrimiento de claves, las llaves digitales, y los sistemas de seguridad informatizados. Y es que en relación con el robo, la fuerza en las cosas supone el quebrantamiento de las medidas de seguridad que su propietario ha colocado con intención de proteger la cosa objeto de sustracción, y esto incluye, hoy en día, también las medidas de ciberseguridad[376].

La fuerza debe utilizarse para acceder al lugar donde se encuentran debidamente protegidas las cosas ajenas, o bien para abandonarlo con posterioridad a la aprehensión, siempre que el sujeto activo tenga el propósito de apoderarse de los bienes apetecidos[377]. Esta fuerza, no obstante, no tiene que ser necesariamente física, toda vez que se ha ido espiritualizando el concepto de fuerza en las cosas, siempre que se violente al menos una de las entradas habituales. Es necesario, por lo tanto, la existencia de un ánimo apropiatorio, y no resulta suficiente utilizar cualquier tipo de fuerza, sino que la misma debe encajar en uno de los medios comisivos que especifica el *numerus clausus* del art. 238 del CP[378]. Tres de ellos resultan idóneos para quebrantar las medidas de ciberseguridad como medio para hacerse con

[375] E.M. Souto García, *Los Delitos de Hurto y Robo,* 1ª ed., Valencia, Tirant lo Blanch, 2017, pp. 125 – 152.

[376] M. Llobet Anglí, "Delitos patrimoniales y contra el orden socioeconómico. Sección 3. Robo con fuerza en las cosas", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, p. 1299. En efecto, en el ámbito del robo, la fuerza en las cosas supone el quebrantamiento de las medidas de seguridad que el propietario ha colocado para proteger la cosa objeto de sustracción.

[377] Llobet Anglí, *Memento Práctico de Derecho Penal 2021*, p. 1299.

[378] Llobet Anglí, *Memento Práctico de Derecho Penal 2021*, p. 1299.

estos bienes: el descubrimiento de claves para la sustracción del contenido del art. 238.3, el uso de llaves falsas del art. 238.4 y la inutilización de sistemas específicos de alarma o guarda del art. 238.5 del CP. Al estar relacionados con la seguridad de las redes y sistemas informáticos, analizaré las características de cada uno de ellos que los hacen idóneos para la defensa de la misma.

3.3.2.2.1.1 Descubrimiento de claves para la sustracción del contenido

Más conocido como fractura interior o mobiliaria, consiste en la fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o bien en el forzamiento de sus cerraduras o descubrimiento de sus claves. Está relacionada con la ciberseguridad la segunda de las dos modalidades de ejecución: el descubrimiento ilícito de las claves. La fuerza típica, el descubrimiento, se despliega sobre un continente mueble con objeto de superar el mecanismo informatizado de defensa y protección establecido por el propietario de la cosa guardada. Aunque, como recuerda la SAP de Barcelona de 5 de noviembre de 2004, debe tenerse en cuenta que el principio de legalidad impide llevar a cabo interpretaciones extensivas en contra del reo, encaja en la conducta típica que un *cracker* utilice una herramienta para descubrir claves basándose en combinaciones de palabras, listados de contraseñas más utilizadas o criterios más elaborados y complejos, siempre con el objetivo de quebrantar las medidas de ciberseguridad para poder acceder a los objetos deseados[379]. Así, el sujeto activo lesiona la integridad del sistema de ciberseguridad, puesto que con el descubrimiento ilícito de sus claves este sistema, aunque continúa disponible a todos los demás efectos, es despojado de toda su utilidad, imposibilitando el objetivo para el que fue creado y siendo el paso intermedio necesario para el acceso al objeto material del delito, que con la consumación cae en manos del delincuente.

[379] Llobet Anglí, *Memento Práctico de Derecho Penal 2021*, pp. 1306 – 1307.

3.3.2.2.1.2 Uso de llaves falsas

El art. 239 del CP aclara el delito previsto en el art. 238.4 del mismo texto al establecer que se consideran llaves falsas, entre otras, las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya una infracción penal, y cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo. Esto incluye, también, aquellas llaves que permitan burlar los sistemas de seguridad informatizados. Dejo de lado las ganzúas u otros instrumentos análogos, aunque de acuerdo con la jurisprudencia (STS de 18 de febrero del 2000) sea suficiente que el instrumento resulte apto para accionar un mecanismo de cierre de una puerta dejando abierto y expedido lo que antes estaba cerrado, porque la última de las acepciones es lo suficientemente amplia como para abarcar los supuestos de copias ilegítimas o duplicadas de llaves digitales, e incluso de llaves maestras, siempre que sean suficientes, por sí mismas, para conseguir dicha apertura. En efecto, la llave no tiene por qué ser un instrumento de metal o compuesto de un material determinado: solo se exige que sirva para abrir o cerrar un determinado mecanismo de apertura o cierre sin producir su rotura, de manera que es posible adaptar la actual redacción de este precepto a las nuevas tecnologías informáticas y relacionarlo con la ciberseguridad. Así, se incluyen en el mismo equiparándolas a las llaves las tarjetas, magnéticas o perforadas, los mandos o instrumentos que permiten la apertura a distancia e incluso, tras la reforma introducida por la LO 5/2010, cualquier otro instrumento tecnológico de eficacia similar.

A día de hoy no se ha resuelto ningún caso en los tribunales que se ajuste a estas características, pero el avance de la tecnología hace conveniente la previsión en este sentido, permitiendo así acomodar convenientemente las novedades tecnológicas[380] que afectan a la integridad de las redes y sistemas informáticos, puesto que con el uso de llaves falsas un sistema de seguridad informatizado puede seguir disponible, si bien deja

[380] Llobet Anglí, *Memento Práctico de Derecho Penal 2021*, pp. 1307 – 1309.

de cumplir el objetivo para el que fue creado a causa de la actividad criminal, que en este caso utiliza un elemento que forma parte del sistema de ciberseguridad para abrir lo que está cerrado y acceder con el objetivo final de hacerse con el objeto material del delito. Igual que sucedía en el caso del descubrimiento de claves para la sustracción del contenido del art. 238.3 del CP, el ataque a las medidas de seguridad informatizadas es un medio para la consecución de un fin, solo que en este caso tiende a recaer menos sobre el *software* y más sobre el *hardware*. No obstante, los avances tecnológicos harán que esta tendencia cambie a medida que se generalice el uso de llaves de seguridad como el *software* USB *Raptor*, que otorgan un mayor de nivel de seguridad al permanecer cifrado el contenido del archivo y, además, aportar un informe del estado del equipo. A través del mismo, el acceso al sistema solo es posible cuando el USB está conectado. Hacerse con una copia de este *software* supone hacerse con la llave que permite el acceso posterior al bien apetecido. Y es que el art. 239, en su último párrafo, sostiene que se consideran llaves las tarjetas, magnéticas o perforadas, los mandos o instrumentos de apertura a distancia y cualquier otro instrumento tecnológico de eficacia similar

Mención aparte requieren los casos de extracción de dinero en cajeros con tarjetas ajenas obtenidas de manera ilícita, los cuales siguen siendo calificados de robo por un sector de la doctrina basándose en que la conducta presenta las características propias de un apoderamiento, más que de una defraudación[381]. La jurisprudencia establece justo lo contrario, incluso pese a la existencia de opiniones enfrentadas en su seno. Y es que al principio coexistieron en relación con los mismos dos líneas jurisprudenciales que los calificaron de manera distinta: la primera los calificó como robo con fuerza en las cosas en su modalidad de uso de llave falsa; sin embargo, la segunda (comenzada por la STS 369/2007, de 9 de mayo de 2007), que acabó convirtiéndose en jurisprudencia mayoritaria (aunque no unánime) gracias a

[381] C. Alastuey Dobón, "Delitos contra el patrimonio y contra el orden socioeconómico I. Hurtos. Robos. Extorsión. Robo y hurto de uso de vehículos. Usurpación", en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho Penal, Parte Especial*, 2ª ed., Granada, Comares, 2022, p. 357.

sentencias como la SAP de Vizcaya de 28 de diciembre de 2009, determinó que la calificación correcta era la de estafa informática, puesto que no solo se ocultaban datos reales, sino que se introducían otros falsos en el sistema. A esta identificación en la que se ocultaba la identidad real del operador y se suplantaba la del verdadero titular había que añadir la introducción del número secreto (ya se hubiese obtenido indebidamente o al margen de cualquier actividad delictiva), que dotaba al hecho de una relevancia o eficacia jurídica que constituía el dato clave para estimar la existencia de una manipulación informática, consistente en identificarse ante el sistema informático de forma mendaz e introducir datos en el mismo que no se correspondían con la realidad.

En efecto, la introducción de la tarjeta, el tecleo del número clave[382] y la selección del importe llevan al aparato a efectuar una transferencia no consentida de un activo patrimonial, pero la disposición voluntaria de la máquina hace imposible afirmar la existencia del apoderamiento propio del robo, que debe producirse contra la voluntad del dueño o, como mínimo, en ausencia de la misma. Y es que el apoderamiento conlleva la ausencia de voluntad del *tradens,* y en la estafa informática el cajero entrega el dinero por la manipulación del sistema. La STS 509/2018, de 26 de octubre[383], establece que la utilización indebida del número de identificación personal propicia la recepción del dinero que entrega o expide el cajero, siendo esto distinto de la toma del mismo por parte del usuario de la tarjeta, quien no lo coge, sino que lo recibe del cajero. Así, recientes sentencias como la STS 204/2020, de 21 de mayo[384], reafirman la tendencia jurisprudencial de defender la existencia

[382] P. Faraldo Cabana, *Las nuevas tecnologías en los delitos contra el patrimonio y el orden* socioeconómico, 1ª ed., Valencia, Tirant lo Blanch, 2009, pp. 53 – 55. El número secreto o PIN ha sido un elemento fundamental para elevar el nivel de seguridad de las tarjetas bancarias tradicionales, pero con el avance de la tecnología se han generalizado las tarjetas electrónicas (que contienen un chip con circuitos integrados e incluso, en ocasiones, hasta un microprocesador) y las tarjetas sin contacto, que usan un campo magnético o radiofrecuencia (RFID) para la lectura a una distancia media, y que obligan a replantear la manera en que los ciberdelincuentes intentarán dejar sin efecto las medidas de seguridad establecidas.

[383] ECLI:ES:TS:2018:3666.

[384] ECLI:ES:TS:2020:1209.

de una estafa tanto en los casos en que se usa la tarjeta de crédito de un tercero para la realización de compras en establecimientos comerciales como en los que se realizan con ella reintegros en cajeros automáticos[385]. Al predominar la defraudación frente al apoderamiento procede, con carácter general, encuadrar esta conducta en el delito de estafa informática del art. 248.2 del CP[386] [387], y no en el de robo con fuerza en las cosas del art. 238.4 del mismo texto[388]. No obstante, cuando el *modus operandi* incluya el ejercicio de violencia o intimidación en las personas, sentencias como la STS 493/2016, de 9 de junio[389] admiten que los hechos puedan calificarse como robo[390], a causa del predominio del apoderamiento frente a la defraudación.

3.3.2.2.1.3 Inutilización de sistemas específicos de alarma o guarda

De las tres modalidades de robo con fuerza en las cosas relacionadas con la ciberseguridad, esta es, sin duda, la que más afecta a los sistemas de seguridad informatizados, toda vez que se fundamenta en un ataque no contra su integridad, sino contra su disponibilidad. En efecto, consiste en inutilizar los sistemas específicos de alarma o guarda, incluyendo los sistemas de seguridad informatizados, siempre que reúnan las características necesarias para considerarse sistemas específicos especialmente diseñados para alertar o avisar de una entrada o acceso a un lugar determinado. Escasamente llevado a cabo en la práctica, el delito del art. 238.5 requiere

---

[385] Alastuey Dobón, *Derecho Penal, Parte Especial*, p. 357.

[386] Velasco Núñez, *Delitos tecnológicos*, p. 58. Mediante la introducción de este artículo, fue posible cubrir un ámbito al que no llegaba la definición tradicional de estafa y castigar como una manipulación informática a quien se identifica mendazmente ante un sistema informático introduciendo datos que no son reales.

[387] C.D. Azcona Albarrán, *Tarjetas de pago y Derecho penal. Un modelo interpretativo del art. 248.2.c) CP*, 1ª ed., Barcelona, Atelier, 2012, pp. 187 – 191. Y es que, como afirma Choclán Montalvo, debe permitirse a la víctima cierto relajamiento de sus deberes de protección, puesto que, de lo contrario, se impondría un principio general de desconfianza en el tráfico jurídico incompatible con la velocidad del intercambio de bienes y servicios actual, siendo importante perseguir a quien se vale de esta circunstancia para defraudar.

[388] Llobet Anglí, *Memento Práctico de Derecho Penal 2021*, p. 1309.

[389] ECLI:ES:TS:2016:2717.

[390] Alastuey Dobón, *Derecho Penal, Parte Especial*, p. 357.

ejercer la fuerza para acceder o abandonar el lugar donde se encuentra la cosa, no siendo posible su aplicación cuando se ejerza sobre los dispositivos electrónicos que la rodean o están adheridos a la misma. La inutilización conlleva desactivar, romper o manipular el sistema informático de que se trate, no siendo de aplicación este artículo en los supuestos de elusión y de utilización ilegítima (como aquellos en los que se marca la clave de acceso a un edificio inteligente), puesto que en dichos casos no se inutiliza realmente el sistema, sino que se hace un uso correcto pero ilegítimo del mismo. De acuerdo a la STS de 25 de junio de 1999, el legislador exige no solo el empleo de fuerza en las cosas, sino que detalla su carácter instrumental, es decir: el hecho de que se utilice para posibilitar el acceso al lugar donde se encuentran, debidamente protegidas, las cosas muebles ajenas. Esto evidencia que los ataques contra las medidas de seguridad informatizadas consistentes en su inutilización encajan en el tipo delictivo, al tratarse de una modalidad típica de fuerza utilizada de manera instrumental con el objetivo final de acceder al objeto material del delito[391].

3.3.2.2.2 Estafa informática

La estafa informática del art. 248.2.a) del CP consiste en conseguir una transferencia no consentida de cualquier activo patrimonial[392] en perjuicio de tercero mediando ánimo de lucro, a través de una manipulación informática[393]

[391] Llobet Anglí, *Memento Práctico de Derecho Penal 2021*, pp. 1309 – 1311.

[392] Romeo Casabona, *Poder informático y seguridad jurídica*, p. 58.

[393] C.M. Romeo Casabona et al., "Informe sobre los nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica. Líneas de investigación y conclusiones", en C.M. Romeo Casabona y F. Flores Mendoza (eds.), *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica,* Granada, Comares, 2012, p. 729. El CP español no define la manipulación informática, al contrario de lo que sucede en los ordenamientos jurídicos de otros países europeos, como Alemania. El § 263a (1) StGB, que tipifica la estafa informática, describe de manera enumerativa y alternativa sus cuatro posibles formas de comisión, delimitado así su conducta típica, en la que se incluye una referencia sorprendentemente genérica a incurrir en la misma a través de cualquier modo de interferencia no autorizada en el proceso de datos. Como sostiene Galán Muñoz, este es un instrumento adecuado para conseguir la sanción penal de todas aquellas manipulaciones que se pudiesen llegar a crear como consecuencia del desarrollo tecnológico o de la inventiva e imaginación de

o artificio semejante[394] [395] [396] [397]. Estas últimas no se dirigen a otras personas, sino a máquinas, las cuales, en su automatismo y a consecuencia de la conducta artera del sujeto activo, actúan en perjuicio de un tercero. La manipulación engloba tanto la alteración como la modificación de programas o datos informáticos, e incluso del propio equipo informático, incluyendo el aprovecharse, servirse usar o utilizar una manipulación ya iniciada o efectuada, incluso por un tercero[398]. Es precisamente esta manipulación[399] la

---

los defraudadores y que resultaban imprevisibles en el momento de la redacción del mencionado artículo por el legislador alemán.

[394] N.J. De la Mata Barranco, "Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general", en J.I. Echano Basaldua (dir.), *Cuadernos penales José María Lidón, no. 4. Delito e informática: algunos* aspectos, 1ª ed., Bilbao, Publicaciones de la Universidad de Deusto, 2007, p. 68. Quedan fuera del precepto aquellos supuestos en que no se producen manipulación informática ni artificio semejante alguno, sino solo la obtención de las claves de acceso lícita o ilícitamente.

[395] M. Bajo Fernández, *Los delitos de estafa en el Código Penal,* 1ª ed., Madrid, Editorial Universitaria Ramón Areces, 2004, p. 166. La doctrina coincide en que aunque incluir elementos de contenido vago como "artificio semejante" es arriesgado por tratarse de un lenguaje difuso, su utilización también resulta inevitable ante el desarrollo tecnológico vertiginoso y ante la imposibilidad de describir un sinfín de conductas típicas.

[396] R.M. Mata y Martín, *Estafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago. El Uso Fraudulento de Tarjetas y otros Instrumentos de Pago*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2007, p. 93. Mediante esta fórmula se buscaba, en efecto, evitar lagunas de punición.

[397] J. Antón Oneca, *Obras. Tomo III*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2003, p. 89. Esta obligación de llevar a cabo una manipulación informática o artificio semejante dificulta la posibilidad de que pueda cometerse la estafa informática por omisión, ya que, igual que en la estafa tradicional, faltaría el artificio exigido por el tipo delictivo. Es importante tener en cuenta, no obstante, que algunos penalistas alemanes opinan que la estafa tradicional puede cometerse por omisión cuando el sujeto tiene el deber de obrar. A esto último se opuso, de manera genérica, J. Cerezo Mir, *Temas fundamentales del Derecho Penal. Tomo II*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2002, p. 103, quien consideraba que, en un delito de acción, no es necesario que el sujeto tenga la obligación de evitar la perpetración del mismo (es decir, que ocupe la posición de garante del bien jurídico protegido) para que se le pueda considerar cómplice por omisión.

[398] A. Galán Muñoz, *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 C.P.,* 1ª ed., Valencia, Tirant lo Blanch, 2005, p. 559.

[399] C. Conde-Pumpido Ferreiro, *Estafas*, 1ª ed., Valencia, Tirant lo Blanch, 1997, pp. 214 – 217. José Antón Oneca era partidario del criterio de la jurisprudencia alemana, al entender que una máquina no puede ser engañada, toda vez que el engaño es una operación intelectual muy por encima del automatismo que las caracteriza. Por tanto, la tipificación de esta conducta debía ser distinta a la de la estafa tradicional. Conde-Pumpido Ferreiro, considero, no contradice, sino que completa la opinión de Antón Oneca al afirmar que sí hay engaño, pero que la víctima del mismo es el hombre que ha programado la máquina. En cualquier caso, con la inclusión expresa del tipo del art.

que permite relacionar este delito con la ciberseguridad, toda vez que al afectar la manipulación informática[400] o el artificio semejante a un sistema informático (ya sea a su *hardware* o a su *software*), se ataca a su integridad, con la peculiaridad distintiva de que, en este delito en concreto, el criminal necesita garantizar la disponibilidad del sistema informático para conseguir su objetivo, y todos sus esfuerzos se concentran en lesionar su integridad perturbando el funcionamiento debido del procesamiento[401], ya sea durante la fase de introducción de los datos o durante el tratamiento de los que ya se encuentran almacenados en el sistema[402]. En efecto, el sujeto activo necesita que el sistema informático funcione para cumplir su objetivo, solo que pretende conseguir un beneficio a través de las manipulaciones o artificios con los que modifica su normal funcionamiento. El sujeto activo del delito ataca la ciberseguridad como medio para conseguir su objetivo final de satisfacer su ánimo de lucro, ya se trate de las medidas de seguridad informática establecidas para proteger el sistema informático o el propio sistema informático una vez eliminadas o desactivadas las primeras[403].

248.2 del CP, la cuestión quedó zanjada: la estafa informática es una estafa especial y analógica que no constituye un subtipo o modalidad de la estafa básica, sino un delito independiente de aquella, y goza de sus propios elementos constitutivos, entre los cuales se encuentra aquel que es de más interés para el objeto de esta investigación: la manipulación de un sistema informático.

[400] R. M. Mata y Martín, "Medios electrónicos de pago y delitos de estafa", en R.M. Mata y Martín (dir.), *Los medios electrónicos de pago. Problemas* jurídicos, 1ª ed., Granada, Comares, 2007, pp. 342 – 348.

[401] Mata y Martín, *Estafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago,* p. 156.

[402] Galán Muñoz, *El fraude y la estafa mediante sistemas informáticos*, pp. 560 - 561. Como pone de manifiesto Galán Muñoz, Romeo Casabona definió ya en 1996 esta manipulación como la incorrecta modificación del resultado de un procesamiento automático de datos, mediante la alteración de los datos que se introducen o están ya contenidos en el ordenador en cualquiera de sus fases de procesamiento o tratamiento, siempre que sea con ánimo de lucro y perjuicio de tercero. Siguen esta definición Orts Berenguer, Roig Torres, Mata y Martín y Pérez Manzano. Gómez Perals, por su parte, se mostraba partidario de una descripción más exhaustiva de las conductas a englobar dentro este concepto.

[403] J. Rodríguez-Miguel Ramos, *La autoprotección en la estafa en la jurisprudencia del Tribunal Supremo*, 1ª ed., Valencia, Tirant lo Blanch, 2013, p. 67. En la estafa tradicional, hubo un intercambio de pareceres entre doctrina y jurisprudencia, ya que mientras que la segunda no se manifestó en este sentido, la primera sí advirtió que, en el ámbito de los delitos patrimoniales, correspondía a la víctima cierto deber de autoprotección. Resulta fácil trasladar esta idea a las estafas informáticas, que deberían obligar a

A pesar de la vaguedad conceptual del tipo delictivo[404], los artificios semejantes, entendidos como artimañas, dobleces, enredos o trucos deben, en cualquier caso, incluir operaciones parecidas a las manipulaciones informáticas, con objeto de respetar el principio de legalidad. El criterio para valorar la adecuación de estos artificios es su aptitud como medio informático para producir el daño patrimonial. Así, se consideran equivalentes conductas como modificar materialmente un programa informático de manera indebida o utilizarlo sin la debida autorización o de forma contraria a como fue diseñado[405].

En teoría, esta forma de estafa se compone de los siguientes elementos: primero, el uso de una manipulación[406] informática u otro artificio semejante; segundo, la causación de la transferencia de un activo patrimonial; tercero, el carácter no consentido de dicha transferencia; cuarto, el ánimo de lucro; y quinto, el perjuicio de un tercero. De todos ellos, el más importante para esta investigación sobre ciberseguridad es el primero: el mecanismo de manipulación informática[407], que supone una alteración o modificación de los presupuestos básicos del sistema o de las órdenes

quienes depositan su confianza en máquinas y mecanismos automatizados a dotarlos de las medidas de seguridad informática necesarias para evitar, en este caso, cualquier manipulación informática o artificio semejante.

[404] M.V. Calle Rodríguez, "El delito de estafa informática", *La ley penal: revista de derecho penal, procesal y penitenciario,* no. 37, 2007, p. 40. Un nivel mayor de especificidad en el tipo delictivo hubiese redundado en una mayor seguridad jurídica, puesto que el término *artificio semejante* resulta excesivamente amplio.

[405] M. Maraver Gómez, "Delitos patrimoniales y contra el orden socioeconómico. Sección 8. Estafa", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, p. 1355. Es indudable que los elementos de contenido utilizados en el precepto pueden resultar algo vagos.

[406] J.A. Choclán Montalvo, *El delito de estafa*, 2ª ed., Barcelona*,* Bosch, 2009, p. 340. Esta manipulación no requiere un contacto inmediato con el ordenador que contiene los datos, sino que cada vez son más habituales los sistemas operados a distancia mediante los que es posible el procesamiento de datos.

[407] R. M. Mata y Martín, "Artículo 248", en M. Gómez Tomillo (dir.), *Comentarios prácticos al Código Penal. Tomo III. Delitos contra el patrimonio y socioeconómicos. Artículos 234 – 318 bis*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, p. 172. Mata y Martín remite a la definición de Romeo Casabona de manipulación informática o artificio semejante, que es el equivalente del engaño bastante y del error en la estafa informática: consiste en la incorrecta modificación del resultado de un procesamiento automatizado en cualquiera de las fases de procesamiento o tratamiento informático con ánimo de lucro y perjuicio de tercero.

recibidas por este de forma que se produzcan resultados no previstos o no autorizados.

Tradicionalmente, se abordó la cuestión del funcionamiento de los sistemas informáticos dividiendo su actividad en tres fases, y atribuyendo un tipo distinto de manipulación a cada una (*input*[408], fraudes de consola, y *output*[409] [410]), conservando esta división su lógica hoy día, pero encontrándose también obsoleta por el avance tecnológico.

En la práctica, la amplitud de la fórmula actualmente empleada por el legislador ha quedado sobradamente justificada por la numerosísima diversidad de modalidades de comisión del delito, como la alteración de los elementos físicos de una máquina, la alteración de los elementos que permiten su programación o la introducción de datos falsos, entre otras muchas. Una de las más frecuentes es el *phishing*[411] [412] [413] mediante *e-mail* fraudulento, que se fundamenta en el envío de un correo electrónico que procede, en apariencia, de una fuente fiable, pero cuyo objetivo es obtener

[408] Conde-Pumpido Ferreiro, *Estafas*, p. 218.

[409] Conde-Pumpido Ferreiro, *Estafas*, p. 219.

[410] C.M. Romeo Casabona, *Las Transformaciones del Derecho penal en un mundo en cambio (Volumen I)*, 1ª ed., Arequipa, Adrus, 2004, p. 385. Si el resultado de la manipulación era percibido por una persona encargada de autorizar la operación, se podía considerar a esta persona como la engañada y la disponente, con independencia de en qué fase del procesamiento de los datos de entre las descritas ocurriese.

[411] E. Willems, *Cyberdanger: Understanding and Guarding Against Cybercrime*, 1ª ed., Cham, Springer, 2019, p. 40. El *phishing* es una forma de estafa muy conocida, pero también muy peligrosa. A través del mismo, los criminales, con un mínimo esfuerzo, pueden obtener información de una persona y aprovecharla. Véase también la reflexión sobre la vulnerabilidad y el *phishing* en A. Abadías Selma, N. Fernández Albesa, y R. Leal Ruiz, *Ciberdelincuencia. Temas prácticos para su estudio*, 1ª ed., A Coruña, Colex, 2021, p. 242.

[412] L.F. Rey Huidobro, "La estafa informática: relevancia penal del *phishing* y el *pharming*", *La ley penal: revista de derecho penal, procesal y penitenciario,* vol. 10, no. 101, 2013, p. 22. Además del *phishing,* existen ciberataques como el *pharming*, mediante los cuales, aprovechando vulnerabilidades en los DNS o en los equipos de los usuarios, se redirige el tráfico web al sitio falso que el atacante haya especificado. Los sitios web falsos pueden utilizarse por el sujeto activo para la instalación de virus o troyanos en el ordenador del sujeto pasivo, o para la recolección de su información personal o bancaria con fines delictivos.

[413] J. Barbero Bajo, "*Phishing* y otros delitos informáticos: el uso ilícito de Internet", *Lex nova: La revista,* no. 53, 2008, p. 6. La complejidad cada vez mayor de estos delitos es el resultado del avance de la tecnología.

datos confidenciales del usuario que se utilizan para llevar a cabo la estafa y acceder a su cuenta corriente, realizando con posterioridad transferencias de dinero dirigidas al autor directo o a un colaborador del fraude[414].

Lo que el sujeto activo desea conseguir es la transferencia no consentida de un activo patrimonial a través de la alteración o modificación de instrumentos informáticos, por lo que el bien jurídico protegido por este delito es, precisamente, el patrimonio[415]. Cuando el acto de disposición económica en perjuicio de un tercero[416] sea consentido, incluso mediando engaño[417], procederá la aplicación del tipo básico. Los activos patrimoniales consisten en objetos con valor económico, en sentido amplio. Aunque es necesario el dolo, se acepta el dolo eventual en casos como los de los denominados intermediarios muleros, mulas o *phisher-mules*, que intervienen en el delito como depositarios momentáneos de los fondos transferidos antes de redirigirlos a un tercero a cambio de una comisión[418].

La estafa o fraude informático incluye las conductas contenidas en los arts. 248.2 a), b) y c) del CP, tratándose de auténticas defraudaciones realizadas mediante procedimientos informáticos. El art. 248.2 a) castiga la conducta de quien, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigue la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero[419]. Al encontrarnos ante

---

414 Maraver Gómez, *Memento Práctico de Derecho Penal 2021*, p. 1356.

415 J. Sánchez Bernal, "El bien jurídico protegido en el delito de estafa informática", *Cuadernos del Tomás: revista de estudios del Colegio Mayor Tomás Luis de Victoria,* no. 1, 2009, p. 121. La opinión mayoritaria de la doctrina defiende que el bien jurídico protegido en el delito de estafa informática es el patrimonio, si bien debe entenderse de manera amplia, es decir, como un conjunto de derechos, bienes y relaciones jurídicas de que puede ser titular un sujeto. Se trata, por tanto, de un delito económico de enriquecimiento.

416 González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 718.

417 P. Sánchez-Ostiz, *A vueltas con la Parte Especial. Estudios de Derecho penal*, 1ª ed., Barcelona, Atelier, 2020, p. 51. En el tipo básico de estafa hay engaño específicamente sobre el sentido de lo comprado.

418 Maraver Gómez, *Memento Práctico de Derecho Penal 2021*, p. 1356.

419 C.M. Romeo Casabona, "Delitos contra el patrimonio y el orden socioeconómico II. Defraudaciones, insolvencias punibles, alteración de precios en concursos y subastas públicas y daños", en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho Penal, Parte Especial*, 2ª ed., Granada, Comares, 2022, p. 380.

un tipo mixto alternativo[420], la segunda conducta prohibida, recogida en el art. 248.2.b) del CP, castiga la fabricación, introducción, posesión o facilitación de programas de ordenador destinados específicamente a cometer las estafas. Estas conductas están limitadas en su alcance por el fin de la norma, de manera que cuando no son idóneas para la comisión de estafas el hecho no puede considerarse típico. De acuerdo a las STS de 26 de junio de 2006 y de 10 de noviembre de 2011, el *modus operandi* para el desplazamiento patrimonial de la víctima deben ser las manipulaciones del sistema informático, siendo la estafa informática un tipo delictivo de naturaleza medial o instrumental respecto de la estafa, de manera que la lesión a la ciberseguridad aparece, una vez más, como un medio para la consecución de un fin. Además, el objeto material del delito[421], que es el programa de ordenador, debe estar específicamente destinado a dicha comisión, no

---

Mediante la utilización de tipos de equivalencia se sustituyeron los elementos propios del delito tradicional de estafa por otros adaptados a las características comisivas de tipo informático. Romeo Casabona prefiere referirse a este delito denominándolo "fraude informático".

[420] Galán Muñoz, *El fraude y la estafa mediante sistemas informáticos*, p. 559.

[421] Velasco Núñez, *Delitos tecnológicos*, pp. 60 – 63. Es muy importante aclarar que el hecho de que el ciberdelincuente haga uso de la última tecnología no conlleva la existencia de una estafa informática, pudiendo tratarse de una estafa tradicional basada en el engaño pero utilizando criptomonedas, como el bitcóin. Así lo demuestra la STS 326/2019, de 20 de junio (ECLI:ES:TS:2019:2109), en la que se condenó por estafa a una persona que se ofreció a gestionar y reinvertir para terceras personas ciertas cantidades de criptomonedas, no haciéndolo ni devolviéndoles posteriormente los bitcoines, puesto que su plan era quedárselos desde el principio. Más allá de esta aclaración, me interesa la cuestión de si una criptomoneda descentralizada como el bitcóin podría ser también objeto material del delito de estafa informática, puesto que se trata de un activo inmaterial de intercambio o contraprestación en transacciones bilaterales aceptadas por quienes las realizan, no siendo ni siquiera dinero electrónico. Sin duda, la mencionada sentencia permite que así sea, pero al ser necesaria la transferencia no consentida de un activo patrimonial, la duda debe ser, entonces, cual es el límite entre lo que encaja en los requisitos del tipo y lo que no. El bitcóin y las demás criptomonedas van a convertirse en verdaderos desafíos para la ciberseguridad y el Derecho penal, ya sea por las posibilidades que ofrecen en relación con delitos tradicionales como el blanqueo de capitales, o por su capacidad de crear delitos nuevos como el *cryptojacking*, término ni siquiera aún traducido que define el uso ilegítimo de un dispositivo electrónico sin el consentimiento de su usuario legítimo para, aprovechando la capacidad de procesamiento y de cálculo de su tarjeta gráfica, su memoria y su procesador, realizar el proceso de obtención de criptomonedas y quedarse con el total de las ganancias. Así lo describe O. Tejerina Rodríguez, "Criptoactivos y ciberseguridad", en M. Barrio Andrés (dir.), *Criptoactivos. Retos y desafíos* normativos, 1ª ed., Madrid, Wolters Kluwer, 2021, pp. 297 – 301.

pudiendo perseguirse a través de este artículo el aprovechamiento de un programa con una meta distinta. *A sensu contrario*, si el programa tiene como fin otras prácticas lícitas además de cometer estafas, esto carece de importancia, pues se cumplen igualmente todos los elementos del delito[422] al resultar idóneo el mismo para lesionar la integridad de un determinado sistema informático. Por último, hay que destacar que este carácter medial o instrumental[423] no impide que las penas previstas para las estafas informáticas en el art. 249 del CP sean las mismas que para las estafas tradicionales[424].

3.3.2.2.3 Utilización ilícita de energías, sustancias u otros servicios ajenos

El delito del art. 255 del CP tipifica conductas que constituyen un fraude pero que, sin embargo, no reúnen los requisitos necesarios para ser consideradas estafas ni delitos de apoderamiento, ya que no recaen sobre cosas materiales. El progreso de la tecnología hace que estos delitos, lejanamente vinculados con la ciberseguridad en el momento de su redacción, adquieran una mayor importancia para la misma, ya que engloban defraudaciones en relación con ciertas tecnologías de transmisión de datos inalámbricas. La conducta típica consiste en la utilización de energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos: en definitiva, sustancias fluyentes medidas por contador (incluyendo el wifi), siempre que el valor de lo defraudado supere los 400 €.

Se trata de un tipo de estructura alternativa que permite varias modalidades comisivas: primera, valerse de mecanismos instalados para realizar la defraudación; segunda, la alteración maliciosa de las indicaciones

[422] Maraver Gómez, *Memento Práctico de Derecho Penal 2021*, p. 1356.

[423] Galán Muñoz, *El fraude y la estafa mediante sistemas informáticos*, p. 527.

[424] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 720. Se prevé, para los reos de estafa (incluyendo la estafa informática), la pena de prisión de seis meses a tres años o, si la cuantía de lo defraudado no excede de 400 euros, la pena de multa de uno a tres meses.

o aparatos contadores; tercera, el empleo de cualesquiera otros medios clandestinos. Sujeto activo puede serlo no sólo el usuario, sino también el distribuidor o prestador defraudadores, si bien lo más frecuente es que éste sea el sujeto pasivo[425] y el ciberdelincuente tenga que valerse, precisamente, de algún tipo de maquinación para superar las medidas de seguridad establecidas por estos.

Rechazando las críticas doctrinales relativas a las dificultades para su delimitación[426], en cualquiera de las tres modalidades, al igual que sucede en las estafas informáticas, se afecta a la ciberseguridad en su faceta de integridad, puesto que de lo que se trata es de, respetando la disponibilidad de la máquina, lucrarse de manera clandestina utilizando ilícitamente energías, sustancias u otros servicios ajenos, objetivo para el cual es necesario que la primera esté disponible de manera que aparente normalidad pero no cumpla su función de manera correcta, y debiendo ser la manipulación efectiva, tal y como exige la jurisprudencia (STS 880/1981, de 20 de junio[427]), de manera que se alteren o modifiquen los contadores logrando que su funcionamiento sea realmente defectuoso.

Para su consumación, hace falta ánimo de lucro y que se produzca un perjuicio económico efectivo[428]. En la actualidad, este delito del art. 255 resulta de sumo interés en relación con la ciberseguridad por las múltiples posibilidades que ofrece la utilización del wifi ajeno, puesto que es una herramienta técnica en ocasiones necesaria para la comisión de otros delitos en la Red. Desde la perspectiva de la seguridad de los sistemas de información, y centrándome en el wifi, surgen dos desafíos: primero, uno

---

425 Romeo Casabona, *Derecho Penal, Parte Especial*, p. 391.

426 P. Faraldo-Cabana, "Defraudación de telecomunicaciones y uso no consentido de terminales de telecomunicación: dificultades de delimitación entre los arts. 255 y 256 CP", en F. Muñoz Conde et al. (dirs.), *Un derecho penal comprometido: libro homenaje al prof. Dr. Gerardo Landrove Díaz,* Valencia, Tirant lo Blanch, 2011, p. 363. No comparto la opinión de que exista, más allá de ciertos matices que siempre son inevitables en la práctica, una verdadera dificultad en la delimitación entre estos arts. 255 y 256 del CP.

427 ECLI:ES:TS:1981:4251.

428 Romeo Casabona, *Derecho Penal, Parte Especial*, p. 391.

menor, la manipulación del propio dispositivo contador (toda vez que el gasto efectuado es un aspecto superado por la actual generalización de las tarifas planas muy por debajo de la cantidad exigida por el tipo que impiden que el gasto se dispare y, por lo tanto, pueda cumplirse la elevada exigencia típica de que la defraudación supere los 400 €); segundo, el más importante, la utilización del wifi ajeno sin permiso de su titular para acceder a Internet y cometer otro tipo de delitos. En caso de perseguir las autoridades delitos cometidos en la Red, es indudable que finalmente llegarían a identificar a un usuario determinado mediante su dirección IP, pero antes de eso su investigación también podría conducirles hasta el titular de un wifi que, de ser privado y estar protegido por contraseña, podría tener que, al menos, colaborar en el esclarecimiento de los hechos. Es importante, en consecuencia, mantener un elevado nivel de seguridad en relación con tecnologías como el wifi, puesto que son susceptibles de convertirse, en el mejor de los casos, en una fuente de (escasos) beneficios para los delincuentes y, en el peor, en una herramienta para la comisión de graves ciberdelitos.

Es decir, y como ya viene siendo habitual en el ámbito de la ciberseguridad, en un delito medio de difícil persecución por las obsoletas exigencias económicas del tipo y realmente orientado a conseguir las herramientas para la consecución de un delito fin, y que encaja mucho mejor dentro del tipo delictivo del art. 197 bis 1 del CP, en el que el ciberdelincuente accede al rúter sin autorización tras superar las medidas de seguridad y no solo tiene acceso a la información contenida en el mismo, sino que puede utilizar el wifi para delinquir. No obstante, cuando el propósito del sujeto activo sea solo servirse de un wifi ajeno en su propio beneficio económico y, siendo esta su intención única, no tenga pretensiones de utilizarlo para nada más que para navegar por la Red dentro de los límites legales, sí será de aplicación este art. 255 del CP, por mucho que, reitero, la defraudación no pueda, excepto por acumulación a lo largo del tiempo, superar nunca los 400 €.

3.3.2.2.4 Daños informáticos

El ataque del *ransomware* WannaCry[429] en 2017, que paralizó, entre otros, a numerosos hospitales y centros sanitarios a nivel mundial, demostró que era necesario poner especial atención a la regulación de los daños informáticos. Como expondré en el capítulo cuarto de esta investigación, la dependencia respecto de las redes y sistemas informáticos en ámbitos como el sanitario es enorme, por lo que resulta esencial poder garantizar en él un alto nivel de ciberseguridad. En el derecho español, el art. 264 del CP tipifica de manera extensa las conductas que, de acuerdo a la doctrina, constituyen el delito de daños informáticos, que se configura como un tipo mixto alternativo escindido en dos apartados. El primero de ellos castiga con la pena de prisión de 6 meses a 3 años a quien por cualquier medio, sin autorización y de manera grave borre, dañe, deteriore, altere, suprima o haga inaccesibles datos, programas informáticos o documentos electrónicos ajenos[430] [431], siempre que el resultado producido pueda considerarse grave. El segundo incrimina una conducta de perjuicio informático en relación con los usuarios, castigando con la misma pena al que, por cualquier medio, sin tener autorización y de manera grave obstaculice o interrumpa el funcionamiento de un sistema informático ajeno introduciendo, transmitiendo, dañando, borrando, deteriorando, suprimiendo o haciendo inaccesibles datos

[429] A.E. Nava Garcés, "El caso WannaCry. Ataque en la red", *Revista Penal*, no. 42, 2018, p. 148.

[430] J.J. González Rus, "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (artículo 264.2 del Código penal)", en J.L. Díez Ripollés, C.M. Romeo Casabona, L. Gracia Martín y J.F. Higuera Guimerá (eds.), *La ciencia del derecho penal ante el nuevo siglo: libro homenaje al profesor doctor don José Cerezo Mir*, Madrid, Tecnos, 2002, p. 1287. A pesar de no ser aprehensibles, ni materiales, ni corporales, estos elementos lógicos también tiene entidad real y pueden ser directamente dañados, pudiendo resultar objeto material del delito de daños, que se construye en torno a la posibilidad de destrucción o deterioro de la cosa, incluyendo todo aquello, ya sea corporal o incorporal, que tenga valor económico, que sea capaz de fundamentar un derecho de propiedad y que sea susceptible de sufrir deterioro o de ser destruido. Carece de importancia su naturaleza (electromagnética, óptica, u otras).

[431] C.M. Romeo Casabona, *Las Transformaciones del Derecho penal en un mundo en cambio (Volumen II)*, 1ª ed., Arequipa, Adrus, 2004, p. 565. La ajenidad es un elemento fundamental de este tipo delictivo.

informáticos, cuando el resultado producido sea grave[432] [433]. En ambos casos se específica que tanto la conducta como el resultado producido deben ser graves, excluyendo de este modo borrados superficiales y menoscabos leves de la información contenida en los soportes informáticos. La gravedad de resultado se refiere, en todo caso, al valor patrimonial del objeto material que ha sido objeto de los daños, toda vez que estos deben ser de tipo patrimonial[434].

Parte de la doctrina, no obstante, defiende que los intereses involucrados en este delito van más allá del patrimonio, y lamenta la falta de visión del legislador en relación con la importancia de la ciberseguridad como bien jurídico independiente que defienda la disponibilidad, la integridad y la confidencialidad de los sistemas informáticos o su equivalente resumido, la seguridad informática; así como la oportunidad perdida de regular este y otros delitos (197 bis 1 del CP) en un nuevo título del mismo, en lugar de ubicarlos en los títulos ya existentes. Y es que el objetivo final de este delito de daños informáticos es proteger tanto la información contenida en los sistemas informáticos como el correcto funcionamiento de los mismos, puesto que la mera quiebra del sistema de seguridad informática, con independencia del peligro que suponga para otros bienes jurídicos, tiene consecuencias inmediatas sobre el funcionamiento de empresas u organizaciones que podrían verse obligadas a cesar en su actividad hasta la subsanación del fallo, con los consiguientes costes directos (como el reemplazo del sistema de seguridad) e indirectos (como los reputacionales). En relación con estos últimos, son muchas las grandes empresas y las administraciones públicas que, habiendo sido víctimas de un ciberdelito, prefieren asumir los costes económicos del ataque antes que el coste reputacional que supondría admitir

[432] P. Guérez Tricarico, “Delitos patrimoniales y contra el orden socioeconómico. Sección 14. Daños”, en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1416 – 1417. En cuanto a los datos, son unidades de información, sin importar su número o combinación, así como la manera específica en la que se encuentran alojados dentro de un sistema de información.

[433] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 721.

[434] Muñoz Conde, *Derecho Penal, Parte Especial*, p. 462.

una vulnerabilidad de su sistema informático. Si a lo anterior se añaden las dificultades probatorias y la complejidad de la persecución penal extraterritorial de los daños más graves, hay un abismo entre lo que sucede en la realidad y los casos relevantes que llegan a los tribunales, abundando en los mismos los casos sucedidos en pequeñas o medianas empresas y llevados a cabo mediante herramientas no demasiado sofisticadas[435].

El objeto protegido es la información, ya se encuentre alojada en un soporte analógico o en uno virtual. Los datos informáticos a los que se refiere el tipo son unidades de información, sin importar su número o combinación, y la manera en la que se encuentran alojados en un sistema de información. Los programas, secuencias de instrucciones que se utilizan para procesar los datos con objeto de ejecutar aplicaciones específicas. Los documentos electrónicos, documentos cuyo soporte material es algún tipo de dispositivo electrónico y en el que el contenido está codificado mediante algún tipo de código digital susceptible de ser leído o reproducido con ayuda de detectores de magnetización. En cuanto a la información protegida, puede ser de distintos formatos, como un texto, y puede encontrarse en cualquier lugar de la memoria del sistema informático: la memoria caché, los discos duros u otros tipos de almacenamiento de memoria, e incluso puede estar borrada en apariencia después de uno o varios formateos del disco duro, siempre que cumpla la característica de poder ser recuperable mediante programas de recuperación de datos.

La conducta típica consiste en destruir, deteriorar, inutilizar o menoscabar sustancialmente una cosa, existiendo varias modalidades típicas de conducta: el borrado de programas, la sobreescritura o cifrado que impliquen inutilización, o la destrucción física del soporte en el que se encuentran alojados los datos mediante acciones como la perforación de un

[435] A. Gil Gil, “Daños informáticos”, en E. Sanz Delgado y D. Fernández Bermejo (coords.), *Tratado de Delincuencia Cibernética*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021, pp. 467 – 471. Es posible encontrar la excepción a este criterio en la SAN 2034/2015, de 11 de junio (ECLI:ES:AN:2015:2034), en la que se juzgó la infección mediante virus de 23.662 ordenadores con un coste estimado de reparación de 3.300.000 euros, pudiendo llegar hasta los 10.000.000 teniendo en cuenta los ordenadores infectados a nivel mundial.

disco duro. Las facetas de la ciberseguridad indudablemente afectadas por este delito son la disponibilidad y la integridad, dependiendo de la modalidad típica de conducta que concurra en cada caso concreto: mientras que la destrucción o la inutilización total de un sistema afecta a su disponibilidad, el deterioro o la inutilización parcial del mismo afecta a su integridad. Es imperativo introducir, en este sentido, una distinción: en los ataques contra el *hardware*, orientados a la destrucción física del continente o soporte material del sistema informático, los daños se castigarían a través del art. 263 del CP, destinado a proteger la seguridad física o seguridad del *hardware* (tanto es así, que las conductas que solo afectan al *hardware* no están contempladas en la Directiva 2013/40/UE)[436]*.* En los ataques lógicos, el medio utilizado carece de importancia, incluyendo tanto la infección con virus, gusanos o bombas informáticas como la utilización de métodos informáticos como el *phishing*, el *spyware*, el *rootkit*, el *ransomware*[437] [438] [439] o cualquier tipo de

[436] Gil Gil, *Tratado de Delincuencia Cibernética*, p. 472.

[437] E. Cartwright, J. Hernández de Castro y A. Cartwright, "To pay or not: game theoretic models of ransomware", *Journal of Cybersecurity*, vol. 5, no. 1, 2019, pp. 10 – 11. Existen, en relación con el *ransomware,* elaborados estudios sobre aspectos como las acciones más ventajosas para la víctima. De los mismos pueden extraerse importantes conclusiones para el Derecho penal, como que en este ámbito solo es posible disuadir a los criminales mediante un antivirus o una vigilancia personal casi perfectos.

[438] Gil Gil, *Tratado de Delincuencia Cibernética*, p. 479. El 4 de julio de 2021, la organización supuestamente rusa *REvil* (*Ransomware Evil*) lanzó un ataque que afectó a numerosas empresas de todo el mundo en lo que se ha calificado como el mayor ataque de *ransomware* de la historia. Una vulnerabilidad en el sistema de servicio de herramientas remotas de una empresa que daba servicio a las afectadas fue el medio para colar un *malware* destinado a encriptar su información bajo la apariencia de un paquete de actualización ordinario. La cantidad solicitada por los ciberdelincuentes fue de 70 millones de dólares en bitcoines.

[439] A. M.ª Esteban Ruiz, "El secuestro 2.0 en la era del Internet de las cosas: el *ransomware*", en F. Bueno De Mata (dir.), *Fodertics 6.0: los nuevos retos del derecho ante la era digital*, Granada, Comares, 2017, p. 135. Es necesario concienciarse sobre el deber de implantar unas medidas adecuadas de ciberseguridad.

malware[440] [441] [442] [443] para acceder ilícitamente a un sistema informático y alterar o destruir elementos contenidos en el mismo. Para determinar el lugar de la comisión de los hechos hay que acudir a la teoría de la ubicuidad, de acuerdo a la cual no importa el lugar desde el que se lanza el ataque, puesto que el delito, de acuerdo al ATS 3627/2013, de 12 de abril[444], se comete donde se producen los daños, donde se destruye el sistema operativo o donde se contaminan los archivos[445], es decir, no donde se lleva a cabo sino donde se perciben los efectos materiales del delito. En ausencia de resultado dañoso, el mero acceso constituye un delito contra la intimidad[446].

Por último, en lo concerniente a la perfección de este delito de resultado, es posible que aparezcan formas de ejecución imperfecta en las que la consumación del delito no llegue a producirse por motivos distintos a

---

[440] M. Medina y M. Molist, *Cibercrimen,* 1ª ed., Barcelona, Tibidabo, 2015, p. 37. Desde un punto de vista técnico, el *malware* no son solo los programas maliciosos, sino todos aquellos no deseados por el usuario. Se considera *malware*, incluso, a programas legales que ocupan espacio en el disco y ralentizan el tiempo de procesado sin que esto interese al usuario, como los que informan de actualizaciones disponibles para aplicaciones que no se utilizan, por mucho que estos, por sus características, no encajen en el tipo delictivo.

[441] L.Y. Connolly y D.S. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures", *Computers & Security,* vol. 87, 2019, p. 14. El *criptoransomware*, que se ha convertido en una significativa amenaza estos últimos años, se caracteriza por el cifrado de los archivos de la víctima y la solicitud del pago de una cantidad a cambio de volver a proporcionar acceso a los mismos.

[442] F. Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio,* 1ª ed., Madrid, Marcial Pons, 2012, p. 64. El hecho de que el art. 264.1 del CP admita cualquier medio para la comisión del delito hace que se pueda llevar a cabo el mismo, además de utilizando virus o *malware*, mediante el aprovechamiento de las vulnerabilidades existentes tanto a través de los ataques DoS como de su evolución, los ataques DDoS, que consisten en el ataque coordinado de distintas máquinas a una sola víctima, teniendo esto un peligro mucho mayor por complicar las estrategias defensivas del servidor o sistema atacados. Además, en la actualidad, la infección de *bots* hace posible el uso de una red de ordenadores (o *botnet*) para llevar a cabo un ataque camuflado bajo la apariencia de un mensaje lícito.

[443] M.ª A. Rueda Martín, "Los ataques de denegación de servicios como ciberdelito en el Código Penal español", *Revista Penal*, no. 49, 2022, pp. 211 – 212. Específicamente en lo que se refiere a los ataques DoS, considera Rueda Martín que las deficiencias existentes en relación con los mismos no se encuentran en el ámbito de la regulación jurídico penal nacional, sino en la cooperación jurídica y judicial internacional.

[444] ECLI:ES:TS:2013:3627A.

[445] Guérez Tricarico, *Memento Práctico de Derecho Penal 2021*, p. 1417.

[446] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 721.

la voluntad del sujeto activo, como cuando el usuario detecta un virus y procede a su eliminación sin que cause daño alguno o tras haber producido un daño de muy escasa entidad. También son frecuentes los casos en los que transcurre un lapso de tiempo entre el inicio de la conducta y los resultados lesivos, como en el caso de las bombas lógicas, que se activan pasados días, semanas o meses. En estos casos, la ejecución del delito se produce cuando el comienzo de la destrucción no puede ser detenido por el autor, y la consumación con la producción del resultado previsto en el tipo, es decir, con el daño informático[447].

En caso de disponer de copias de seguridad de los datos, documentos o programas atacados, estaríamos únicamente ante una tentativa punible para un sector de la doctrina[448], ante hechos atípicos para otro sector[449], y ante un delito plenamente consumado para un tercero[450]. A pesar de que en

[447] N. J. De la Mata Barranco y L. Hernández Díaz, "El delito de daños informáticos: una tipificación defectuosa", *Estudios penales y criminológicos,* no. 29, 2009, pp. 352 – 353. En 2016, tuvo lugar en Pensilvania (EE. UU.) un caso en el que un informático instaló bombas lógicas en las hojas de cálculo de una gran empresa que solía requerir sus servicios. Cada varios días, estas se activaban, obligando a la empresa a solicitar su ayuda y pagarle. No obstante, una de las bombas lógicas se activó un día en que no pudo acudir a la llamada de la empresa y, cuando se vio obligado a entregar la contraseña de administrador a un técnico distinto, no tardó en descubrirse lo sucedido, estando castigados hechos como estos en EE. UU. con una pena de prisión de hasta diez años, una multa de un cuarto de millón de dólares, o ambas.

[448] C.M. Romeo Casabona, "Los delitos de daños en el ámbito informático", *Cuadernos de política criminal*, no. 43, 1991, p. 110. Esta valoración es lógica, dado que los daños los sufren meras copias de los originales.

[449] Velasco Núñez, *Delitos tecnológicos*, pp. 87 – 88. La STS 220/2020, de 22 de mayo (ECLI:ES:TS:2020:1520) inclina la balanza, en cierto modo, a favor de este sector doctrinal, ya que cuando es posible la recuperación de los archivos borrados se considera que ni siquiera existe un delito de daños informáticos del art. 264.1 del CP en grado de tentativa (art. 16.1 del CP), puesto que los hechos no alcanzan a colmar los elementos esenciales que exige el tipo delictivo a causa de la falta de gravedad tanto en la acción como en el resultado: dos gravedades encadenadas y acumulativas sin las cuales no hay delito. Al no operar esta doble gravedad, el resultado es que los daños informáticos resultan atípicos. Hay que aclarar que el TS no relaciona la gravedad con criterios cuantitativos como el hipotético coste de una reparación, sino con el entorpecimiento y perturbación que sufre el sistema informático. La gravedad sí se apreciaría en los casos en que resultase imposible recuperar la plena operatividad del sistema o en los que la puesta en marcha del mismo exigiese grandes esfuerzos de dedicación tanto técnica como económica.

[450] Distinto es el parecer de M.J. Rodríguez Mesa, *Los delitos de daños: Capítulo IX del Título XIII del CP tras la reforma de la LO 1/2015,* 1ª ed., Valencia, Tirant lo Blanch, 2017, pp. 75 y 76, para quien la consumación del delito tiene lugar cuando se produce

dicho caso decantarse por la tentativa relativamente inidónea, punible, es la opción más viable, no sucedería lo mismo en caso de eliminarse los datos de un fichero informático de especial importancia para el adecuado funcionamiento de una empresa cuando su copia no se encontrara en la misma sede física donde hubiese tenido lugar la eliminación o, incluso, cuando la enorme cantidad de datos eliminados requiriese para su reimplantación una cantidad de tiempo que paralizara la actividad de la empresa durante la misma. Sería factible apreciar la tentativa cuando, partiendo del supuesto anterior, la reimplantación de las copias pudiese ser efectiva en un breve espacio de tiempo[451].

El art. 264.2 del CP contempla cinco agravaciones para este delito, castigándolas con la pena de prisión de 2 a 5 años y multa de tanto al décuplo del perjuicio ocasionado: primera, su comisión en el marco de una organización criminal; segunda, que el mismo haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos; tercera, que haya perjudicado de forma grave el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad; cuarta, que haya afectado al sistema informático de una infraestructura crítica o se haya creado una situación de peligro grave para la seguridad del Estado, de la UE o de un Estado miembro de la UE; quinta, la utilización para la comisión del delito de un programa informático concebido o adaptado principalmente para ello o una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a un sistema de información, total o parcialmente. Por infraestructura crítica hay que entender un elemento, sistema o parte de este que es esencial para el mantenimiento de funciones vitales de la sociedad, como la salud o la seguridad, teniendo su perturbación o destrucción un impacto significativo al no poder mantener sus funciones. El

el borrado, y en cualquier caso siempre antes de la restauración de la copia de seguridad. Así, la hipotética existencia de una copia de seguridad solo sería relevante en la fase de agotamiento del delito, y únicamente para la graduación de la pena a imponer.

451 De la Mata Barranco y Hernández Díaz, “El delito de daños informáticos: una tipificación defectuosa”, pp. 353 – 354.

art. 264.2, en su párrafo segundo, incluye una agravación facultativa para los casos en los que los hechos resultan de extrema gravedad, en cuyo caso puede imponerse la pena superior en grado: una pena de prisión de 5 a 7 años más la multa proporcional. Su extraordinaria amplitud y la pena resultante ha hecho que SsTC como la 136/1999 se planteen su constitucionalidad, puesto que vulneran el principio de proporcionalidad y las consideraciones en este sentido de la mayoría de la doctrina penal, sobre todo en lo que concierne a la dificultad para cuantificar una multa proporcional en relación con este delito[452].

El art. 264 bis incluye un tipo básico mixto alternativo y varios subtipos agravados, castigando con la pena de prisión de 6 meses a 3 años a quien, en ausencia de autorización y de manera grave, obstaculice o interrumpa el funcionamiento de un sistema informático ajeno realizando alguna de las conductas de daños informáticos del art. 264, introduciendo o transmitiendo datos o destruyendo, dañando inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Se trata de un delito de mera actividad que se consuma con la realización de cualquiera de las modalidades típicas previstas. Existe la posibilidad de imponer la pena en su mitad superior a los casos en los que se perjudique de manera relevante la actividad normal de una empresa, negocio o Administración pública, siendo la duración de la pena resultante de 3 a 4 años y medio. Por último, el art. 264 bis 3 prevé la imposición de la pena en su mitad superior en los casos en los que concurra alguna de las cinco modalidades agravatorias del delito de daños informáticos, lo que se traduciría en una pena de prisión de 3 a 8 años y una multa del triplo al décuplo del perjuicio ocasionado y que resulta criticable por los motivos ya expuestos en relación con la agravación facultativa del párrafo segundo del art. 264.2.

En último lugar, el art. 264 ter recoge un delito de anticipación: la utilización de programas o contraseñas preordenados a la comisión de los

[452] Guérez Tricarico, *Memento Práctico de Derecho Penal 2021*, p. 1418.

delitos de daños informáticos. Se trata de un tipo mixto alternativo que castiga con una pena de prisión de 6 meses a 2 años o multa de 3 a 18 meses a la persona que, sin estar debidamente autorizada, produzca, adquiera para su uso, importa o, de cualquier modo, facilite a terceras personas, con intención de facilitar la comisión de los delitos previstos en los arts. 264 y 264 bis del CP, un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren dichos artículos, o bien una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a un sistema de información, total o parcialmente. Cuando, utilizando estos medios comisivos, el sujeto activo realiza alguno de los delitos de los arts. 264 y 264 bis, el concurso de leyes resultante debe resolverse a favor de los mismos, atendiendo al principio de subsidiariedad del art. 8.2 del CP. Las elevadas penas previstas para estos delitos principales de los arts. 264 y 264 bis hace aconsejable, atendiendo al principio de inherencia, la aplicación de un concurso de leyes, incluso cuando subsista algún riesgo para otros sistemas informáticos que no han sido dañados[453].

3.3.2.2.5 Conductas relacionadas con la superación de dispositivos de protección en los delitos relativos a la propiedad intelectual

Los delitos de los arts. 270.5, párrafos c) y d), y 270.6 del CP tienen una escasa aplicación jurisprudencial, y suponen una manifestación evidente del incremento de la represión penal en relación con la propiedad intelectual[454]. Resulta especialmente criticable la tipificación de conductas muy alejadas de la concreta lesión de los derechos de propiedad intelectual que no son sino actos preparatorios de posteriores comportamientos recogidos en el tipo básico, recibiendo, además, una pena similar a la de estos y valorando como ya efectiva la vulneración del bien jurídico protegido mediante la elevación de dichos actos preparatorios a la categoría de delito

[453] Guérez Tricarico, *Memento Práctico de Derecho Penal 2021*, p. 1419.
[454] Romeo Casabona, *Poder informático y seguridad jurídica*, p. 144.

autónomo[455]. Las conductas típicas recogidas en el art. 270.5 que afectan a la ciberseguridad son dos: primera, favorecer o facilitar la realización de las conductas de los arts. 270.1 y 270.2 del CP mediante la eliminación o modificación, sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, de las medidas tecnológicas eficaces incorporadas por estos con la finalidad de impedir o restringir su realización (párrafo c) del art. 270.5); segunda, eludir o facilitar la elusión de las medidas tecnológicas eficaces dispuestas para evitarlo con ánimo de obtener un beneficio económico directo o indirecto, sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, y con la finalidad de facilitar a terceros el acceso a un ejemplar de una obra literaria, artística o científica, o a su transformación, interpretación o ejecución artística, fijada en cualquier tipo de soporte o comunicada a través de cualquier medio (párrafo d) del art. 270.5) [456]. Por último, el art. 270.6 del CP castiga la fabricación, importación, puesta en circulación o incluso mera tenencia de medios principalmente[457] destinados a superar dispositivos de protección de obras con un fin comercial[458]. A la dificultad para encajar conductas concretas y reales en estos artículos se suman críticas incontestables como lo

[455] C.M. Romeo Casabona, "De los delitos informáticos al cibercrimen", en F. Pérez Álvarez (edit.), *Universitas vitae. Homenaje a Ruperto Núñez Barbero*, 1ª ed., Salamanca, Ediciones Universidad de Salamanca, 2007, p. 660. Esta discutible decisión político-criminal procede del Derecho comunitario. Sobre este particular, véase también C.M. Romeo Casabona, "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político criminal", en C.M. Romeo Casabona (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, Comares, 2006, pp. 1 – 42.

[456] C. Tomás-Valiente Lanuza, "Delitos patrimoniales y contra el orden socioeconómico. Sección 15. Delitos relativos a la propiedad intelectual", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1430 – 1431. El avance de la tecnología y los cambios en las necesidades relativas a la ciberseguridad hacen inevitable la desactualización de estos artículos del CP.

[457] Cámara Arroyo et al., *Cibercriminalidad*, p. 261. En la reforma del CP del año 2015 se sustituyó la expresión "medio específicamente destinado" por la de "medio principalmente destinado", ampliando así el ámbito penal de manera poco concreta y comprensible más allá de evitar que un dispositivo creado para inutilizar o neutralizar un sistema de protección pero dotado, además, de otras utilidades añadidas, impida la aplicación del tipo penal con la excusa de no haberse concebido exclusivamente para ese propósito.

[458] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 727.

inadecuado de que para los delitos de los párrafos c) y d) del art. 270.5 del CP se prevean penas equivalentes a las de las conductas que realmente vulneran el derecho de propiedad intelectual o, en relación con el art. 270.6, que se castigue con hasta tres años de prisión la mera tenencia de dispositivos de elusión aunque no se utilicen, o su indeterminación del ámbito de lo punible tras la modificación conceptual realizada por la LO 1/2015[459], especialmente sabiendo que solamente se pone en peligro, pero no se lesiona, el patrimonio del titular, bien jurídico que pretenden proteger estos delitos[460].

Incluso teniendo en cuenta que suponen una cesión a los grupos de presión defensores de la máxima intervención en materia de propiedad intelectual[461], estas conductas constituyen, sin duda, el elemento más anacrónico relacionado con la ciberseguridad en el ordenamiento jurídico-penal español, puesto que están pensadas para una forma de protección de la propiedad intelectual basada, por lo general, en la adquisición de un *hardware* cuyo contenido estaba protegido por medidas establecidas para tal fin. En la actualidad, los usuarios adquieren directamente el *software* a través de licencias, ya se trate de programas o de material artístico de distintas clases sujeto a propiedad intelectual. Las tiendas en línea de las empresas que ponen a disposición de los usuarios esta clase de *software* tienden a estar protegidas por unas medidas de ciberseguridad adecuadas, pero resulta

[459] N.J. De la Mata Barranco, "Delitos contra la propiedad intelectual e industrial y violación de secretos de empresa", en N.J. De la Mata Barranco et al. (autores), *Derecho penal económico y de la empresa,* Madrid, Dykinson, 2018, pp. 339 – 340. La STJUE de 23 de enero de 2014 determinó la legalidad de la elusión de un sistema de protección siempre que su uso previsto sea exclusivamente personal y no afecte de ninguna manera a los derechos de autor. La decisión del TJUE se contrapone con la SAP de Cádiz de 23 de mayo de 2013, que sí condenó la puesta en circulación de la tecnología necesaria para conseguir dicha elusión.

[460] M.ª D. C. Gómez Rivero, *Los delitos contra la propiedad intelectual e industrial. La tutela penal de los derechos sobre bienes inmateriales*, 1ª ed., Valencia, Tirant lo Blanch, 2012, p. 141. Basta con una conducta tan lejana de la lesión al bien jurídico como la producción de estos medios para sufrir el reproche penal.

[461] J.G. Fernández Teruelo, *Cibercrimen: los Delitos Cometidos a Través de Internet*, 1ª ed., Madrid, Constitutio Criminalis Carolina, 2007, p. 103. Ya en sus orígenes se trató de un exagerado adelanto de la intervención del Derecho penal que suponía una clara vulneración del principio de proporcionalidad.

muy difícil, en la práctica, la persecución de la eliminación de las medidas que impiden duplicar y transmitir a terceros un determinado *software* una vez se ha adquirido de manera legal. Tanto es así que determinadas empresas discográficas han decidido adelantarse a las acciones de los ciberdelincuentes y ya liberan por sí mismas las obras sujetas a propiedad intelectual al comprender el inevitable cambio tecnológico ocurrido, que otorga a cualquier usuario la posibilidad o bien de incurrir en la conducta típica o bien, sobre todo, de hacerse con un material que, sin ningún remedio, va a ser liberado y puesto a disposición de los usuarios de Internet. En este sentido, las discográficas han sido pioneras al entender que la tecnología ha cambiado su negocio, debiendo renovar la manera en que ofrecen sus productos a los usuarios con objeto de hacer poco atractivas las copias ilegales y de ofrecer beneficios adicionales a quienes respetan la legalidad y acceden a sus productos respetando las medidas de seguridad, como una atención al cliente de alto nivel. Medidas, todas ellas, que por coherencia pertenecen al ámbito extrapenal, incluyendo la posible imposición de unas sanciones más relacionadas con figuras de Derecho civil como el lucro cesante que con la protección de bienes jurídicos que corresponde al Derecho penal.

3.3.2.2.6 Descubrimiento y revelación de secretos de empresa

Los secretos empresariales se protegen en los arts. 278 a 280 del CP. Si bien el CP no define qué es un secreto empresarial[462], la doctrina y la jurisprudencia han adoptado la definición utilizada en el ámbito civil añadiéndole el requisito de la licitud, es decir, la exigencia de que la actividad sea legal para poder ser penalmente protegida, requisito respaldado por la STS 285/2008, de 12 de mayo[463]. El AAP de Madrid 261/2019, de 29 de

[462] A. Doval País, "La intimidad y los secretos de empresa como objetos de ataque por medios informáticos", *Eguzkilore*, no. 22, 2008, p. 115. En este sector de delitos, es notoria la indefinición de conceptos fundamentales, entre los que destacan los propios "secretos de empresa". Lo principal es que la información resulte valiosa por su carácter exclusivo o por ser el resultado de notables inversiones de dinero y de tiempo.

[463] ECLI:ES:TS:2008:2885.

marzo[464], sostiene, apoyándose en la mencionada sentencia, que los secretos de empresa son los propios de la actividad empresarial que, de ser conocidos contra la voluntad de la empresa, podrían afectar a su capacidad competitiva. Estos delitos, cuyo bien jurídico protegido es la capacidad competitiva de la empresa, se consideran delitos de peligro, consumándose por poner en riesgo la capacidad competitiva de la empresa, incluso cuando no existe aún un daño específico[465]. El tipo básico del art. 278 del CP consiste en el acceso ilícito a la información secreta, ya sea apoderándose de ella o mediante el control de las señales de comunicación y el control audiovisual ilícitos. En cuanto al apoderamiento, el art. 278.1 castiga con una pena de dos a cuatro años de cárcel y una multa de doce a veinticuatro meses a quien, para descubrir un secreto de empresa[466], se apodere por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al secreto empresarial. El apoderamiento supone la apropiación de la información secreta, yendo la conducta típica más allá de la obtención de su soporte material, y llegando incluso a su memorización o cualquier otra técnica para la captación mental o intelectual de dicha información[467]. Como delito de actividad, se consuma por el simple hecho de apropiarse ilícitamente de esta, con independencia de que el sujeto activo

[464] ECLI:ES:APM:2019:1645A.

[465] A. Benetó Santa Cruz y L. Cachón Marinello, "La creciente importancia de proteger los secretos comerciales", en J. Velázquez (coord.), *Cuadernos de Derecho para ingenieros: ciberseguridad,* Las Rozas, Madrid, Wolters Kluwer, 2017, pp. 243 – 244. Es importante tener en cuenta, en relación con este delito en particular, la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas. En su exposición de motivos resalta el valor de los secretos comerciales al reconocer que son una de las formas más comunes de proteger la innovación, a pesar de lo cual están muy poco protegidos contra la actuación ilícita por parte de terceros. Su finalidad principal fue la homogeneización de normas relativas a la protección de secretos comerciales entre Estados miembros, atendiendo a los niveles de protección dispares que existían. El 9 de junio de 2018 concluyó el plazo para incorporar sus disposiciones a los respectivos ordenamientos jurídicos de los Estados miembros.

[466] C. Martínez-Buján Pérez, *Derecho penal económico y de la empresa*, 1ª ed., Valencia, Tirant lo Blanch, 2013, p. 145. El tipo, además de ser doloso, incorpora también este elemento subjetivo del injusto.

[467] Benetó Santa Cruz y Cachón Marinello, *Cuadernos de Derecho para ingenieros: ciberseguridad,* p. 244.

tome conocimiento efectivo de la misma. El art. 278.3 prevé la apropiación o destrucción de soportes informáticos, en cuyo caso será posible apreciar también la existencia del delito correspondiente siempre que la apropiación o destrucción afecte a soportes informáticos y no a documentos, muestras o prototipos, por muy criticado que haya sido este matiz[468].

El art. 278.1 del CP castiga también, por remisión al art. 197.1 del mismo texto, la interceptación de las telecomunicaciones o la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, siempre que estas acciones tengan como objetivo descubrir secretos empresariales[469]. La pena para este delito es idéntica a la prevista para el apoderamiento[470].

El art. 278.2 del CP recoge el tipo agravado, que consiste en difundir, revelar o ceder a terceros el secreto empresarial descubierto, y se castiga con una pena de tres a cinco años de cárcel y una multa de doce a veinticuatro meses[471]. El sujeto activo debe ser quien se apropió de manera ilegítima de la información[472]. La tentativa, desde un punto de vista conceptual, es posible, pero un sector mayoritario de la doctrina considera que es más adecuado condenar por el delito básico consumado (la apropiación) que por el delito agravado en grado de tentativa (la revelación frustrada), y esto porque la pena resultante del delito agravado en grado de tentativa resultaría inferior a la pena del delito básico consumado, lo que supone un sinsentido desde una perspectiva de justicia material.

---

[468] Benetó Santa Cruz y Cachón Marinello, *Cuadernos de Derecho para ingenieros: ciberseguridad,* p. 245.

[469] C. Martínez-Buján Pérez, *Delitos relativos al secreto de empresa*, 1ª ed., Valencia, Tirant lo Blanch, 2010, pp. 52 – 53. Estos secretos deben ser evaluables económicamente y resultar idóneos para comportar ventajas competitivas. Basta, por otro lado, con el mero deseo de conocerlos por parte del ciberdelincuente.

[470] Benetó Santa Cruz y Cachón Marinello, *Cuadernos de Derecho para ingenieros: ciberseguridad,* pp. 245 – 246.

[471] Benetó Santa Cruz y Cachón Marinello, *Cuadernos de Derecho para ingenieros: ciberseguridad,* p. 246.

[472] Benetó Santa Cruz y Cachón Marinello, *Cuadernos de Derecho para ingenieros: ciberseguridad,* pp. 246 – 247.

Igual que sucedía con los arts. 197 y sucesivos del CP[473], estos delitos obligan a analizar la existencia y naturaleza de las medidas de seguridad informática interpuestas entre el ciberdelincuente y la información que se pretende proteger, es decir, si existen o no medidas de ciberseguridad y, en caso afirmativo, cómo afectan al Derecho penal[474]. Hay que partir de la base de que el titular de la información goza de una posición legítima de dominio sobre un secreto empresarial, y que ha establecido, para su protección, unas barreras adecuadas a este objetivo. Es inspiradora la redacción del proyecto alternativo del CP alemán del año 1977, cuyo parágrafo 180, apartado tercero, incluía en la conducta típica la superación de medidas de protección, estableciendo un equilibrio entre las necesidades de prevención y las garantías al reo[475] y asegurando que solo las conductas más graves fuesen constitutivas del tipo penal. No obstante, hay que considerar que aceptar la superación de las barreras de protección como criterio de relevancia penal supuso introducir un criterio amplio y, al mismo tiempo, una barrera de

[473] P. Gómez Pavón, "Capítulo 5. Los delitos de descubrimiento y revelación de secretos de empresa", en P. Gómez Pavón, M. Bustos Rubio, y D. Pavón Herradón (autores), *Delitos Económicos. Análisis doctrinal y jurisprudencial. Adaptado a la LO 1/2019, de 20 de febrero, por la que se modifica la LO del CP, para transponer Directivas de la UE en los ámbitos financieros y de terrorismo,* 1ª ed., Madrid, Wolters Kluwer, 2019, p. 135. El acceso ilícito al secreto debe ser buscado a propósito por parte del sujeto activo del delito.

[474] A. Salvador Cerqueda, "Gestión de incidentes de seguridad desde la perspectiva de la protección de datos y los secretos empresariales", en S. Pereira Puigvert y F. Ordoñez Ponz (dirs.), *Investigación y proceso penal en el siglo XXI. Nuevas tecnologías y protección de datos*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021, pp. 371 – 372. Para reconocer a una información o conocimiento la categoría de secreto empresarial, el art. 1.c) de la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, introdujo la obligación de establecer medidas razonables por parte de su titular para mantenerlos en secreto. Entre dichas medidas se encuentran, sin dudas, las relativas a la ciberseguridad. Solo habiendo establecido una adecuada barrera de seguridad informática en torno a una determinada información o conocimiento se la podrá considerar como secreto de empresa y pretender, por tanto, su protección mediante el Derecho penal.

[475] A. Estrada i Cuadras, *Violaciones de secreto empresarial. Un estudio de los ilícitos mercantiles y penales*, 1ª ed., Barcelona, Atelier, 2016, p. 81. Creo que resultaría mucho más garantista que, siguiendo la inspiración de la mencionada corriente de pensamiento alemana, se incluyesen de manera específica en el tipo delictivo correspondiente del CP español las medidas de ciberseguridad establecidas por el titular.

contención del tipo que impidió su desbordamiento por una excesiva inclusión provocada por la total apertura de los medios de comisión[476].

El tipo delictivo del art. 278 del CP no incluye de manera literal la obligación de que existan medidas de ciberseguridad entre los ciberdelincuentes y la información a proteger, incluso cuando una mayoría de la doctrina y de la jurisprudencia estadounidenses las exige, incluso en el ámbito jurídico-penal. Su naturaleza dogmática es más discutible, toda vez que en ocasiones se las considera como un requisito configurador autónomo del concepto de secreto empresarial, mientras que otras veces se las considera un supuesto normativo del requisito del carácter secreto de la información, e incluso como una manifestación necesaria de la voluntad de mantener la información bajo secreto. La única forma coherente de exigir medidas de autoprotección al titular de la información como vía para restringir el correspondiente régimen jurídico de protección es considerar la adopción de estas medidas como un elemento configurador de la conducta típica también en el CP español[477].

El art. 279 del CP castiga la misma conducta de difundir, revelar o ceder a un tercero un secreto empresarial, solo que en este caso el sujeto activo debe estar sometido a una obligación legal o contractual de guardar reserva, siendo la pena prevista de dos a cuatro años de cárcel y de doce a veinticuatro meses de multa. Cuando el sujeto utilice el secreto empresarial en su propio provecho, el CP prevé una atenuación de la pena, que se impondrá en su mitad inferior[478]. De acuerdo a la STS 285/2008, de 12 de mayo, solo pueden ser autores de este delito quienes están obligados por una exigencia expresa a guardar en secreto la información empresarial, como los administradores, el resto de empleados que conocen el secreto por razón de sus funciones, los trabajadores de empresas distintas que se relacionan con la titular del secreto y los terceros que lo hayan conocido por causas legales,

[476] Estrada i Cuadras, *Violaciones de secreto empresarial*, p. 82.

[477] Estrada i Cuadras, *Violaciones de secreto empresarial*, p. 83.

[478] Benetó Santa Cruz y Cachón Marinello, *Cuadernos de Derecho para ingenieros: ciberseguridad,* p. 247.

como los funcionarios. Las demás personas implicadas solo pueden ser cooperadoras: inductoras, cooperadoras necesarias o cómplices, dependiendo del caso[479].

El CP no especifica el tiempo durante el que perdura la obligación de guardar el secreto, pero la doctrina mayoritaria sostiene que perdura durante tanto tiempo como esté en condiciones de aportar un valor económico. De ser necesario, eternamente. Este criterio evita que se vacíe de contenido el art. 279 mediante el desarrollo de estrategias o abusos.

El delito se consuma con la comunicación a terceros de la información confidencial, sin importar si toman conocimiento efectivo de la misma o no. Cuando esta información se usa en provecho propio, la consumación coincide con su efectiva utilización. Son posibles la formar imperfectas de ejecución, tanto las tentativas acabadas como las inacabadas y es posible cometer este delito por omisión cuando haya una intencionalidad de comunicar la información confidencial a través del actuar pasivo[480]. Lo que no resulta posible es su comisión por negligencia, siendo atípica la divulgación por descuido de esta información.

Por último, el art. 280 del CP castiga con una pena de cárcel de uno a tres años y una multa de doce a veinticuatro meses a quien, conociendo su origen ilícito y sin haber tomado parte en su descubrimiento, lleva a cabo alguna de las conductas descritas en los arts. 278 y 279. A través del mismo, se busca castigar las divulgaciones en cadena persiguiendo a las personas que, sin haber participado en el descubrimiento de la información confidencial, la difunden siendo conscientes de su origen ilícito. En ausencia de dicho conocimiento, la conducta se considera atípica. Igual que en los artículos anteriores, es posible apreciar la existencia de formas imperfectas

[479] Benetó Santa Cruz y Cachón Marinello, *Cuadernos de Derecho para ingenieros: ciberseguridad,* pp. 247 – 248.

[480] Benetó Santa Cruz y Cachón Marinello, *Cuadernos de Derecho para ingenieros: ciberseguridad,* p. 248.

de ejecución cuando la difusión de la información confidencial se produce por razones ajenas a la voluntad del sujeto[481].

Resulta recomendable, en el ámbito empresarial, el desarrollo de un Plan de Prevención de Delitos, pues permite si no la exención de responsabilidad sí al menos la atenuación de la responsabilidad por los actos cometidos por el personal y por los directivos, ya sea en su propio beneficio o en el de terceras personas. A través de la dedicación de un apartado específico del mismo a los delitos que afectan a la ciberseguridad, es posible prevenir la comisión de actos ilícitos que puedan vulnerar los derechos de terceros o la pérdida de información esencial para el desarrollo de la actividad de la organización[482].

3.3.2.3 Ciberseguridad en los delitos contra la seguridad colectiva

3.3.2.3.1 Estragos

El art. 346 del CP castiga con una pena de prisión de 10 a 20 años a quien, provocando explosiones o utilizando cualquier medio de similar potencia destructiva, perturbe gravemente cualquier clase o medio de comunicación produciendo con ello un peligro para la vida o la integridad de las personas. Cuando los estragos no produzcan dicho peligro, la conducta se castigará con una pena de prisión de 4 a 8 años. Dentro de la enumeración casuística y cerrada de las conductas castigadas, dicha perturbación grave resulta idónea para lesionar la disponibilidad de las redes informáticas, especialmente de Internet. Es posible castigar tanto la participación como la tentativa, siendo un delito que puede cometerse en comisión por omisión, y

[481] Benetó Santa Cruz y Cachón Marinello, *Cuadernos de Derecho para ingenieros: ciberseguridad,* p. 249.

[482] O. López Rodríguez, "Gestión de riesgos en protección de datos y seguridad de la información", en P. Simón Castellano y A. Abadías Selma (coords.), *Mapa de riesgos penales y prevención del delito en la empresa*, 1ª ed., Madrid, Wolters Kluwer, 2020, pp. 256 – 257. La introducción del Plan de Prevención de Delitos en la empresa disminuye también la posibilidad de que sus trabajadores transgredan las leyes.

en relación con el cual se castigan tanto la modalidad dolosa (ya sea el dolo directo o eventual, siempre que abarque el riesgo para la vida o la integridad de las personas) como la imprudencia grave. El hecho de que el delito de estragos sea un tipo mixto de resultado (por los daños materiales) y de peligro (en lo que concierne a la vida o la salud de las personas) resulta fundamental en relación con el capítulo cuarto de esta investigación, puesto que cuando los estragos que afectan a la disponibilidad de las redes informáticas, además del peligro, produzcan una lesión para la vida, la integridad física o la salud de las personas, el art. 346.3 del CP prevé que los hechos se castiguen separadamente con la pena correspondiente al delito cometido. Y es que, aunque el bien jurídico protegido es la seguridad colectiva, se protegen también, de manera mediata, la vida y la integridad de las personas. Cuando se lesionan, la jurisprudencia, como la STS 136/2006, de 15 de febrero[483], y parte de la doctrina coinciden en la necesidad de apreciar un concurso real entre el delito de estragos y el delito o los delitos de resultado lesivo[484]. Este concurso real se justifica por la naturaleza indeterminada del colectivo de personas cuya vida, integridad física o salud han sido puestas en peligro a causa de los estragos[485].

3.3.2.4 Ciberseguridad en los delitos de falsedades

3.3.2.4.1 Fabricación o tenencia de programas informáticos destinados a la comisión de estos delitos

[483] ECLI:ES:TS:2006:620.

[484] M. Maraver Gómez, "Delitos contra la seguridad colectiva. Sección 1. Delitos de riesgo catastrófico. B. Estragos", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1691 – 1693. En el siguiente capítulo de esta investigación ahondaré más en las relaciones concursales entre el delito de estragos y las lesiones sobre la vida o la salud de las personas.

[485] A.C. Andrés Domínguez, "Artículo 346", en M. Gómez Tomillo (dir.), *Comentarios prácticos al Código Penal. Tomo IV. Delitos contra el medio ambiente, el patrimonio histórico, la ordenación del territorio y contra la seguridad colectiva. Artículos 319 – 385 ter*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, p. 245.

El art. 400 del CP castiga la fabricación, recepción, obtención o tenencia de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad u otros medios que, de manera específica, estén destinados a la comisión de los delitos descritos en los arts. 390 y siguientes del mismo texto legal. Los objetos a los que hace referencia deben tener la aptitud y cualidad de estar específicamente destinados a la falsificación, no pudiendo tener ninguna otra utilidad normal. El delito se consuma con la disposición sobre dichos instrumentos sin que sea necesario saber cómo funcionan, puesto que el legislador, castigando la mera tenencia de útiles, pretende evitar que sean puestos a disposición de quien disponga del conocimiento técnico necesario para utilizarlos[486].

3.3.2.5 Ciberseguridad en los delitos contra la Administración pública

3.3.2.5.1 Infidelidad en la custodia de documentos y violación de secretos

Los arts. 413 a 418 del CP protegen la correcta preservación y utilización de determinado tipo de elementos e instrumentos que resultan esenciales para el cumplimiento de los fines de la Administración[487], como los documentos bajo su custodia y la información restringida o secreta de la que los funcionarios tienen conocimiento por razón de su cargo[488]. Al tiempo que se defiende la confidencialidad, se impide que nadie se aproveche de esta información, toda vez que su utilización con fines ajenos a la función pública

[486] Barja de Quiroga López, Encinar del Pozo, y Villegas García, *Código Penal*, pp. 1248 – 1249.

[487] E.R. Turner, *Public Confidence in Criminal Justice: A History and Critique,* 1ª ed., Londres, Palgrave Macmillan, 2018, p. 5. La confianza de la ciudadanía en la Administración de Justicia, especialmente en lo concerniente al Derecho penal, ha variado a lo largo de los siglos, y ha sido objeto de extensos estudios. A principios del siglo veintiuno, dejó de tratarse de una figura retórica para convertirse en algo real y medible.

[488] A. Delgado Gil, *Delitos cometidos por funcionarios públicos. Negociaciones prohibidas, actividades incompatibles y uso indebido de secreto o información privilegiada*, Valencia, Tirant lo Blanch, 2008, p. 233.

suponen una quiebra de su credibilidad. Con la excepción de los delitos de los arts. 414.2, 416 y 418 del CP, que son delitos comunes, las infracciones tipificadas son delitos especiales propios[489].

Atendiendo a la proliferación casi general de los medios electrónicos, es más que probable que la información a la que se tenga acceso esté almacenada en formato digital[490].

No obstante, solo algunos de estos preceptos afectan a la ciberseguridad. Y es que, igual que sucedía con distintos delitos comentados en otros títulos, no solo puede apreciarse una dudosa decisión del legislador en relación con la ubicación conjunta de los mismos, sino que se engloban conductas que carecen, entre sí, de la más mínima unidad o coherencia interna de contenidos que justifique su regulación conjunta más allá de su relación con la deslealtad de las autoridades y funcionarios públicos respecto del objeto de su función. En efecto, pese a su diversidad, en todas ellas el bien jurídico protegido es la confianza de los administrados en el cuidado y fidelidad en la custodia de los documentos por parte de los funcionarios públicos que la tienen encomendada, aunque, al mismo tiempo, se protegen también el propio contenido documental y los derechos que puedan extraerse del mismo[491].

De acuerdo con la STS 914/2003, de 19 de junio[492], se protege también la estricta confidencialidad de las informaciones de que dispone la Administración, que no deben ser aprovechadas por los funcionarios, entendidos como primeros custodios de la legalidad, so riesgo de suponer la quiebra de la credibilidad tanto en sí mismos como en las instituciones.

---

[489] L. Pozuelo Pérez, “Delitos contra la Administración pública. Sección 5. Infidelidad en la custodia de documentos y violación de secretos”, en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1886 – 1887. Aunque no se mencione la ciberseguridad en ninguno de estos tipos delictivos, resulta esencial para la actualización de artículos como el 415 del CP.

[490] M.ª P. Serrano Ferrer, *El reflejo de las nuevas tecnologías en el Derecho penal y otros destellos*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2016, p. 30. Esto, a pesar de la indefinición del arcaico art. 26 del CP.

[491] Pozuelo Pérez, *Memento Práctico de Derecho Penal 2021*, p. 1887.

[492] ECLI:ES:TS:2003:4269.

Teniendo esto en cuenta, es posible encontrar tres conductas típicas relacionadas con la ciberseguridad que, pese a ser alternativas, reflejan un voluntario incumplimiento por parte de un funcionario o autoridad de su deber de custodiar los documentos incorporados a los expedientes administrativos, o propios del uso de la Administración pública[493].

La primera y la principal es, sin duda, la inutilización de los medios establecidos para custodiar un documento del art. 414 del CP, el cual, a pesar de su mala redacción, tipifica las conductas de destrucción o neutralización de los medios utilizados para proteger documentos reservados respecto de los cuales la autoridad competente haya restringido el acceso, dejándolos accesibles a terceros no autorizados para su conocimiento sin importar que dicho acceso se produzca efectivamente o no. Al no mencionar el tipo delictivo característica alguna sobre la naturaleza de los medios, es posible deducir que puede tratarse tanto de medidas de seguridad físicas como lógicas, siempre que tanto las mismas como los datos protegidos tras ellas puedan incluirse dentro de las categorías exigidas por el tipo: la razón de ser de estos medios de protección atacados debe ser la protección de documentos que el funcionario o autoridad deba custodiar por razón de su cargo, y estos últimos han de haber sido objeto de una declaración expresa y formal de reserva por parte de otra autoridad. La conducta típica puede ser activa cuando el funcionario o autoridad destruya o inutilice personalmente los medios de protección[494], o pasiva cuando consienta que otras personas sean las que lleven a cabo las conductas prohibidas[495]. En cualquiera de las dos modalidades, lo que se persigue es el ataque a ciertas medidas de ciberseguridad establecidas específicamente para proteger información que encaje en la descripción típica. Se trata de castigar, en definitiva, cualquier ataque a la disponibilidad y a la integridad de estas medidas de seguridad,

[493] E. Mestre Delgado, "Tema 22. Delitos contra la Administración Pública", en C. Lamarca Pérez (coord.), *Delitos. La parte especial del Derecho penal*, 6ª ed., Madrid, Dykinson, 2021, p. 895.

[494] Serrano Ferrer, *El reflejo de las nuevas tecnologías en el Derecho penal y otros destellos*, p. 30.

[495] Mestre Delgado, *Delitos*, p. 896.

tengan naturaleza informática o no la tengan. Este delito puede cometerlo también un particular (art. 414.2 del CP) sin necesidad de acceder de manera efectiva a los documentos y sin acordarlo previamente con el funcionario o autoridad.

La segunda conducta típica consiste en el acceso no autorizado a documentos secretos del art. 415 del CP. Con la misma redacción deficiente del artículo antes analizado, el legislador abunda en la protección de los documentos reservados mediante una figura subsidiaria del tipo del art. 414 del CP, especial y de mera actividad (o inactividad, dependiendo del caso), mediante la que se castiga al funcionario o autoridad que. o bien accede por sí mismo a documentos secretos cuya custodia tenga encomendada por razón de su cargo, o bien permite, de manera consciente y en ausencia de autorización, el acceso de terceros a los mismos[496]. Se echa de menos, en este sentido, la específica mención en el tipo a lo que en la segunda de las conductas tipificadas aparece como evidente: deben existir ciertas medidas de seguridad informática que resulta imposible que el tercero traspase por sí mismo, de manera que solo pueda hacerlo ayudado por el funcionario o autoridad, siendo por completo innecesaria la intervención de este en caso contrario. Así, la redacción de este art. 415 del CP mejoraría si hiciese referencia a documentos secretos "y protegidos", encajando el resto de conductas relativas a información no protegida en las de mera divulgación de la misma por parte del funcionario o autoridad, mucho menos graves.

La tercera y última de las tres conductas relacionadas con la ciberseguridad es la desaparición física de un documento del ámbito material de custodia del funcionario o autoridad del art. 413 del CP. El tipo describe, a su vez, cuatro acciones alternativas: la sustracción, la destrucción, la inutilización o el ocultamiento del mencionado documento[497]. Se trata, por

[496] Mestre Delgado, *Delitos*, p. 897.

[497] C. Tomás-Valiente Lanuza, "Artículo 413", en M. Gómez Tomillo (dir.), *Comentarios prácticos al Código Penal. Tomo V. Delitos de falsedades, contra la Administración Pública y contra la Administración de Justicia. Artículos 386 – 471 bis*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, pp. 253 – 254. "Sustraer" supone desplazar el documento fuera de su esfera de custodia correspondiente; "destruir" significa deshacer su materialidad total o parcialmente; "inutilizar" suponía, cuando solo existían los

tanto, de una infracción especial y de resultado, de acuerdo con jurisprudencia como el ATS 635/2016, de 14 de abril[498], mediante la que el legislador buscar proteger los expedientes administrativos y el cumplimiento de las finalidades propias de los documentos incorporados a los mismos[499], o, en el ámbito de la ciberseguridad, la disponibilidad (en lo que se refiere a su sustracción, a su destrucción o a su ocultamiento) y la integridad (en lo referente a su inutilización, que, aunque puede ser parcial, encajará también en la disponibilidad cuando el grado de la misma pueda considerarse absoluto) de los datos contenidos en un sistema informático. Este precepto, como todos los anteriores, hace imperativa la actualización del art. 26 del CP, toda vez que la definición de documentos que incluye, aunque amplia, debe aceptarse ya como plenamente adaptada a los datos informáticos, sobre todo teniendo en cuenta el imparable y generalizado proceso de digitalización de una Administración cuyo contenido lógico el CP pretende proteger.

El art. 416 del CP, por su parte, castiga la comisión de cualquiera de los hechos descritos cuando el sujeto activo es un particular accidentalmente encargado del despacho o de la custodia de los documentos, ya sea por comisión del Gobierno o de las autoridades o funcionarios públicos a los que se les hayan confiado por razón de su cargo[500].

3.3.2.6 Ciberseguridad en los delitos contra la Constitución

documentos en formato físico, también su destrucción en la práctica totalidad de los casos, pero con la llegada de los documentos informáticos cobró sentido su mención individualizada, toda vez que estos sí pueden inutilizarse sin destruirse; "ocultar", por último, abarca mucho más que esconder el documento donde no pueda ser hallado, sino que incluye tanto la paralización de su tramitación como la dilatación indefinida de la presencia del documento impidiendo que alcance los fines que corresponden a su contenido y su destino. Nos encontramos, en cualquiera de los cuatro casos, ante la vertiente de la ciberseguridad dedicada a la protección no de los sistemas informáticos en sí, sino de su contenido, frente a conductas que afectan desde a la integridad de los datos informáticos (inutilización) hasta su disponibilidad (destrucción).

[498] ECLI:ES:TS:2016:3566A.

[499] Mestre Delgado, *Delitos*, p. 895.

[500] Pozuelo Pérez, *Memento Práctico de Derecho Penal 2021*, p. 1889.

3.3.2.6.1 Delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad

Los arts. 534 a 536 del CP sancionan los comportamientos de autoridades o funcionarios públicos que, durante la investigación de un delito, se exceden en la manera en que pretenden obtener información para la misma[501]. Algunas de estas conductas resultan idóneas para lesionar la ciberseguridad. Es el caso del registro de los efectos de una persona que se encuentre en su domicilio sin consentimiento de la misma (art. 534.1.2), puesto que, al tratarse del conjunto de cosas de su propiedad, pueden encuadrarse en dicho término objetos como un ordenador, cuya confidencialidad deja de estar garantizada. La pena prevista es una multa de 6 a 12 meses, además de otra de inhabilitación especial para empleo o cargo público de 2 a 6 años. Además, en caso de que no devolver de manera inmediata los efectos registrados a su dueño, las penas serían una multa de 12 a 24 meses y la inhabilitación especial para empleo o cargo público de 6 a 12 años, sin perjuicio de la pena que pudiese corresponder por la apropiación cometida. Otra de las conductas es la causación de daños innecesarios con ocasión del registro lícito del art. 534.2, que sanciona los comportamientos abusivos que afecten a los bienes de las personas cuyo domicilio se está investigando, causándoles daños innecesarios. Esta conducta resulta idónea para lesionar la disponibilidad o la integridad de un sistema informático. La consecuencia jurídica es la pena prevista para este mismo hecho impuesta en su mitad superior, a la que hay que añadir una pena de inhabilitación especial para empleo o cargo público de 2 a 6 años[502].

El art. 535 del CP castiga la interceptación de correspondencia privada, siendo el bien jurídico protegido la intimidad de la correspondencia privada,

[501] Juanes Peces, *Comentarios al Código Penal*, p. 1561.

[502] L. Pozuelo Pérez, "Delitos contra la Constitución. Sección 6. Delitos cometidos por funcionarios públicos contra las garantías constitucionales", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 2025 – 2026. De nuevo, la (relativa) antigüedad de estos delitos en el CP hace que se utilicen términos poco relacionados con los sistemas de información, pero las conductas típicas no dejan lugar a dudas de que lo que se pretende proteger también es la ciberseguridad.

como los correos electrónicos. Esta conducta afecta a la ciberseguridad de una determinada red informática, y más específicamente a su confidencialidad. Por tanto, la pena prevista es la inhabilitación especial para empleo o cargo público de 2 a 6 años, pena que se impondrá en su mitad superior junto a una pena de multa de 6 a 18 meses si la información obtenida se divulga o revela a un tercero. En último lugar, el art. 536 tipifica la conducta consistente en interceptar las telecomunicaciones o utilizar artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación violando las garantías legalmente establecidas. El bien jurídico protegido es la intimidad, solo que en este caso en sentido amplio, y las penas previstas, al igual que la manera en que la conducta afecta a la ciberseguridad de una red informática, son idénticas a las del art. 535 del CP[503].

Es importante que las autoridades o funcionarios públicos actúen de acuerdo con las normas, toda vez que en caso contrario podría plantearse la nulidad de las pruebas obtenidas, que hubiesen podido resultar útiles para el esclarecimiento de los hechos[504].

El artículo 536 del CP tipifica la interceptación de comunicaciones o la utilización de artificios técnicos de escucha, grabación o reproducción por parte de agentes públicos mediante causa legal por delito cuando media violación de las garantías constitucionales o legales, es decir, cuando la autoridad o funcionario público se extralimita gravemente en el curso de una investigación judicial. La información incorporada a la Red, por su parte, merece un tratamiento propio, y plantea interrogantes sobre la validez de los rastreos informáticos de archivos y datos de pornografía infantil incorporados a la misma cuando se realizan por la policía en ausencia de autorización

[503] Pozuelo Pérez, *Memento Práctico de Derecho Penal 2021*, pp. 2026 – 2027.

[504] E. Cortés Bechiarelli, “Sobre la pluriofensividad de los delitos cometidos por los funcionarios públicos contra las garantías de la intimidad (artículos 534 a 536 del Código penal español)”, en F. Muñoz Conde et al. (dirs.), *Un Derecho penal comprometido,* 1ª ed., Valencia, Tirant lo Blanch, 2011, pp. 234 – 235.

judicial y conllevan la averiguación de direcciones IP[505]. La STS 236/2008, de 9 de mayo[506], avaló los rastreos informáticos del equipo de Delitos Telemáticos de la Policía Judicial de la Guardia Civil en Internet, en una decisión que apoyo plenamente: cuando los agentes presentaron el listado de direcciones IP ante un juzgado y reclamaron una orden judicial para que los proveedores identificasen a sus titulares, impidieron que estos se amparasen en la excusa de la confidencialidad para llevar a cabo sus deleznables actividades. La búsqueda condujo hasta una mujer, cuyo ordenador se intervino y analizó, comprobando que había realizado búsquedas y descargado archivos ilegales relacionados con bebés, si bien no pudo acreditarse que su pretensión fuese la de obtener pornografía infantil. La clave de esta sentencia es que determina que, al contrario de lo que sucede con las comunicaciones por telefonía convencional, en las que los números de ambos lados de la línea están protegidos por el derecho al secreto de comunicaciones, en las comunicaciones por Internet el teléfono es solo un instrumento para comunicarse con la Red, de manera que quien utiliza un programa P2P (red de pares) admite que, inevitablemente, muchos de sus datos sean públicos, ya que la dirección IP no identifica específicamente a la persona del usuario y sí el ordenador que ha usado. Es posible acceder a estos datos, por lo tanto, en ausencia de una orden judicial, teniendo siempre en cuenta que esta orden sí es necesaria para conocer el teléfono o la identidad del titular del contrato relacionados con una determinada dirección IP por estar protegidos por el derecho a la intimidad personal. En este mismo sentido se pronuncia la STS 292/2008, de 28 de mayo[507], según la cual cuando la comunicación a través de la Red se establece mediante un programa P2P, el operador debe asumir que muchos

[505] C. Guisasola Lerma, "Tutela penal del secreto de comunicaciones. Estudio particular del supuesto de interceptación ilegal de telecomunicaciones por autoridad o funcionario público", en J.C. Carbonell Mateu, J.L. González Cussac, y E. Orts Berenguer (dirs.), *Constitución, derechos fundamentales y sistema penal. Semblanzas y estudios con motivo del setenta aniversario del profesor Tomás Salvador Vives Antón. Tomo I*, 1ª ed., Valencia, Tirant lo Blanch, 2009, pp. 968 – 969.

[506] ECLI:ES:TS:2008:1932.

[507] ECLI:ES:TS:2008:3346.

de los datos que incorpora pasarán a ser de conocimiento público, incluyendo esto la dirección IP[508].

Esta materia es indudablemente compleja[509], puesto que obliga a plantearse ciertos límites de la ciberseguridad. La STS 342/2013, de 17 de abril[510], matizó que la incautación de ordenadores, instrumentos de comunicación telefónica o dispositivos de almacenamiento masivo de información digital con motivo o como consecuencia de una entrada y registro no conlleva, por sí misma, la posibilidad de acceder a su contenido, careciendo de validez suficiente la motivación genérica de la resolución judicial que ordene dicha entrada y registro. Será necesaria una motivación especial e independiente, razonada en todo caso, que confirme también la necesidad de acceder al entorno digital del investigado[511].

3.3.2.7 Ciberseguridad en los delitos contra el orden público

3.3.2.7.1 Daños a instalaciones de telecomunicaciones

El art. 560.1 prevé una pena de prisión de 1 a 5 años para quienes causen daños que interrumpan, obstaculicen o destruyan líneas o instalaciones de telecomunicaciones. Este precepto, introducido en nuestro ordenamiento jurídico en el año 1948, ha recibido críticas de la doctrina a causa de su rigor punitivo derivado de la proliferación de estas conductas en los años siguientes a la Guerra Civil, lo cual hace aconsejable, desde una perspectiva de política criminal, su modificación o su abolición. Quizá por ello

[508] Guisasola Lerma, *Constitución, derechos fundamentales y sistema penal,* pp. 970 – 971.

[509] Guisasola Lerma, *Constitución, derechos fundamentales y sistema penal,* pp. 972 – 973.

[510] ECLI:ES:TS:2013:2222.

[511] S. Álvarez de Neyra Kappler, “Doctrina del Tribunal Supremo con relación a la protección de la relación de confidencialidad abogado-cliente”, en L. Bachmaier Winter (coord.), *Investigación penal, secreto profesional del abogado, empresa, y nuevas tecnologías: retos y soluciones jurisprudenciales,* 1ª ed., Cizur Menor, Navarra, 2022, pp. 215 – 217.

la jurisprudencia del TS ha intentado restringir la aplicación del precepto en el ámbito objetivo, estimándolo únicamente en casos en los que el objeto sustraído resulte imprescindible para el mantenimiento del servicio. A los requisitos típicos hay que añadir dos más: primero, que el delito lo cometa un grupo; y segundo, que la finalidad sea la destrucción o alteración de la paz pública, del normal funcionamiento y uso de los servicios de esta naturaleza y de la coexistencia pacífica de la comunidad, a través de la violación del orden público. La existencia de dicho dolo de propósito excluye el ánimo de lucro como impulsor de la conducta. La finalidad de alterar el orden público es la que da todo su sentido al art. 560.1[512].

3.3.2.7.2 Terrorismo

A nivel internacional[513], terrorismos como el yihadista proyectan su ideología radical y actúan en todo el mundo, incluyendo el territorio europeo, donde ya ha protagonizado terribles atentados. Actualmente, Dáesh es la principal amenaza en este sentido, dada su capacidad operativa, los medios de los que dispone, su proyección mediática y la rapidez con la que se expande. No hay que olvidar, además, que estos grupos se caracterizan por su rápida mutabilidad y por su capacidad de adaptarse a los cambios y a las estrategias que se desarrollan contra ellos[514]. A nivel nacional[515], aunque la

[512] M. Llobet Anglí, "Delitos contra el orden público. Sección 3. Desórdenes públicos", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, p. 2084.

[513] S.S. *Olănescu* y A.V. *Olănescu*, "Cyberterrorism: The Latest Crime Against International Public Order", *Lex ET Scientia International Journal,* vol. 1, no. XXVI, 2019, p. 100. El objetivo de las agencias de inteligencia de los países occidentales no es solo encontrar a los terroristas, sino comprender sus capacidades y motivaciones. En este sentido, a medida que avancen las nuevas tecnologías será más difícil garantizar la seguridad del ciberespacio. Se espera que en los próximos cinco años tengan lugar ataques terroristas en países occidentales, y que los mismos se estructuren, al menos parcialmente, sobre las TIC.

[514] Fernández Bermejo y Martínez Atienza, *Ciberseguridad, Ciberespacio y Ciberdelincuencia*, pp. 91 – 92.

[515] B. Andrés Segovia, *La convergencia de las telecomunicaciones, los medios de comunicación y las tecnologías de la información*, 1ª ed., Navarra, Aranzadi, 2020, p. 421. Dentro de su definición de terrorismo, como posibles objetivos, se incluyen los sistemas de comunicación internacionalmente protegidos.

organización terrorista ETA ya no es una amenaza relevante, España sigue comprometida en la lucha contra el terrorismo, y para ello ha elaborado una respuesta basada en un modelo de integridad que hace posible la incorporación de su experiencia y la coordinación con sus aliados en las iniciativas internacionales, especialmente cuando las integran otros Estados miembros[516] de la UE[517].

A pesar de todo, los avances tecnológicos[518] han ampliado el acceso de los grupos terroristas a los recursos disponibles, incrementando así su capacidad para financiarse, reclutar y adiestrar nuevos miembros y difundir propaganda[519], lo que hace necesaria la prevención legal de sus actividades ilícitas cuando hacen uso de las redes informáticas[520].

El art. 573.2 del CP afirma que se considerarán delitos de terrorismo los delitos informáticos tipificados en los arts. 197 bis y 197 ter y 264 a 264 quater del mismo texto, cuando los hechos se cometan con alguna de las

[516] M. Cancio Meliá, *Los delitos de terrorismo: estructura típica e injusto*, 1ª ed., Madrid, Editorial Reus, 2010, pp. 148 – 150. En Alemania, la aprehensión del terrorismo se regula en el parágrafo 129a de su StGB, y en Francia en los arts. 421-1 y 421-2 de su CP. Por desgracia, no es posible desarrollar un análisis más profundo, puesto que ninguno de los artículos anteriores hace referencia específica a la ciberdelincuencia en relación con el terrorismo, ni tampoco a posibles medidas de ciberseguridad establecidas para impedirla.

[517] M. Marsili, "The War on Cyberterrorism", *Democracy and Security,* vol. 15, no. 2, 2019, p. 191.

[518] J. Jimeno Muñoz, *Derecho de daños tecnológicos, ciberseguridad e Insurtech*, 1ª ed., Madrid, Dykinson, 2019, pp. 81 – 82. Y, pese a todo, no existe una definición legal expresa de ciberterrorismo, más allá de considerarlo como el uso de sistemas informáticos para atacar infraestructuras críticas o sistemas pertenecientes a la Administración Pública, o la coacción o la intimidación capaz de afectar a los organismos públicos y la población civil. Para Jimeno Muñoz, el criterio para diferenciar los ciberataques del ciberterrorismo estaría en el impacto obtenido por los mismos y en los efectos que de ellos se derivan.

[519] S. Morán Blanco, "La ciberseguridad y el uso de las Tecnologías de la Información y la Comunicación (TIC) por el terrorismo", *Revista española de derecho internacional,* vol. 69, no. 2, 2017, p. 220. La utilización de las TIC con fines terroristas y delincuenciales es un fenómeno que se ha extendido con gran rapidez desde principios del siglo XXI, y que obliga a los Estados a actuar de manera coordinada contra el mismo.

[520] Fernández Bermejo y Martínez Atienza, *Ciberseguridad, Ciberespacio y Ciberdelincuencia*, p. 92.

finalidades a las que se refiere el art. 573.1 del CP[521] [522], a saber: primero, la subversión del orden constitucional, o la supresión o desestabilización grave del funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, o la obligación a los poderes públicos a realizar un acto o a abstenerse de hacerlo; segundo, la alteración grave de la paz pública; tercero, la desestabilización grave del funcionamiento de una organización internacional; cuarto, la creación de un estado de terror en la población o en parte de ella. Se trata, por lo tanto, de los delitos de los arts. 197 y 197 ter y 264 a 264 quater del CP que ya he analizado, solo que debe existir la voluntad por parte de los sujetos activos de cometerlos para lograr alguna de las finalidades recogidas en el art. 573.1. Siendo así, el apartado 3 del art. 573 bis del mismo texto legal prevé la imposición de la pena superior en grado a la pena respectivamente prevista para el delito cometido en los artículos correspondientes[523].

Especial atención merecen los ataques contra infraestructuras críticas definidas en el CP (art. 264.2.4 del mismo) con fines subversivos, como los dirigidos contra hospitales[524].

Esta clasificación resulta importante no solo por este motivo, sino porque cuando las conductas anteriores se tipifican como actos de terrorismo,

[521] Fernández Bermejo y Martínez Atienza, *Ciberseguridad, Ciberespacio y Ciberdelincuencia*, p. 93.

[522] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 728.

[523] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 729.

[524] Velasco Núñez, *Delitos tecnológicos*, p. 317.

su investigación[525] cuenta con mayores medios y se asegura una cooperación internacional mucho más rápida y eficaz[526].

En la actualidad, hay que entender que los actuales planteamientos en política antiterrorista encuentran su sustento teórico en el nuevo concepto de seguridad destinado a sustituir a la tradicional concepción de defensa sobre la que se sostenía el instituto militar tradicional. Garantizar esta noción de seguridad, que recibe el calificativo de "integrada", dada su amplitud y complejidad, constituye hoy por hoy el principal objetivo de las organizaciones internacionales. Se busca hacer hincapié en las decisiones tácticas de carácter geoestratégico dirigidas a la neutralización de posibles amenazas antes de que se materialicen[527].

3.3.2.8 Ciberseguridad en los delitos de traición y contra la paz o la independencia del Estado y relativos a la Defensa Nacional

3.3.2.8.1 Descubrimiento y revelación de secretos e informaciones relativas a la Defensa Nacional

Los arts. 598 a 603 del CP recogen una serie de conductas cuyo patrón común es que afectan a la seguridad y defensa nacional a través de

[525] J. Escribano Úbeda-Portugués, "La comunidad internacional frente al terrorismo: desarrollos y nuevos retos en el siglo XXI", en L. Zúñiga Rodríguez (dir.), *Nuevos desafíos frente a la criminalidad organizada transnacional y el terrorismo*, 1ª ed., Madrid, Dykinson, 2021, pp. 381 – 382. La derrota del terrorismo requiere un enfoque holístico: además del uso de la fuerza, de las medidas de aplicación de la ley y de las operaciones de inteligencia, también son necesarias medidas preventivas antiterroristas que impidan su propagación, empezando por el bloqueo de sus fuentes de financiación, como la extorsión que lleva a cabo la criminalidad organizada. Las medidas de ciberseguridad, como protección frente a la extorsión o a cualquier otro tipo de delito, adquieren una especial importancia para garantizar una adecuada prevención.

[526] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 728.

[527] J.M. Alcoceba Gil, "Contraterrorismo en el siglo XXI: de *seguridad* a *defensa*", en V. Moreno Catena y A. Arnáiz Serrano (dirs.), *El estado de derecho a prueba: seguridad, libertad y terrorismo*, 1ª ed., Valencia, Tirant lo Blanch, 2017, pp. 147 – 148. Esta nueva orientación en la lucha contra el terrorismo ha sido ampliamente criticada por la doctrina a causa de su alejamiento, muy especialmente, del imperio de la ley.

actuaciones ilícitas en relación con información legalmente calificada como reserva o secreta, incluyendo tanto conductas de descubrimiento y revelación de la misma como su falseamiento o su destrucción. Estas conductas también se recogen en el Código Penal Militar[528], de acuerdo a cuyo art. 26[529], cuando sea un militar el que cometa uno de los delitos previstos en los arts. 277 o 598 a 603 del CP, se le castigará con la pena establecida en el mismo, solo que incrementada en un quinto de su límite máximo[530]. De suceder los hechos en situación de conflicto armado o estado de sitio, se prevé la imposición de la pena superior en uno o dos grados. Esto, además de demostrar que el art. 277 hubiese tenido mejor encaje de haber utilizado como criterio sistematizador su bien jurídico protegido (la defensa nacional), evidencia los profundos cambios que ha sufrido el Código Penal Militar con el paso de los años[531] [532].

[528] A. Delgado Gil, "La responsabilidad del militar por el delito de revelación de secretos e informaciones relativas a la seguridad y defensa nacionales (comentario a la STS, Sala de lo Militar, de 16 de marzo de 2017), *CEFLegal: revista práctica de derecho. Comentarios y casos prácticos,* no. 203, 2017. En ocasiones, como en la STS comentada, la aplicación del actual Código Penal Militar resulta más favorable al acusado.

[529] A. Urruela Mora, "Derecho penal militar", en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho Penal, Parte Especial*, 2ª ed., Granada, Comares, 2022, p. 915. La noción de delito militar abarca no solo los definidos de manera específica en la Parte Especial del Código castrense como tales, sino también aquellas conductas que lesionan bienes jurídicos estricta o esencialmente militares incriminados en la legislación penal común, siempre que sean cualificados por la condición militar del autor y, además, por su especial afección a los intereses, al servicio y a la eficacia de la organización castrense.

[530] F.J. De León Villalba, "Condicionantes, normativos y extra normativos, del ilícito militar", en F.J. De León Villalba (dir.), *Derecho penal militar. Cuestiones fundamentales*, 1ª ed., Valencia, Tirant lo Blanch, 2014, p. 63. El Derecho penal militar, como Ley especial, contiene los mismos principios y garantías y aplica el mismo concepto de delito que la legislación común, incluso en lo tocante a la naturaleza y fines de la pena.

[531] A. Delgado Gil, "El delito de revelación de secretos de estado en los artículos 598 CP común y 53 CP militar: reflexiones sobre sus diferencias", *Revista electrónica de ciencia penal y criminología,* no. 7, 2005, p. 2. En efecto, exceptuando algunos matices y la pena (mucho más severa), el antiguo art. 53 del CP militar era casi idéntico al art. 598 del CP común. Actualmente, el art. 26 del primero remite al art. 598 del segundo.

[532] F. Molina Fernández, "Delitos de traición y contra la paz o la independencia del Estado y relativos a la Defensa Nacional. Sección 3. Descubrimiento y revelación de secretos e informaciones relativas a la Defensa Nacional", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, p. 2194.

La pretensión del legislador en relación con estos delitos parecía ser la de introducir un sistema escalonado que proporcionase al juzgador distintos niveles de valoración dependiendo de la gravedad de la conducta teniendo en cuenta cuestiones como el grado de ejecución del delito, pero el resultado final es una catalogación de conductas farragosa que hace difícil delimitar cuáles son las propias de cada tipo. En cualquier caso, todos delitos que voy a analizar a continuación comparten un elemento común: afectan, de un modo u otro, a información legalmente calificada como reservada o secreta. El art. 616 prevé, si los mismos se cometen por una autoridad o funcionario público, la imposición de una pena de inhabilitación absoluta por tiempo de 10 a 20 años, y si se cometen por un particular, la una pena de inhabilitación especial para empleo o cargo público por tiempo de 1 a 10 años.

Los arts. 598 y 599 del CP castigan el descubrimiento y revelación de información reservada o secreta, una conducta muy similar a la descrita en el art. 584 del CP, con el matiz de que en este el elemento subjetivo del tipo es favorecer a una potencia extranjera[533] [534]. Estos preceptos recogen la que, muy posiblemente, sea la conducta nuclear de estos delitos, si bien en ninguno de ellos se hace referencia alguna a la posibilidad de llevarlos a cabo por vía telemática[535]. Así, el art. 598 del CP castiga con la pena de prisión de 1 a 4 años al civil que se procure, revele, falsee o inutilice información legalmente calificada como reservada o secreta, siempre que esté relacionada con la seguridad nacional o la defensa nacional o con los medios técnicos o sistemas empleados por las Fuerzas Armadas o industrias de interés militar. El concepto de "información legalmente calificada como

[533] I. De Miguel Beriain, "Delitos de traición y contra la paz o la independencia del Estado, y relativos a la defensa nacional", en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho Penal, Parte Especial*, 2ª ed., Granada, Comares, 2022, pp. 876 – 877. En efecto, el art. 584 del CP se distingue por exigir al sujeto activo el propósito de favorecer a, entre otros, una potencia extranjera.

[534] J.A. Fernández Rodera, "Artículo 598", en M. Gómez Tomillo y A. M.ª Javato Martín (dirs.), *Comentarios prácticos al Código Penal. Tomo VI. Delitos contra la Constitución, el orden público. Delitos de traición y contra la paz o la independencia del Estado y relativos a la defensa nacional. Delitos contra la Comunidad internacional. Artículos 472 – 616 quáter*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, p. 723.

[535] Serrano Ferrer, *Derecho penal y nuevas tecnologías*, p. 40.

reservada o secreta" es el elemento más importante del tipo objetivo, puesto que por información clasificada hay que entender los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puede dañar o poner en riesgo la seguridad y la defensa del Estado[536]. El art. 599 recoge las modalidades agravadas: se castiga con la pena del art. 598 en su mitad superior al sujeto activo que sea depositario o conocedor del secreto o información por razón de su cargo o destino[537], y a quien revele el secreto o información dándole publicidad en algún medio de comunicación social o de forma que se asegure su difusión[538].

El art. 600.1 del CP recoge la conducta consistente en reproducir sin autorización expresa planos o documentación referentes a zonas, instalaciones o materiales militares que sean de acceso restringido y cuyo conocimiento esté protegido y reservado por una información legamente calificada como reservada o secreta, castigándola con una pena de prisión de 6 meses a 3 años. El art. 600.2 del mismo texto castiga con la misma pena a quien tenga en su poder objetos o información legalmente calificada como reservada o secreta, relativos a la seguridad o a la defensa nacional, sin cumplir las disposiciones establecidas en la legislación vigente. Tanto el primer como el segundo delito son criticables por la dificultad para delimitar unas figuras de otras. Algo más claro es el art. 601 del CP, que recoge la única conducta imprudente punible en este ámbito, castigando con una pena de prisión de 6 meses a un año a quien, por razón de su cargo, comisión o servicio, tenga en su poder o conozca oficialmente objetos o información legalmente calificada como reservada o secreta o de interés militar, relativos a la seguridad nacional o la defensa nacional, y por imprudencia grave de lugar a que sean conocidos por una persona no autorizada o divulgados, publicados o inutilizados. Se trata del único caso en que se protege la información de interés militar, siendo la extensión del tipo imprudente superior

[536] Muñoz Conde, *Derecho Penal, Parte Especial*, pp. 746 – 747.

[537] A. Delgado Gil, "El delito de descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional (por el depositario o conocedor), *Cuadernos de política criminal*, no. 125, 2018, p. 45.

[538] Molina Fernández, *Memento Práctico de Derecho Penal 2021*, p. 2195.

a la del doloso, siendo esta una decisión difícilmente justificable. En cualquier caso, solo es punible la imprudencia grave, y solo puede ser sujeto activo de este delito la persona que lleva a cabo la conducta teniendo la información en su poder por razón del cargo que ostenta[539].

El tipo penal del art. 602 del CP recoge una modalidad específica de descubrimiento o revelación de secretos sin vinculación directa con información propia de la seguridad o defensa nacional, pero que afecta a un sector especialmente sensible de la seguridad en general: la energía nuclear. Así, se castiga con una pena de prisión de 6 meses a 3 años a quien descubra, viole, revele, sustraiga o utilice información legalmente calificada como reservada o secreta relacionada con la energía nuclear, a no ser que el hecho tenga señalada una pena más grave en otra ley. Cuando la información también afecta a la defensa o seguridad nacional, no se aplica este artículo, sino el que corresponda a dicho desvalor suplementario, estando esta subsidiariedad prevista de manera expresa en este art. 602[540].

Por último, el art. 603 del CP prevé una pena de prisión de 2 a 5 años y la inhabilitación especial de empleo o cargo público por tiempo de 3 a 6 años a quien destruya, inutilice, falsee o abra sin autorización la correspondencia o documentación legalmente calificada como reservada o secreta, relacionadas con la defensa nacional y que tenga en su poder por razones de su cargo o destino. Esta conducta, muy parecida a la del art. 598 cuando es posible apreciar la agravación del art. 599.1, tiene una pena algo superior, motivo por el cual debe referirse a conductas de una especial gravedad. Errores como que solo se haga referencia a documentos, y no a cualquier información, y de que no se recojan conductas como la revelación a terceros de la información, que es mucho más grave que el mero conocimiento, evidencian la pobre técnica legislativa utilizada en estos

[539] Molina Fernández, *Memento Práctico de Derecho Penal 2021*, pp. 2195 – 2196.
[540] Molina Fernández, *Memento Práctico de Derecho Penal 2021*, p. 2196.

preceptos, hasta el punto de que estas carencias pueden llegar a condicionar la seguridad jurídica[541].

3.3.3 La responsabilidad penal de las personas jurídicas en los delitos que afectan a la ciberseguridad

La clásica discusión en torno a si las personas jurídicas deben caer dentro de la esfera de la responsabilidad se ha extendido, también, al ámbito de las TIC. Y es que el paso del tiempo ha puesto de manifiesto cada vez con mayor intensidad que la responsabilidad de las personas físicas, por sí misma, no resulta suficiente, incluso existiendo consecuencias accesorias para las primeras. El propio Convenio sobre la Ciberdelincuencia de Budapest apuntó en esta dirección, otorgando un margen de discrecionalidad a los Estados parte para decidir la naturaleza de esta responsabilidad, pudiendo ser civil, administrativa o penal[542]. En la actualidad, son varios los artículos del CP español que prevén la responsabilidad de las personas jurídicas, como el art. 197 quinquies y el art. 264 quater[543]. Existe, en relación con dicha responsabilidad, un *numerus clausus*[544] de delitos por los que las personas jurídicas pueden ser penalmente responsables.

El primero es el delito de descubrimiento y revelación de secretos, cuyo art. 197 quinquies del CP, de acuerdo a lo establecido en el art. 31 bis, permite que una persona jurídica sea responsable de los delitos comprendidos en los arts. 197, 197 bis y 197 ter, previendo una pena de multa de 6 meses a 2 años. Respetando las reglas establecidas en el art. 66 bis, también es posible para los jueces y tribunales imponer a la persona jurídica las penas recogidas

[541] Molina Fernández, *Memento Práctico de Derecho Penal 2021*, p. 2196.

[542] Romeo Casabona et al., *La adaptación del derecho penal al desarrollo social y tecnológico,* p. 518.

[543] De la Mata Barranco, *Adaptación del derecho penal español a la política criminal de la Unión Europea,* p. 239.

[544] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 779.

en las letras b) a g) del apartado 7 del artículo 33 del CP, como la suspensión de sus actividades por un plazo que no puede ser superior a cinco años[545].

El segundo es la estafa informática, a través del art. 251 bis del CP, que castiga con una pena de multa del doble al cuádruple de la cantidad defraudada los delitos que tienen prevista una pena de prisión para las personas físicas inferior a cinco años, como los del art. 248.2. Si hay agravantes, la pena prevista por el art. 250.1 aumenta a más de cinco años de prisión, de manera que el art. 251 bis también eleva su pena para la persona jurídica a una multa del triple al quíntuple de la cantidad defraudada. Es posible, también en relación con la estafa informática, la imposición de las penas recogidas en las letras b) a g) del art. 33.7.

El tercero son los daños informáticos del art. 264 quater, que, de acuerdo a lo establecido en el art. 31, permite responsabilizar a una persona jurídica por la comisión de los delitos de los arts. 264 y siguientes. Las penas previstas son una multa del doble al cuádruple del perjuicio causado, si el delito cometido por la persona física tiene prevista una pena de prisión superior a los 2 años, y una multa del doble al triple del perjuicio causado en los demás casos. Se prevé, también, la imposición de las penas recogidas en las letras b) a g) del art. 33.7 del CP. A estas penas para las personas jurídicas se las puede criticar en el mismo sentido que a la agravación facultativa del art. 264.2, párrafo segundo, puesto que cabe plantearse su inconstitucionalidad por vulnerar el principio de proporcionalidad[546].

El cuarto y último delito por el que las personas jurídicas pueden ser penalmente responsables es el 270.6 del CP, que castiga la importación, puesta en circulación o incluso mera tenencia de medios destinados a superar dispositivos de protección de obras con un fin comercial. En relación con el mismo (en realidad, con el art. 270 en su totalidad), el art. 288.1.a del CP prevé una pena de multa del doble al cuádruple del beneficio obtenido, o que se hubiera podido obtener, si el delito cometido por la persona física tiene

[545] Romeo Casabona, *Derecho penal, Parte Especial*, p. 274.

[546] Guérez Tricarico, *Memento Práctico de Derecho Penal 2021*, p. 1418.

prevista una pena de prisión de más de dos años. A este delito también se extiende la posibilidad de imponer por parte de jueces y tribunales las penas recogidas en las letras b) a g) del art. 33.7 del CP.

Resulta muy difícil prevenir y perseguir la comisión de delitos informáticos en algunos casos, a causa de lo fácil que es destruir las pruebas del delito y del anonimato con el que es posible actuar en la Red[547]. Esto conduce a plantearse cuestiones de índole procesal.

3.4 Derecho procesal penal

3.4.1 La determinación de la ley penal aplicable en el espacio y de la jurisdicción competente

Ya he analizado cómo el art. 22 del Convenio sobre la Ciberdelincuencia de Budapest resuelve[548] la cuestión de la jurisdicción en el ámbito internacional en relación con los ciberdelitos acudiendo al criterio de la territorialidad: el tratado internacional obliga a cada Estado parte a adoptar las medidas legislativas que sean necesarias para afirmar su jurisdicción en relación con cualquier delito previsto en sus arts. 2 a 11 cuando se haya cometido en su territorio (art. 22.1.a), a bordo de un buque que enarbole su pabellón (art. 22.1.b), a bordo de una aeronave matriculada de acuerdo a las leyes de dicho Estado parte (art. 22.1.c) o cuando el delito se cometa por uno de sus nacionales, siempre que sea susceptible de ser sancionado penalmente en el lugar donde se ha cometido, o bien si ningún Estado tiene competencia territorial en relación con el mismo (art. 22.1.d). No

[547] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, p. 779.

[548] S.W. Brenner, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law", *Murdoch University Electronic Journal of Law,* vol. 8, no. 2, 2001. El criterio del Convenio de Budapest supuso la respuesta a las críticas doctrinales que se habían venido planteando durante años, y que habían señalado la imposibilidad para los investigadores de utilizar normas pensadas para el mundo real en la persecución de ciberdelitos, como sucedía con las dificultades para recabar pruebas de carácter intangible.

obstante, el art. 22.4 sostiene que no se excluye ninguna jurisdicción penal ejercida por un Estado parte de acuerdo a su derecho interno. Además, se prevén las controversias en las que varios Estados parte reivindican su jurisdicción, debiendo celebrar consultas siempre que sea oportuno para determinar cuál es la jurisdicción más adecuada para llevar a cabo las actuaciones penales. A nivel internacional, es factible aplicar este criterio a los delitos que afectan a la ciberseguridad, como pertenecientes a la categoría más amplia de los ciberdelitos.

A nivel nacional, la respuesta no está tan clara. No hay que olvidar la importancia que también tiene la identificación del ciberdelincuente cuando hace uso de un sistema informático compartido, cuestión que tiende a pasarse por alto en muchos casos, pero que resulta fundamental desde el punto de vista del Derecho penal. Cuando el rastreo de una dirección IP permite ubicar geográficamente el terminal utilizado para el delito, esto no equivale de manera automática a la identificación del autor del mismo, sino que puede haber personas que lo utilicen y no sean conocedores de la acción delictiva ni hayan participado en ella. En estos casos, al rastreo técnico le siguen las diligencias convencionales de prueba con el fin de identificar al autor de los hechos[549]. Resuelta esta cuestión, existen dos grandes cuestiones a resolver: el derecho aplicable y el juez competente para conocer y juzgar unos hechos penalmente incriminados[550] cuando se traten de delitos que afecten a la ciberseguridad.

El art. 24.1 de la CE, que garantiza el derecho a la tutela judicial efectiva y el derecho de acceso a la jurisdicción[551], sumado al art 9.6 de la LOPJ, que determina que la jurisdicción es improrrogable[552], obligan a

[549] E. Velasco Núñez, *Delitos cometidos a través de Internet. Cuestiones* procesales, 1ª ed., Madrid, Wolters Kluwer, 2010, p. 262. Si dichas diligencias no permitiesen identificar al autor, podrían analizarse indicios como la persona más beneficiada, o realizarse análisis del nivel individual de conocimientos informáticos.

[550] Romeo Casabona, *El cibercrimen*, p. 30.

[551] A. Melón Muñoz et al., *Memento Práctico Procesal Penal 2022*, Madrid, Francis Lefebvre, 2021, p. 13.

[552] J. Barja de Quiroga López et al., *Ley de Enjuiciamiento Criminal. Comentada, con jurisprudencia sistematizada y concordancias,* 8ª ed., Madrid, Francis Lefebvre, 2021, pp. 47 - 48. Los artículos 9.6 de la LOPJ y 8 de la LECrim determinan que la jurisdicción,

resolver siempre este problema, no siendo jurídicamente aceptable dejarlo sin respuesta. El art. 23 del mismo texto legal, por su parte, prescribe en su párrafo primero que en el orden penal corresponde a la jurisdicción española el conocimiento de las causas por delitos cometidos en territorio español o cometidos a bordo de buques o aeronaves españoles, sin perjuicio de lo previsto en los tratados internacionales en los que España sea parte. Su párrafo segundo atribuye a la jurisdicción española el conocimiento de los delitos cometidos fuera del territorio nacional únicamente en los casos en que quienes los cometan sean españoles o extranjeros que hayan adquirido la nacionalidad española con posterioridad a la comisión del hecho, y concurran una serie de requisitos. Estos arts. 23.1 y 23.2 de la LOPJ, como puede apreciarse, dan respuesta a las exigencias establecidas por el art. 22 del Convenio sobre la Ciberdelincuencia de Budapest[553].

Durante años[554] [555], el Gobierno de España se ha preocupado por estructurar de manera adecuada la lucha contra los ciberdelitos, pese a lo cual el poder legislativo no ha desarrollado ningún criterio específico que sirva para responder a las dos cuestiones planteadas, que encuentran su respuesta en el ámbito de la jurisprudencia, es decir, en el del poder judicial.

---

incluyendo la criminal, es siempre improrrogable con objeto de facilitar la seguridad jurídica y de cumplir el derecho a la tutela judicial efectiva. Incluso así, sentencias como la de 4 de abril de 2001 de la Sala Segunda del TS evidencian que pueden surgir controversias para decidir cuál es el juez predeterminado legalmente para la instrucción de una causa.

[553] J. Zarzalejos Nieto, "La competencia de los tribunales penales", en J. Banacloche Palao y J. Zarzalejos Nieto (eds.), *Aspectos fundamentales de Derecho procesal penal*, 5ª ed., Madrid, Wolters Kluwer, 2021, pp. 48 – 49. El apartado c) del art. 23.2 incluye una previsión en relación con el principio *non bis in idem*.

[554] Fiscalía General del Estado, *Instrucción no. 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías",* Madrid, Fiscalía General del Estado, 2011, p. 5. Esta Instrucción sirvió para reforzar la unidad de actuación del Ministerio Fiscal en materia de criminalidad informática, favoreciendo también la especialización del Ministerio Público.

[555] Consejo de Seguridad Nacional, *Estrategia Nacional de Ciberseguridad 2019*, Madrid, Consejo de Seguridad Nacional, 2019, p.48. Dentro de la tercera de sus líneas de acción, la cuarta medida consiste en el fomento del traslado a los organismos competentes de la jurisdicción penal de la información relativa a incidentes de seguridad que presenten caracteres de delito, y especialmente de aquellos que afecten o puedan afectar a la provisión de los servicios esenciales y a las infraestructuras críticas, como las sanitarias.

Comenzando por el supuesto más sencillo posible, no cabe duda de que cuando la acción se realiza en el territorio de un Estado y el resultado de la misma se produce en dicho Estado procede aplicar su ley, sin importar la nacionalidad del autor[556].

Cuando se trata de ciberdelitos, los supuestos no suelen tener unas características tan nítidas. La doctrina, en este sentido, ha puesto de manifiesto que en relación con los mismos no es válida la legislación penal concebida de manera tradicional como cuerpo legislativo vigente para un determinado territorio. Hay dos soluciones al respecto, que pueden ser concurrentes: primera, armonizar las legislaciones nacionales y reforzar los mecanismos de cooperación internacional y bilaterales[557]; y segunda, establecer cláusulas de extraterritorialidad, como las que ya existen para delitos como el terrorismo.

La respuesta a las preguntas formuladas se puede buscar mediante la precisión del lugar donde se entiende cometido el delito, o *locus commissi delicti*, con objeto de poder aplicar la *lex loci commissi delicti.* Son tres las construcciones jurídicas que permiten resolver esta cuestión: primera, la teoría de la actividad[558], de acuerdo a la cual el delito se entiende cometido en el lugar en el que el sujeto lleva a cabo a nivel externo la conducta delictiva; segunda, la teoría del resultado, según la cual el delito se perpetra donde tiene lugar el resultado externo; y tercera, la teoría de la ubicuidad[559], la más

---

[556] Romeo Casabona, *El cibercrimen*, p. 31.

[557] P. De Hert y V. Papakonstantinou, "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area", *Brussels Privacy Hub Working Paper Series,* vol. 1, no. 1, 2014, pp. 34 – 35. Es necesario avanzar hacia una mayor armonización de las leyes dentro de la UE, tanto en materia de Derecho penal sustantivo como de Derecho procesal penal.

[558] J. Cerezo Mir, *Curso de Derecho Penal español. Parte General. Tomo II. Teoría Jurídica del Delito*, 6ª ed., Madrid, Tecnos, 2000, p. 77. Así, sería competente el Tribunal del lugar en que se realizó la acción.

[559] C.M. Romeo Casabona, "La protección penal de la intimidad y de los datos personales: los mensajes de correo electrónico y otras comunicaciones de carácter personal a través de Internet y problemas sobre la ley penal aplicable", *Estudios Jurídicos. Ministerio Fiscal,* no. 2, 2003, pp. 101. Ya en 2003, la doctrina se decantaba por la teoría de la ubicuidad, si bien se preveían casos en que su aplicación no sería satisfactoria.

acertada, según la cual el delito se entiende cometido donde se lleva a cabo la actividad o se manifiesta el resultado.

Aunque la elección entre estas tres construcciones jurídicas ha sido objeto de un intenso intercambio de pareceres tanto a nivel doctrinal como jurisprudencial, la teoría de la ubicuidad es la más compartida, ya sea en el derecho comparado como en nuestra doctrina y jurisprudencia[560], incluyendo las más altas instancias judiciales. En efecto, el Pleno No Jurisdiccional de la Sala Segunda del TS de 3 de febrero de 2005 adoptó el criterio de la ubicuidad, siendo competente de acuerdo con el mismo el Juez de Instrucción de cualquiera de las circunscripciones implicadas y, ante un conflicto en este sentido, el primero que haya realizado actuaciones procesales. El TS considera que, al ser el delito informático un delito de tracto mutante e itinerante que despliega sus efectos en múltiples ubicaciones geográficas, se produce en todos los lugares donde se manifiestan sus efectos, tanto en lo concerniente a la acción como al resultado, justificando esto la atribución de competencia.

Hay que tener muy en cuenta que este criterio de la ubicuidad es una regla provisional, toda vez que si resulta posible determinar el lugar de la comisión del delito, entendiendo como tal la localización del terminal desde el que se ha llevado a cabo la principal acción comisiva, procederá la aplicación del art. 14 de la LECrim, debiendo inhibirse quien haya intervenido hasta el momento en favor del Juez de Instrucción que corresponda al lugar de los hechos. Es necesario introducir dos críticas a este sistema: primera, que no siempre coincide el lugar de comisión del delito[561] con el del lugar donde radica el equipo informático, dependiendo esto del tipo de delito de que se trate; segunda y más importante, que no siempre resulta adecuado considerar

[560] Barrio Andrés, *Delitos 2.0,* pp. 51 – 53.

[561] F.J. Sospedra Navas y S. Beltrán Miralles, “Cuestiones generales”, en F.J. Sospedra Navas (dir.), *Prácticum Proceso Penal 2022*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021, p. 28. El criterio nuclear de atribución de jurisdicción a los órganos jurisdiccionales españoles es el *forum delicti comissi*, que plantea problemas en los delitos a distancia. Para estos delitos que tienen su consumación en lugar diferente a aquel en que se inició o se llevó a cabo la acción resulta mucho más adecuado el criterio de la ubicuidad.

competente a quien abre primero diligencias, sino que debería conocer del asunto quien esté en mejores condiciones para ello de acuerdo a criterios objetivos, como una mayor proximidad respecto a las fuentes de prueba.

Además, en algunos casos, a causa de la modalidad delictiva, será de aplicación no el art. 14 LECrim, sino ciertas reglas especiales. Así, la Audiencia Nacional será competente para conocer de los delitos cometidos fuera del territorio nacional para los que sea competente la jurisdicción española de acuerdo al art. 65.1.e) de la LOPJ. Es necesario hacer una interpretación restrictiva de este precepto para no colapsar la Audiencia Nacional atribuyéndole cualquier delito que se haya cometido en el extranjero. Para ello, conviene que se le atribuya exclusivamente el conocimiento de los delitos cometidos por bandas organizadas transnacionales y a gran escala. La Audiencia Nacional también será competente para conocer de los delitos de terrorismo[562] cometidos por bandas organizadas, puesto que son modalidades delictivas tradicionales en los que el uso de medios informáticos se entiende como una particularidad que en nada afecta a la competencia[563].

Por último, esta atribución de competencia a un órgano judicial central con autoridad a nivel nacional es también una manera adecuada de lidiar con el problema de la ubicuidad real en los delitos informáticos de carácter patrimonial que perjudiquen a una generalidad de personas. Así, la Sala Segunda del TS, en su ATS de 11 de junio de 2007, atribuyó al Juzgado Central de Instrucción la competencia para conocer de un delito cometido a

[562] F.J. Jiménez Fortea, "¿Existe un *Derecho procesal del enemigo* en la lucha contra el terrorismo en España?", en F.J. Garrido Carrillo (dir.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumentos, límites y perspectivas en la era digital*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2022, pp. 211 – 212. En estos casos, la competencia no la ostenta el llamado juez natural, sino que tanto la instrucción como el enjuiciamiento corresponden a la Audiencia Nacional (de acuerdo con lo dispuesto en el art. 65 de la LOPJ, en relación con la Disposición Transitoria de la Ley Orgánica 4/1988, de 25 de mayo).

[563] M. Fernández López, "Algunas propuestas para regular la investigación del cibercrimen", en J.M. Asencio Mellado y O. Fuentes Soriano (dirs.), *La reforma del proceso penal,* Madrid, Wolters Kluwer, 2011, pp. 275 – 278. Es necesario contar con una regulación procesal actualizada a la realidad de los ciberdelitos.

través de Internet basándose en el elevado nivel de complejidad inherente a la instrucción[564].

3.4.2 Líneas de evolución futuras

El imparable avance de la tecnología hace que cada vez se planteen cuestiones más complejas de Derecho procesal penal, como las relacionadas con el *cloud computing*. Las características técnicas de estos avances hacen cada vez más difícil para los países la adjudicación de la competencia penal dentro de sus territorios, puesto que resulta muy complejo determinar aspectos como el lugar donde se almacenan los datos. Es necesario, por lo tanto, que organismos internacionales como el Consejo de Europa constituyan grupos de trabajo en los que participen expertos tanto del sector público como del privado, así como académicos, colaborando para proponer soluciones en relación con la legislación relativa a las nuevas tecnologías[565]. Del mismo modo, también resultan recomendables las investigaciones transfronterizas y la coordinación a nivel nacional e internacional[566].

En relación con la investigación penal[567], la novedad que más reclama la mejor doctrina es la creación de una Policía Judicial que dependa del Ministerio Fiscal tanto desde un punto de vista funcional como orgánico, adaptando así España a los países de su entorno y sin perjuicio de la

---

[564] C. Velasco San Martín, *Jurisdicción y Competencia Penal en Relación al Acceso Transfronterizo en Materia de Ciberdelitos,* 1ª ed., Valencia, Tirant lo Blanch, 2016, pp. 209 – 224. España, al igual que Alemania, es un país con un sistema de derecho codificado, en contraposición al sistema de *Common Law.*

[565] E. Tejada de la Fuente y A.M. Martín Martín de la Escalera, "Cibercrimen", en A.M. Díaz Fernández (dir.), *Conceptos fundamentales de inteligencia,* Valencia, Tirant lo Blanch, 2016, p. 39. Muchas veces, solo será factible perseguir de forma eficaz esta clase de actividades delictivas utilizando las TIC en la investigación.

[566] Velasco San Martín, *Jurisdicción y Competencia Penal en Relación al Acceso Transfronterizo en Materia de Ciberdelitos,* pp. 383 – 384.

[567] A. Marín Cano, "Investigación penal de delitos tecnológicos", en F. Bueno de Mata (dir.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia,* Granada, Comares, 2020, p. 285. A destacar, en la misma obra (pp. 259 – 272), "Prevención e investigación de delitos en España: ¿un nuevo terreno para la IA?", de L. Estévez Mendoza. No cabe duda de que las nuevas tecnologías van a obligar a los juristas a prevenir conductas cada vez más complejas pero, éticamente utilizadas, pueden ser también un apoyo de gran valor.

colaboración de las FFCCSE cuando corresponda[568]. Es necesario que una ley específica regule su estructura, su funcionamiento y el estatuto de su personal[569].

En cuanto a los delitos que afectan a la ciberseguridad, el principal obstáculo de tipo procesal para hacerles frente de manera eficaz es la inexistencia de una adecuada cooperación entre países, lo cual es grave si se tiene en cuenta que más de la mitad de las investigaciones penales necesitan una solicitud transfronteriza para obtener pruebas electrónicas de prestadores de servicios establecidos en Estados miembros distintos o, incluso, fuera de la UE. Con la intención de eliminar esta dificultad, la Comisión Europea presentó el 17 de abril de 2018 sus nuevas propuestas para la facilitación de la recogida y de la admisibilidad de la prueba digital (o *e-evidence*), con las que se pretenden dotar de más agilidad y seguridad a la recogida por parte de las autoridades policiales y judiciales de un Estado miembro de correos electrónicos, mensajes de texto y datos almacenados en la nube, entre otros materiales informáticos, y a su admisión y valoración como pruebas en un proceso penal transnacional[570]. Estas iniciativas orientadas a conseguir una serie de garantías procesales se han materializado, sobre todo, en la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal. Este Reglamento no eliminará la Orden de Investigación Europea (OIE) ni la Asistencia Legal Mutua (ALM), pero introducirá una alternativa más rápida centrada específicamente en la prueba electrónica: la nueva Orden Europea de Entrega (OEE)[571]. Gracias a la misma, la autoridad judicial de un Estado miembro podrá solicitar pruebas electrónicas de todo tipo directamente a un

[568] P. Otero, "El derecho penal frente a los riesgos de internet: el ciberdelito", *Actuarios*, no. 48, 2021, p. 32.

[569] Barrio Andrés, *Delitos 2.0,* p. 224.

[570] F. Bueno De Mata, "Análisis de las medidas de cooperación judicial internacional para la obtención transfronteriza de pruebas en materia de cibercrimen", en L. Fontestad Portalés (dir.), *La transformación digital de la cooperación jurídica penal internacional*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021, p. 25.

[571] Barrio Andrés, *Delitos 2.0,* p. 225.

prestador de servicios que los ofrezca dentro de la UE y cumpla los requisitos de estar establecido o representado en alguno de los Estados miembro, con independencia de la ubicación de los datos. El prestador de servicios estará obligado a responder en un breve plazo de 10 días, o en uno de 6 horas en caso de urgencia, lo que supone una notable mejora respecto a los 120 días previstos en la Orden de Investigación Europea (OIE) y los 10 meses que prevé la Asistencia Legal Mutua (ATM), facilitando la persecución de esta clase de delitos[572].

Además, la nueva Orden Europea de Conservación otorgará la capacidad a la autoridad judicial de un Estado miembro para obligar a un prestador de servicios que cumpla los mismos requisitos mencionados en el párrafo anterior a conservar unos datos específicos para facilitar su petición más adelante utilizando los distintos mecanismos previstos al efecto.

Del mismo modo, la Propuesta de Reglamento incluye en su articulado varios Anexos y formularios que podrán ser utilizados en todo el territorio de la UE. Por ejemplo, el Anexo I contiene el llamado EPOC (*European Production Order Certificate*), el Anexo II el EPOC-PR (*European Preservation Order Certificate*), y el Anexo III un formulario que deberá cumplimentarse en los casos en que resulte imposible la utilización de los dos anteriores.

Con carácter adicional, existe una Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, cuyo objetivo es facilitar la recepción, cumplimiento y control en la aplicación de las resoluciones judiciales y de las órdenes emitidas por las autoridades competentes de los Estados miembros[573].

Por último, hay que destacar la ciber resiliencia, entendida como la capacidad para resistir, proteger y defender el uso del ciberespacio de los

[572] Barrio Andrés, *Delitos 2.0,* p. 225 – 226.
[573] Barrio Andrés, *Delitos 2.0,* p. 226.

atacantes, como factor clave en la lucha futura contra los ciberdelitos, escenario en el cual la ciberseguridad, y más específicamente los delitos que afectan a la ciberseguridad, cobrarán máxima prioridad[574].

3.5 Cuestiones de *lege ferenda*

3.5.1 La ciberseguridad como bien jurídico protegido autónomo

3.5.1.1 El avance de la tecnología hace inevitable la aparición de nuevos bienes jurídicos protegidos

Hace menos de diez años, la posibilidad de establecer llamadas y videollamadas a través de Internet, aunque existía, estaba aún lastrada por limitaciones tecnológicas y por la reticencia a utilizarlas de parte de los usuarios, que seguían considerando las llamadas telefónicas tradicionalmente entendidas superiores a las primeras, e innecesarias e invasivas de la intimidad las segundas. Hoy, en pleno 2020, cuando existe una tendencia a utilizar más el teléfono móvil que el ordenador, y más el ordenador que el teléfono fijo, las llamadas y videollamadas a través de distintos *software* que permiten establecer comunicaciones de texto, voz y video a través de Internet son una innovación tecnológica aceptada y utilizada por la mayoría de los usuarios. La nueva realidad tecnológica, de la cual lo anterior es solo uno de muchos ejemplos, requiere un análisis sustentado sobre la misma.

[574] Barrio Andrés, *Delitos 2.0,* p. 227.

La doctrina[575] [576] ya adelantó la necesidad de establecer un bien jurídico protegido autónomo que, teniendo en cuenta el avance de las TIC, protegiese a sus usuarios.

Y es que la importancia que han adquirido las nuevas tecnologías en todos los ámbitos de la vida diaria ha supuesto la introducción de nuevas y, en ocasiones, complejas conductas que obligan a plantearse la posibilidad de reconocer nuevos bienes jurídicos protegidos autónomos como la ciberseguridad, puesto que dichas conductas trascienden ámbitos tradicionalmente protegidos como la intimidad o los datos de carácter personal reservados. Este avance de la tecnología, que resulta éticamente criticable pero que, desde una perspectiva práctica, es indudablemente imparable, supone un continuo riesgo de obsolescencia para el Derecho penal, que se enfrenta al desafío de responder cada vez con más rapidez a difíciles cuestiones respetando siempre los principios que lo caracterizan. Es por esto que creo que la mejor manera para justificar la existencia de este nuevo bien jurídico protegido y para darle forma es basarme en la legislación nacional e internacional existente.

3.5.1.2 La ciberseguridad en la Declaración Universal de los Derechos Humanos

Aunque, como es lógico, no se menciona de manera específica la ciberseguridad en la DUDH por ser imposible atendiendo al estado de la tecnología en el año en que se aprobó (1948), es posible encontrar en la misma tres artículos en los que la seguridad informática podría encontrar amparo, siempre mediante una interpretación objetiva de los mismos. En

[575] Romeo Casabona, *El cibercrimen*, pp. 187 – 190. Ya en 2006, se predijo que las reflexiones político-criminales sobre los nuevos escenarios para la intimidad, los datos personales y las telecomunicaciones a través de Internet se acrecentarían en los años siguientes a causa, por un lado, de la presión doctrinal existente en torno a dichos delitos y, por otro, de los compromisos derivados de la legislación internacional.

[576] J. Zaldívar Robles, “La protección penal del derecho a la intimidad”, *Teoría y derecho: revista de pensamiento jurídico,* no. 19, 2016, pp. 162 – 188. Se cita a Louis Brandeis, quien sostuvo que el derecho a ser dejado en paz es el más absoluto de los derechos, y el más valorado por los hombres libres.

efecto, el art. 27.1 de la DUDH sostiene que toda persona tiene derecho a, entre otras cosas, participar en el progreso científico y en los beneficios que de él resulten. Se trata de una defensa de la ciberseguridad en sentido positivo, ya que las redes y sistemas informáticos son uno de los resultados del progreso científico, y los delitos que afectan a la ciberseguridad impiden de distintas maneras que sus víctimas disfruten de los beneficios derivados del mismo. El art. 19 de la DUDH, por su parte, defiende el derecho de todo individuo a la libertad de opinión y de expresión, que incluye, entre otros, el derecho de recibir y difundir informaciones y opiniones sin limitación de fronteras por cualquier medio de expresión[577].

La palabra información hace referencia a la comunicación o adquisición de conocimientos que permiten la ampliación o precisión de los que ya se poseen en relación con una determinada materia, por lo que se refiere a toda información en sentido genérico, como la que se transmite a través de las redes y sistemas informáticos. Este art. 19 supone una defensa de la ciberseguridad en sentido negativo, puesto que gracias al mismo nadie puede ser molestado durante una legítima difusión o recepción de informaciones u opiniones. En último lugar, el art. 28 de la DUDH afirma que toda persona tiene derecho a que se establezca un orden social e internacional en el que los derechos y libertades proclamados en la DUDH se hagan plenamente efectivos. A través de este artículo, el legislador internacional pretende asegurarse de que el contenido de la DUDH se traslade a los ordenamientos jurídicos estatales, algo que, en relación con los arts. 27.1 y 19, cristalizó años después en España mediante los arts. 18.4 de la CE de 1978 y 82 de la LOPD-GDD.

3.5.1.3 La ciberseguridad en la Constitución española de 1978

[577] C.M. Romeo Casabona, "Derecho penal y libertades de expresión y comunicación en Internet", en C.M. Romeo Casabona y F. Guanarteme Sánchez Lázaro (eds.), *La adaptación del derecho penal al desarrollo social y tecnológico*, Granada, Comares, 2010, p. 299.

Aunque el art. 17.1 de la CE de 1978 garantiza el derecho a la seguridad[578], no se menciona de manera específica en la misma la ciberseguridad. No obstante, en su Título I (dedicado a los derechos y deberes fundamentales), Capítulo segundo (derechos y libertades), Sección primera (de los derechos fundamentales y de las libertades públicas), el art. 18.4 sostiene que la ley deberá limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos, así como el pleno ejercicio de los derechos. Esta última expresión, que obliga a limitar por ley el uso de la informática para que los ciudadanos puedan ejercitar de manera plena sus derechos, debe conectarse con los arts. 27.1 y 19 de la DUDH, que amparan a los ciudadanos españoles, estando obligado el legislador a establecer las medidas necesarias para que se hagan plenamente efectivos. La protección integral de las redes y sistemas informáticos requiere, además de la existencia de los bienes jurídicos ya existentes, la aceptación de la ciberseguridad como uno autónomo, puesto que solo así puede protegerse su disponibilidad, integridad y confidencialidad en los casos en los que no se lesione ninguno de los primeros.

Esta idea se ve reforzada por el art. 18.3 de la CE, que garantiza el secreto de las comunicaciones en ausencia de resolución judicial, y que obliga a defender, al menos, una de las tres facetas de la ciberseguridad: la relativa a la confidencialidad. No obstante, considero que el artículo clave, en este sentido, es el 18.4 de la CE en relación con los arts. 27.1 y 19 de la DUDH, puesto que permiten la aceptación como bien jurídico protegido autónomo de las tres facetas que componen la ciberseguridad, y no solo de una de ellas. Comparto, en este sentido, la certeza del sector doctrinal que defiende que la ciberseguridad debe abarcar la disponibilidad, la integridad y la confidencialidad[579], es decir, que solo puede entenderse garantizada la ciberseguridad cuando se asegura de manera íntegra y total.

---

[578] G. Portilla Contreras, *El Derecho penal a la libertad y seguridad (de los derechos)*, 1ª ed., Madrid, Iustel, 2012, p. 21. Cuanto más crece el derecho a la seguridad, más recortado se ve el derecho a la libertad.

[579] Fernández Bermejo y Martínez Atienza, *Ciberseguridad, Ciberespacio y Ciberdelincuencia*, pp. 27 – 28.

3.5.1.4 La ciberseguridad en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales

Al empuje del avance de la tecnología, los arts. 27.1 y 19 de la DUDH y el art. 18.4 de la CE hay que añadir el derecho a la seguridad digital consagrado en el art. 82 de la LOPD-GDD, de contenido sucinto pero muy claro. De acuerdo al mismo, los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet.

Especialmente en este caso, la ausencia específica del término *ciberseguridad* carece de importancia, pues no cabe duda, una vez más, de la voluntad del legislador de proteger la seguridad de las redes y sistemas informáticos. Esta voluntad, que también puede apreciarse en textos legales de primer orden tanto a nivel internacional (DUDH) como nacional (CE), justifica la existencia de un nuevo bien jurídico protegido como es la ciberseguridad, siendo necesario, para su adecuada materialización, un análisis conceptual desde la perspectiva del Derecho penal que posibilite su encaje en dichos textos legales.

3.5.1.5 Conceptualización de la ciberseguridad como bien jurídico protegido autónomo en el Derecho penal

El Convenio sobre la Ciberdelincuencia de Budapest indica en su preámbulo que es necesario prevenir las acciones que suponen un atentado contra la disponibilidad, la integridad y la confidencialidad de las redes y sistemas informáticos, así como su uso fraudulento, velando por su incriminación. Esta es la base para la definición del bien jurídico protegido en la tipificación de las conductas consistentes en el acceso ilícito a redes o sistemas informáticos, teniendo siempre en cuenta que hay que distinguir el continente del contenido, y que lo que se pretende proteger son tanto dichas redes y sistemas (el continente) como los datos (el contenido). No obstante, los datos informáticos son parte del *software* de los sistemas informáticos, de manera que la protección de estos últimos ya implica la salvaguarda de los

primeros. Pero es que, además, el CP ya protege los datos que se almacenan en los sistemas informáticos a través de distintos tipos delictivos que se ajustan a la naturaleza de los mismos, algo muy adecuado desde un punto de vista sistémico. Me centraré, por lo tanto, en la disponibilidad, la integridad y la confidencialidad de las redes y sistemas informáticos, y en la necesidad de que exista en el Derecho penal un bien jurídico protegido autónomo que proteja dichas cualidades: la ciberseguridad[580].

El Derecho penal debe proteger los bienes vitales fundamentales tanto de los individuos como de la comunidad[581]. Para conseguir este objetivo, estos bienes son elevados, mediante la protección que otorgan las normas, a la categoría de bienes jurídicos. Aunque carecen de entidad material o física, se distinguen por ser valores ideales que la sociedad atribuye a ciertos objetos, cosas, situaciones o relaciones basándose en su aptitud e idoneidad instrumental para satisfacer las necesidades individuales y colectivas[582].

A pesar de que dichas necesidades no solo son plurales, sino que muchas veces colisionan entre sí, el bien jurídico debe ser una entidad libre de conflictos y antagonismos capaz de configurar un espacio social que delimite, a su vez, las condiciones necesarias para el correcto desenvolvimiento de otros bienes jurídicos involucrados en dicho espacio, permitiendo un mayor rendimiento y aprovechamiento de los mismos.

---

[580] M.ª A. Rueda Martín, "La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español", *Diritto Penale Contemporaneo: Rivista Trimestrale*, no. 3, 2020, pp. 210 – 211. Para Rueda Martín, el bien jurídico protegido dotado de autonomía que sirve como barrera para contener riesgos que pueden afectar a otros bienes jurídicos implicados en la utilización de redes y sistemas informáticos es la confidencialidad, integridad y disponibilidad de los sistemas informáticos. En este sentido, aunque mi definición de ciberseguridad es más amplia y contiene, como es lógico, otros elementos adicionales, también incluye, en su vertiente lógica, la disponibilidad, la integridad y la confidencialidad de los sistemas informáticos.

[581] A. J. Sanz Morán, "Reflexiones sobre el bien jurídico", en J.C. Carbonell Mateu, J.L. González Cussac, y E. Orts Berenguer (dirs.), *Constitución, derechos fundamentales y sistema penal. Semblanzas y estudios con motivo del setenta aniversario del profesor Tomás Salvador Vives Antón. Tomo II*, 1ª ed., Valencia, Tirant lo Blanch, 2009, p. 1769. La función del Derecho penal reside en la protección de los bienes jurídicos, entendidos como condiciones para el libre desarrollo del ser humano en su relación con otros seres.

[582] Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 364 – 365.

Existen, en este sentido, dos grandes clases de bienes jurídicos: primera, los bienes jurídicos individuales (como la vida), de corte clásico, fáciles de determinar por referirse a las relaciones entre las personas; segunda, los bienes jurídicos supraindividuales (también llamados colectivos, comunitarios, o generales, como la salud pública), resultado del dinamismo que caracteriza a la sociedad moderna, que resultan útiles para la sociedad en su conjunto, pero son más difíciles de determinar[583]. Estos últimos se consideran, desde una perspectiva material, complementarios de otros bienes jurídicos. Esta característica de los bienes jurídicos colectivos de prestar utilidades a otros bienes jurídicos individuales se divide en dos funciones: la función negativa, o de contención de riesgos para otros bienes jurídicos, que crea una relación de complementariedad con ellos; y la función positiva, en la que los bienes jurídicos a los que complementan tienen la capacidad para cumplir una función social en beneficio de todos los ciudadanos, estando dotados de autonomía. En cualquier caso, y salvo excepciones, una vez el ordenamiento jurídico reconoce un bien jurídico colectivo se admiten tanto su independencia como la posibilidad de que resulte lesionado sin necesidad de que dicha lesión afecte de manera simultánea a bienes jurídicos individuales[584].

El bien jurídico propuesto, la ciberseguridad, constituye una barrera de contención de riesgos para otros bienes jurídicos involucrados en la función social que desempeñan las redes y sistemas informáticos, como la intimidad personal y familiar[585]. En efecto, unos datos de carácter personal reservados estarán más protegidos si, además de protegerse como bien jurídico protegido la intimidad personal y familiar, se protege también la

[583] Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 365 – 367.

[584] J.M. Luzón Cuesta, A. Luzón Cánovas, y M. Luzón Cánovas, *Compendio de Derecho Penal, Parte Especial*, 23ª ed., Madrid, Dykinson, 2021, p. 320. El delito contenido en el art. 316 del CP supone la elevación de la seguridad (en este caso, no de los sistemas de información, sino en el trabajo) a la categoría de bien jurídico autónomo, incluso cuando para interpretarlo es necesario recurrir a normas extrapenales.

[585] Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 367 – 369.

ciberseguridad del sistema informático que los contiene. Esto es igual de cierto para otros bienes jurídicos como la capacidad competitiva de la empresa, el patrimonio, e incluso la defensa nacional[586].

No obstante, para la adquisición de la categoría de bien jurídico colectivo, es necesario no solo el cumplimiento de la mencionada función negativa de contención de riesgos, sino también satisfacer una función positiva mediante la creación y configuración de espacios capaces de delimitar las condiciones necesarias para que los bienes jurídicos a los que complementan puedan cumplir su función social. En la sociedad actual, las TIC tienen una importancia innegable, influyendo, incluso, en ámbitos como el sanitario con adelantos como la salud electrónica[587]. Es inevitable, en un escenario como este, que tanto los particulares como los empresarios, e incluso las Administraciones públicas, sean partidarios de proteger la disponibilidad, la integridad y la confidencialidad de las redes y sistemas informáticos[588], con independencia de las ulteriores finalidades perseguidas por el sujeto activo. Las consecuencias del desarrollo de la función positiva de la ciberseguridad como bien jurídico son varias: primera, su existencia hace innecesario añadir una finalidad ilícita adicional para la intervención del Derecho penal, el cual, dada la importante función social que desempeña este bien jurídico, debe no solo protegerlo, sino también reprimir los comportamientos que lo lesionen; segunda, la incorporación de ulteriores exigencias objetivas, como la vulneración de medidas de seguridad, puede

[586] J. Cerezo Mir, *Curso de Derecho Penal español. Parte General. Tomo I. Introducción*, 6ª ed., Madrid, Tecnos, 2005, p. 17. Cerezo Mir consideraba que en la selección de los bienes jurídicos tutelados por el Derecho penal y, especialmente, en la determinación del ámbito de protección de los mismos, tenían una importancia fundamental las concepciones ético-sociales, jurídicas y políticas dominantes en la sociedad en un momento determinado. Nadie podría dudar de que la seguridad de los sistemas de información es, en la actualidad, esencial para el correcto funcionamiento de una sociedad dependiente de los mismos.

[587] Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 369 – 371.

[588] Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 371 – 373.

ser aceptada desde una perspectiva político-criminal como manifestación de una mayor gravedad de la acción[589].

En consecuencia, considero que concurren los requisitos necesarios para la elevación de la ciberseguridad a la categoría de bien jurídico protegido autónomo, a través del cual será posible proteger de acuerdo con su vital importancia la seguridad de las redes y sistemas informáticos, garantizando su disponibilidad, su integridad y su confidencialidad.

3.5.2 El delito de intrusión en un sistema de información, o delito de *cracking*

3.5.2.1 Propuesta político-criminal sobre la represión penal autónoma de esta conducta

Fundamentada la existencia y la autonomía de la ciberseguridad como bien jurídico protegido, procede analizar la necesidad político-criminal de criminalizar las conductas idóneas para lesionarla[590] [591]. Este análisis se compone de tres argumentos esenciales.

Primero, es importante otorgar a la ciberseguridad, a través del Derecho penal, una protección adicional a la que ofrece el Derecho administrativo. Y esto porque la función social que desempeña se ha convertido en esencial en una sociedad que ha pasado a depender extraordinariamente de la misma, como en el caso del sistema sanitario. Además, en los últimos años se ha reconocido el valor social positivo de las TIC como necesario y vinculante para el correcto funcionamiento del sistema

[589] Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 373 – 376.

[590] M.ª A. Rueda Martín, "Los ataques contra los sistemas informáticos: conductas de hacking. Cuestiones político-criminales", en C.M. Romeo Casabona y F. Guanarteme Sánchez Lázaro (eds.), *La adaptación del derecho penal al desarrollo social y tecnológico,* 1ª ed., Granada, Comares, 2010, pp. 348 – 349.

[591] Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal,* p. 64.

social, de manera que resulta lógico garantizar su seguridad mediante un bien jurídico protegido autónomo que, además, sirva como barrera de contención de riesgos respecto a otros bienes jurídicos implicados en su utilización[592].

Segundo, la elevación de esta clase de comportamientos a la categoría de delito en nuestro CP supone la armonización de nuestra legislación penal en este ámbito con la de otros Estados miembros de la UE, de acuerdo con lo dispuesto tanto en la Directiva 2013/40/UE como en el Convenio sobre la Ciberdelincuencia de Budapest[593]. Dichos comportamientos son especialmente peligrosos por su naturaleza internacional o transfronteriza, de manera que resulta ineludible adaptar nuestra legislación a la de la UE. Y es que, en la actualidad, el acceso no autorizado a un sistema informático ajeno violentando las medidas de seguridad establecidas para protegerlo constituye, por sí mismo, un delito en las legislaciones penales de países como Alemania (parágrafo 202a de su StGB), Italia (art. 615-ter del CP italiano) o Austria (art. 118a de la norma penal austríaca)[594].

Y tercero, características como su potencialidad multiplicadora de las acciones ilícitas hacen que el ciberespacio tenga un gran interés para el Derecho penal. Esto es apreciable, sobre todo, en las conductas de acceso ilícito a sistemas informáticos, dotadas de un efecto criminógeno. No cabe duda, por tanto, de que el ciberespacio es una fuente de riesgos necesitada de control y, atendiendo a las graves repercusiones de los delitos perpetrados en el mismo sobre distintos bienes jurídicos, queda legitimada la intervención

---

592 J.L. Díez Ripollés, *Política criminal y derecho penal -Estudios-*, 2ª ed., Valencia, Tirant lo Blanch, 2013, p. 131. A causa de la importancia de la ciberseguridad, considero que hemos de ser capaces de ir más allá de esa búsqueda de la efectividad en el corto plazo que critica Díez Ripollés. No se trata, por lo tanto, de barrer la Red de ciberdelincuentes con medidas exageradas y cortoplacistas, sino de desarrollar preceptos eficaces y duraderos verdaderamente orientados a los objetivos de tutela que legítimamente perseguimos.

593 Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal,* pp. 64 – 65.

594 J.G. Fernández Teruelo, *Derecho penal e Internet: especial consideración de los delitos que afectan a jóvenes y adolescentes,* , 1ª ed., Valladolid, Lex Nova, 2011, p. 94. La adaptación a las normas internacionales y comunitarias también ha sido progresiva en estos países. Como ya expuse en el capítulo primero de esta investigación, originalmente el parágrafo 202a del StGB tenía una configuración diferente.

del Derecho penal mediante la represión penal autónoma de la conducta de *cracking*[595].

Y digo *cracking*, y no *hacking*, porque es necesario repetir la precisión que ya realicé nada más comenzar esta investigación: a pesar de que en lengua española se tiende a confundir el *hacking* con el *cracking*, estos términos tienen significados distintos cuyo conocimiento resulta inexcusable si se pretende su valoración con miras a su tipificación como conductas típicas[596]. El *hacker* es únicamente una persona que posee grandes habilidades en el manejo de ordenadores, permitiéndole dichas habilidades llevar a cabo investigaciones en los sistemas informáticos no con el objetivo de delinquir, sino, entre otros, con el de avisar de los posibles fallos

[595] Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal,* p. 65.

[596] E. Gutiérrez Mayo, M.ª V. Castro Romero, e I. Pérez Golpe, *Delitos informáticos. Paso a paso. Análisis detallado de las conductas delictivas más comunes en el entorno informático*, 1ª ed., A Coruña, Colex, 2021, pp. 16 y 96 – 100. El *hacker* es una persona que posee amplios conocimientos informáticos y que, gracias a los mismos, es capaz de descubrir fallos de seguridad en los sistemas informáticos. El *cracker*, por su parte, es un sujeto que quebranta, de forma ilícita, cualquier sistema de seguridad informático. Es posible encontrar un ejemplo paradigmático del delito de *cracking* en la STS 310/2015, de 27 de mayo (ECLI:ES:TS:2015:2198). Se trata de un delito completamente distinto del fenómeno conocido como *hacking* de desafío de sentencias como la STS 494/2020, de 8 de octubre (ECLI:ES:TS:2020:3215), en el que el sujeto pretende demostrar su habilidad informática o descubrir fallos en un sistema. El adelantamiento de la barrera protectora se justifica, a mi juicio, por la intencionalidad criminal del sujeto activo, que no deja lugar a dudas respecto a su firme voluntad de lesionar el bien jurídico ciberseguridad.

existentes, permitiendo así la elaboración de técnicas de mejora[597] [598] [599]. Siempre que no incurra en ninguna conducta típica o, habiendo sido contratado por terceros, no se exceda del cometido encomendado, el *hacker* y, por ende, el *hacking* permanecen dentro de la más estricta legalidad. No sucede lo mismo con el *cracker*[600], que se caracteriza, precisamente, por sus fines delictivos durante la utilización de los sistemas informáticos, caracterizándose el *cracking* no solo por la comisión de un hecho delictivo, sino por la intencionalidad de delinquir utilizando como herramientas las redes y sistemas informáticos. Hasta ahora, y durante demasiado tiempo, ha

[597] D. Arroyo Guardeño, V. Gayoso Martínez, y L. Hernández Encinas, *Ciberseguridad*, 1ª ed., Madrid, CSIC – Catarata, 2020, p. 29. El verdadero problema, además de la diferencia entre los *hackers* y los *crackers*, es que los primeros se dividen, a su vez, en distintas categorías fácilmente distinguibles para los profesionales de la informática, pero completamente ajenas para el mundo del Derecho penal, que no puede absorberlas como tal por la confusión que conllevarían. Así, existen los *hackers* de sombrero blanco o *hackers* éticos, que son los profesionales de la ciberseguridad que se atienen a la legalidad al tiempo que ayudan a mejorar la seguridad de la entidad para la que trabajan. Los *hackers* de sombrero gris son considerados algo más maliciosos, puesto que si bien buscan mejorar la seguridad, se valen para conseguirlo de métodos, técnicas y herramientas que no son éticas. Por último, los *hackers* de sombrero negro son los piratas informáticos, quienes estudian y utilizan técnicas y herramientas de ciberseguridad con el objetivo de obtener ganancias personales mediante actividades maliciosas. Por interesante que pueda resultar esta diversidad, no es serio pretender trasladar el sistema de sombreros de colores al Derecho penal, en el que se hace imperativa una distinción radical en lo concerniente a la nomenclatura como la que permite distinguir al *hacker* del *cracker*, pues permite identificar con eficacia al ciberdelincuente.

[598] F. Pérez Bes et al., *Memento Experto en Ciberseguridad*, 1ª ed., Madrid, Francis Lefebvre, 2021, p. 18. El Manual de Tallin definió a los *hackers* como aquellas personas que, mediante su habilidad y sus altas capacidades técnicas, intentan acceder sin autorización al *software* o al *hardware*, pero siempre con fines de investigación. En ningún caso deben confundirse con los *crackers*, quienes se caracterizan por cometer actividades delictivas y son conocidos, también, como *hackers* de sombrero negro o ciberdelincuentes.

[599] Cámara Arroyo et al., *Cibercriminalidad*, p. 100. Fueron los propios *hackers* quienes, a finales de los años 80 del siglo pasado, acuñaron el término *cracker* para referirse a aquellos que realizaban acciones dañinas o delictivas dentro de su comunidad. Actualmente, los *crackers* se caracterizan por realizar actividades con fines criminales como la modificación del comportamiento de redes y sistemas informáticos.

[600] M. Saiz Blanco, "Seguridad de la información", en O. Tejerina (coord.), *Aspectos jurídicos de la ciberseguridad*, Madrid, Ra-Ma, 2020, p. 25. El uso continuado de la palabra *hacker* con una connotación peyorativa o negativa ha sido la causa de que, para la mayoría de las personas, *hacker* signifique lo mismo que *cracker* o ciberdelincuente, cuando esta última es una palabra anglosajona que se refiere de manera específica a los ciberdelincuentes que, con voluntad de hacerlo, llevan a cabo acciones de índole criminal.

prevalecido la confusión terminológica en este ámbito, atribuyendo a la figura del *hacker* o intrusista blanco las características que, en realidad, corresponden al *hacker* y trasladando, a su vez, al *hacker* las connotaciones negativas que corresponden al *cracker*. Existe, sobre todo en el ámbito anglosajón, un enorme espectro de categorías entre el *hacker* y el *cracker* imposible de trasladar al Derecho penal e impropio de una propuesta político-criminal de estas características, que debe estar dotada de una elevada claridad conceptual al tener como objetivo la tipificación de una conducta que, en última instancia, podría conllevar la pena de prisión para una persona. Por todo lo anterior, creo conveniente desechar la figura del *hacker* o intrusista blanco, y utilizar solo los términos *hacking* y *cracking*, puesto que los mismos, sin necesidad de recurrir a la adjetivación, son suficientes para distinguir las conductas legales de aquellas que merecen un reproche penal. Y es que es posible apreciar esta distinción incluso en las definiciones contenidas en diccionarios de ciberseguridad: mientras que el *hacking* consiste en la utilización de las características de algo para llevar a cabo una acción inesperada e imprevista, el *cracking* se define como la intrusión ilegal en un sistema informático[601]. El propio INCIBE[602] distingue en su glosario entre el *hacker* y el *cracker*, definiendo al primero como una persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático con el objetivo de reportar fallos de seguridad y elaborar técnicas para prevenir accesos no autorizados (conducta totalmente alejada de cualquier delito y del Código Penal), y al segundo, literalmente, como un ciberdelincuente que se caracteriza por acceder de forma no autorizada a sistemas informáticos con la finalidad de menoscabar la integridad, la disponibilidad y el acceso a la información disponible en un sitio web o en un dispositivo electrónico. La propia definición de *cracker* no solo equivale a la de ciberdelincuente, sino que, en un ámbito extrapenal,

[601] L. Ayala, *Cybersecurity Lexicon*, 1ª ed., Nueva York, NY, Apress Media LLC, 2016, pp. 41 – 77.

[602] Instituto Nacional de Ciberseguridad de España, *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario,* León, Instituto Nacional de Ciberseguridad de España, 2020, pp. 33 - 47.

encontramos prácticamente descrita la conducta típica del art. 197 bis 1 del CP.

Antes de analizar este delito de acceso ilícito a un sistema informático, delito de intrusión informática, o delito de *cracking*, creo conveniente explicar el motivo por el que el actual art. 197 bis 1 del CP, cuya conducta típica permite, en principio, la persecución de esta clase de accesos, no es suficiente. Como ya he comentado, considero dicho artículo un eslabón en la cadena que conduce a la creación de un delito genérico contra la ciberseguridad, o delito de *cracking*, siendo sin duda el eslabón más cercano, quizá el eslabón previo, a la inclusión en el CP de dicho delito. No obstante, su localización actual lo identifica como un tipo delictivo que ampara principalmente (aunque no en exclusiva) la intimidad y los datos de carácter personal reservados. La necesidad de proteger un bien jurídico distinto, la ciberseguridad, mediante el que se proteja la seguridad de las redes y sistemas informáticos, garantizando su disponibilidad, su integridad y su confidencialidad, conlleva el deber de tipificar los accesos indebidos de manera autónoma, con el objetivo de que las conductas que, pese a encajar en el tipo delictivo, no lesionen bienes jurídicos como la intimidad o los datos de carácter personal reservados puedan ser también castigadas.

Debo señalar, por último, que soy consciente de que la postura que defiendo en relación con la nomenclatura del nuevo artículo es absolutamente minoritaria y que entiendo que, a fuerza de repetirla de manera errónea, se ha generalizado esta identificación científicamente errónea entre el *hacking* y el *cracking*. Comprendo también que, en aras del entendimiento común, existen tendencias contra las que no se puede luchar. No obstante, por motivos de corrección académica, he de reiterar que, con independencia del nombre que finalmente prevalezca, considero que la terminología más adecuada es la que defiendo.

3.5.2.2 Sistema de criminalización

El Derecho penal hace posible la criminalización del *cracking* de dos maneras distintas. La primera de ellas es la creación de tipos específicos o de equivalencia que prevean el mero acceso ilícito a los sistemas informáticos en las conductas típicas en relación con las cuales sea pertinente, opción que tiene como inconvenientes su excesivo casuismo y lo inapropiada que resulta para adaptarse con rapidez a los avances de una tecnología en constante progreso. La segunda, que es mucho más adecuada por adaptarse mejor a las nuevas formas de criminalidad, es establecer un nuevo tipo penal genérico[603].

La redacción del tipo delictivo de *cracking* que propongo es la siguiente, tratándose de una reproducción exacta del actual art. 197 bis 1 del CP: *"El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o a una parte de un sistema de información, o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".*

El *cracking*, tal y como lo he estructurado, se trata de un delito *malum in se* de mera actividad cuya descripción y contenido material se agotan con la realización de la conducta, no siendo necesario que se produzca un resultado distinto del comportamiento mismo. Atendiendo a la forma de la acción, es un delito por comisión, ya que para incurrir en la conducta típica el *cracker* debe realizar la acción prohibida por la norma. En cuanto al resultado, el *cracking* es un delito indudablemente formal, puesto que el resultado coincide en el tiempo con la acción. Al tratarse de un delito común, puede ser autor[604] del mismo cualquier persona que sea dueña y señora del hecho, es

[603] Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 377 – 379.

[604] E. M.ª Gorriz Royo, *El concepto de autor en Derecho penal*, 1ª ed., Valencia, Tirant lo Blanch, 2008, p. 426. Para Welzel, el rasgo general de la autoría es, como explicaré a continuación, el dominio del hecho.

decir, que realice una decisión de voluntad con sentido[605]. Para poder apreciar una coautoría, como en los casos en que varios *crackers* coordinan sus acciones para lesionar el bien jurídico protegido, es necesario que el dominio del hecho delictivo corresponda conjuntamente a todos los participantes[606].

Un matiz específico de los delitos que afectan a la ciberseguridad, que afecta muy especialmente a este delito de *cracking*, es que una de las características de sus autores, los *crackers*, es el rechazo que muchos de ellos sienten hacia las normas establecidas en relación con las redes y sistemas informáticos. En este sentido, en el *cracking* no resulta necesario que el autor participe en los bienes jurídicos para poder considerarle culpable de este delito en sentido material, ya que, de otro modo, la vigencia del ordenamiento jurídico dependería de la aceptación en conciencia de sus normas por parte de los ciudadanos[607].

En cuanto a la forma de culpabilidad, el *cracking* es un delito doloso[608] [609], ya que ciertos requisitos del tipo delictivo tienen una naturaleza muy

---

[605] H. Welzel, *Derecho Penal. Parte General*, Buenos Aires, Roque Depalma Editor, 1956, pp. 105 – 106.

[606] H. Welzel, *Estudios de Derecho penal,* Buenos Aires, B de F, 2007, citado en F. Almenar Pineda, *El delito de hacking,* 1ª ed., Cizur Menor, Navarra, Aranzadi, 2018, pp. 216 - 219. En este sentido, el Prof. Dr. Dr. h. c. mult. José Cerezo Mir sostenía que para que exista coautoría es preciso que varias personas tengan un acuerdo de voluntades para ejecutar el hecho. Así, el dominio del hecho pertenecería de manera conjunta a todos ellos de acuerdo a la teoría de Welzel, llevando a cabo cada una de las personas algún elemento del tipo. Esto es distinto a la codelincuencia, en la que concurren varios delincuentes en la comisión del delito, pese a lo cual es posible que solo uno de ellos sea el autor y los demás sean partícipes.

[607] J. Cerezo Mir, "El delito como acción culpable", *Anuario de derecho penal y ciencias penales*, vol. 49, no. 1, 1996, p. 28. Asunto distinto es la inexistencia de culpabilidad moral, pero sí existe culpabilidad jurídica.

[608] Cerezo Mir, *Curso de Derecho Penal español. Parte General. Tomo II*, p. 130. Aunque el CP español no contiene una definición exacta de dolo, puede deducirse su significado a partir de otros términos que el legislador utiliza para designarlo a lo largo del mismo, como "intención", "malicia" o actuar "a sabiendas".

[609] J. Cuello Contreras, "Acción, capacidad de acción y dolo eventual", *Anuario de derecho penal y ciencias penales*, vol. 36, no. 1, 1983, pp. 95 – 98. No es posible considerar que media dolo eventual en ninguna de las categorías propuestas: primera, la dificultad que requiere vulnerar unas medidas de ciberseguridad obligatoriamente complejas impide que la acción realizada por el autor pueda, en ningún caso, definirse como indiferente, por mucho que este sea intelectualmente capaz de prever la producción del resultado; segunda, el carácter lineal de estas nuevas tecnologías hace

compleja, como en el caso de la vulneración de medidas de seguridad: el *cracker*, para llegar a vulnerarlas, debe ser plenamente consciente de ello por el indudable esfuerzo intelectual que, en mayor o menor medida, requiere una acción de estas características, y debe desear el resultado, puesto que la misma necesita una motivación. Así, no cabe duda de que el autor del delito debe tener siempre la intención de cometerlo realizando todos los elementos recogidos en el tipo delictivo[610], siendo prácticamente inexistentes las

evidente la unión entre acción y resultado (se introduce la contraseña para acceder a un sistema informático en caso de que sea correcta, no esperando ningún otro resultado distinto, ni en sentido positivo ni en sentido negativo), de manera que en todos los casos la acción del autor está dirigida a la producción del resultado (la intrusión), sin que pueda admitirse que la interposición de hipotéticos elementos neutralizadores del factor de riesgo -por otro lado, carentes de lógica en sí mismos si atendemos a la voluntad y al actuar del sujeto activo- hagan que finalmente no se produzca; tercera, tampoco puede considerarse que el dolo eventual, en la actualidad, equivalga al erróneamente denominado dolo alternativo, puesto que no resulta posible que la conducta del sujeto activo abarque dos resultados queridos pero excluyentes entre sí, toda vez que, de nuevo, el carácter lineal de estas tecnologías solo permite frente a los intentos de intrusión intelectualmente elaborados resultados o bien negativos (fracaso de la intrusión e imposibilidad de acceder al sistema informático), o bien positivos (triunfo de la intrusión y acceso al mismo), con la muy remota posibilidad intermedia de que, ante el intento de una cantidad inusitadamente alta de accesos, generalmente llevada a cabo mediante programas orientados a introducir distintas contraseñas de forma automática y masiva, un sistema informático mal preparado para esta eventualidad sucumba y deje de estar disponible aun sin haber permitido el acceso del ciberdelincuente, y posteriormente impida el acceso a quienes sí disponen de credenciales legítimas.

[610] C.M. Romeo Casabona, “Sobre la estructura monista del dolo. Una visión crítica”, en H. Joachim Hirsch, J. Cerezo Mir y E. Alberto Donna (dirs.), *Hans Welzel en el pensamiento penal de la modernidad*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2005, pp. 460 – 461. De acuerdo con Romeo Casabona, el dolo es, parafraseando a Welzel, la voluntad del sujeto activo de realizar los elementos del tipo delictivo.

posibilidades de que concurra el tipo culposo o imprudente[611] [612] [613] por las propias características que lo configuran, aspecto ya alabado por la doctrina en relación con la actual redacción del art. 197 bis 1 del CP[614].

La intencionalidad del sujeto activo condicionará la consideración como delito instrumental del *cracking*. Cuando este delito se lleve a cabo como medio para la comisión de otros que afecten a bienes jurídicos distintos, podrá considerarse un delito instrumental. No sucederá lo mismo cuando el ciberdelincuente no busque lesionar ningún otro bien jurídico excepto la ciberseguridad, en cuyo caso se tratará de un delito fin en el que el *actus reus*

[611] C.M. Romeo Casabona, "La peligrosidad y el peligro en la estructura del tipo del delito imprudente", en J.L. Díez Ripollés, C.M. Romeo Casabona, L. Gracia Martín y J.F. Higuera Guimerá (eds.), *La ciencia del derecho penal ante el nuevo siglo: libro homenaje al profesor doctor don José Cerezo Mir*, Madrid, Tecnos, 2002, p. 947. Debe individualizarse de manera coherente el diferente desvalor de lo injusto de cada delito imprudente en relación con su respectiva modalidad dolosa. Establecer que la pena de la forma imprudente sea inferior a la de la forma dolosa es, en este sentido, la solución legislativa correcta, puesto que se guarda la adecuada correspondencia o proporcionalidad de la imprudencia en relación con la comisión dolosa del hecho. No obstante, considero que la comisión imprudente del delito de *cracking* es prácticamente imposible. De ahí que el tipo imprudente no exista en la actual redacción del art. 197 bis 1 del CP ni yo proponga modificación o mejora alguna relativa a la imprudencia en mi propuesta de *lege ferenda.*

[612] J. Cuello Contreras, *El derecho penal español. Parte general. Volumen II. Teoría del delito (2)*, 1ª ed., Madrid, Dykinson, 2009, pp. 360 – 361. Las características del delito de *cracking* y la imposibilidad de un tipo imprudente en relación con el mismo convierten en más cierta que nunca la afirmación de Hans Welzel de que el legislador no puede prever todas las situaciones concretas que exigen atenerse al cuidado debido y a su medida. Para ayudar a precisar el tipo del delito imprudente, es necesario acudir a la figura heurística del hombre cuidadoso y a dos criterios que sirven para concretar el cuidado debido: primero, el juicio de adecuación o previsibilidad objetiva de que ciertas acciones crean peligros para los bienes jurídicos; segundo, el riesgo permitido. La acción que se encuentre por debajo de lo adecuado en cuanto a cuidado objetivo debe entenderse como prohibida, y quien no sea capaz de actuar respetando este límite deberá abstenerse de actuar. No es posible aplicar esta teoría al delito de *cracking*, ya que resulta imposible la vulneración de medidas de seguridad robustas (las únicas admitidas para ser consideradas como tales) en ausencia de la voluntad real e inequívoca de vulnerarlas a través de acciones intelectualmente exigentes.

[613] C. Pérez del Valle, *La imprudencia en el Derecho penal. El tipo subjetivo del delito imprudente*, 1ª ed., Barcelona, Atelier, 2012, p. 43. Siguiendo a Cerezo Mir, es importante abandonar la idea de la finalidad potencial y distinguir entre finalidad y dolo como finalidad referida a un tipo. En el tipo imprudente no hay una acción, una resolución de voluntad, sino inobservancia del cuidado objetivamente debido, que resulta completamente imposible en un contexto tecnológico que demanda acciones intelectualmente elaboradas.

[614] Romeo Casabona, *Derecho Penal, Parte Especial*, p. 286.

no estará vinculado a un propósito que trascienda la realización del acceso ilícito[615] [616].

La consecuencia jurídica del delito de *cracking* debe ser, en mi opinión, una pena de prisión[617] [618] de seis meses a dos años, siendo esta una pena menos grave de acuerdo a la clasificación basada en su naturaleza y duración (art. 33.3.a) del CP) que permite encuadrar este delito entre los delitos menos graves del art. 13.2 del CP. Considero esta pena apropiada[619], toda vez que hará posible que el juzgador recorra una banda punitiva que, aunque no es muy amplia, le permitirá dar una respuesta adecuada a cada caso concreto, imponiendo una pena casi simbólica a aquellos casos donde apenas se lesione el bien jurídico protegido[620], pasando por los casos que serán mayoría, en los que sí se lesionará la ciberseguridad, pero un análisis de los hechos hará recomendable la suspensión de la ejecución de la pena privativa

[615] Cerezo Mir, *Curso de Derecho Penal español. Parte General. Tomo II*, p. 131.

[616] J. Cerezo Mir, *Curso de Derecho Penal español. Parte General. Tomo III. Teoría Jurídica del Delito II*, 1ª ed., Madrid, Tecnos, 2002, p. 114. Deben concurrir los elementos volitivo e intelectual, algo inevitable si se consuma con éxito una acción tan elaborada como la superación de medidas de ciberseguridad complejas.

[617] L. Gracia Martín, M.A. Boldova Pasamar y C. Alastuey Dobón, *Lecciones de consecuencias jurídicas del delito*, 5ª ed., Valencia, Tirant lo Blanch, 2016, pp. 25 – 26. Pena privativa de libertad prevista en el art. 35 del CP para cuya determinación, como sostiene F. De Marcos Madruga, "Artículo 35", en M. Gómez Tomillo (dir.), *Comentarios prácticos al Código Penal. Tomo I. Parte General. Artículos 1 – 137*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, p. 501, he tenido en cuenta el efecto deshumanizador de las estancias en prisión.

[618] J. Antón Oneca, *Obras. Tomo II*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2002, p. 52. Antón Oneca menciona los resultados negativos, incluso, de las penas cortas carcelarias a causa de sus efectos corruptores sobre los delincuentes primarios y de la escasa intimidación que ejercen sobre los crónicos.

[619] Cerezo Mir, *Curso de Derecho Penal español. Parte General. Tomo I*, p. 29. La considero apropiada, entre otros motivos, porque se adapta a los criterios de Cerezo Mir, quien sostenía que la pena debía ser justa, adecuada a la gravedad del delito, y, además, necesaria para el mantenimiento del orden social.

[620] J. Cerezo Mir, *Temas fundamentales del Derecho Penal. Tomo III*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2006, p. 194. Comparto el criterio de Cerezo Mir cuando afirma que las penas privativas de libertad de corta duración solo sirven para desarraigar al delincuente al separarle de su familia y hacerle perder su trabajo, en el caso de que lo tuviera. Además, impiden trabajar de manera eficaz en su reeducación y en su reinserción social. La pena simbólica que propongo teniendo en cuenta estas ideas impediría que el delincuente primario y ocasional, tan habitual en el ámbito de los accesos ilícitos, quedase expuesto a la perniciosa influencia de los delincuentes habituales, otorgándole una segunda oportunidad para obrar bien.

de libertad (art. 80.1 del CP), hasta los casos más graves que harán necesaria la imposición de una pena privativa de libertad de dos años[621] [622]. La doctrina ya ha analizado, incluso, las particularidades de este delito cuando lo cometen menores de edad, así como sus consecuencias específicas en estos casos[623]. Esto convertirá al delito de *cracking* en una norma versátil en manos

[621] J.L. Díez Ripollés, *Delitos y penas en España*, 1º ed., Madrid, Catarata, 2015, p. 105. La pena abstracta que propongo es el fruto de una reflexión en la que he tenido en cuenta no solo las consecuencias jurídicas de la mayoría de delitos analizados en esta investigación, sino el hecho de que nuestra tasa de encarcelamiento es la más alta de toda Europa occidental. Sabiendo que estos números tan elevados no son fruto de una elevada tasa de criminalidad, sino que la misma se mantiene tradicionalmente en los niveles más bajos de Europa occidental, siendo esta, a su vez, una de las regiones con menor criminalidad del mundo, considero que es una manera de que no se perpetúe una política criminal que castiga con la pena de prisión un excesivo número de delitos y que, además, impone unas penas de prisión, por lo general, de más larga duración que las de países de nuestro entorno como Alemania, Francia o Reino Unido. Una pena como la que propongo, aplicable solo en los casos más extremos, evitaría también los perniciosos efectos sobre posibles delincuentes ocasionales que describe M.A. Boldova Pasamar, "Penas privativas de libertad", en L. Gracia Martín (coord.), *Tratado de las consecuencias jurídicas del delito*, 1ª ed., Valencia, Tirant lo Blanch, 2005, pp. 93 – 108, además de ser también adecuada a los fines de protección de bienes que justifican la incriminación de una conducta, como defiende N.J. De la Mata Barranco, *La individualización de la Pena en los Tribunales de Justicia. La atención a la finalidad de la pena, la gravedad del hecho y las circunstancias personales del procesado en la Jurisdicción Penal, en su vinculación a la exigencia de imposición de penas proporcionadas*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2008, p. 50.

[622] R. Rodríguez Fernández, "Las penas en el Código Penal de 1995", en R. Rodríguez Fernández y P. Simón Castellano (autores), *La pena de ingreso en prisión. Regulación actual y antecedentes históricos*, 1ª ed., Madrid, Wolters Kluwer, 2021, pp. 281 – 282. Las propias características del delito de intrusión en un sistema de información, que lo convierten en un objetivo idóneo para las tentativas a través de los intentos de acceso mediante múltiples ataques, obligan a tener en cuenta, precisamente, las consecuencias jurídicas de la comisión del mismo en grado de tentativa, siempre que se trate de intentos peligrosos (como aquellos en los que se utiliza un *software* específico para tratar de acceder destruyendo o desactivando las medidas de ciberseguridad establecidas), y no de vulgares intentonas (como aquellas en las que se introducen un par de veces los caracteres que, se espera, pueden corresponder a una contraseña; corresponde a la profesionalidad del experto en seguridad informática impedir que esta conducta no pueda repetirse más de un cierto número de veces antes de bloquear la petición de usuario y contraseña para inmediatamente alertar del suceso al legítimo titular de la cuenta). En este caso, al tratarse de un delito no consumado, sino intentado, corresponderá la imposición de la pena inferior en uno o dos grados a la señalada para el delito consumado, atendiendo a criterios como el peligro inherente al intento y el grado de ejecución alcanzado.

[623] G. Martínez Galindo, "Motivación criminal de los adolescentes en el ciberespacio", en A. Abadías Selma, S. Cámara Arroyo, y P. Simón Castellano (coords.), *Tratado sobre delincuencia juvenil y responsabilidad penal del menor. A los 20 años de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores,* 1ª ed., Madrid, Wolters Kluwer, 2021, pp. 511 – 513. Las conductas de mera intrusión en un sistema de información se sancionarían mediante el art. 197 bis 1 del CP, pero, por lo

de unos juzgadores que necesitarán una herramienta como esta para enfrentarse a una realidad compleja y en constante cambio, como la que caracteriza a la ciberseguridad. Supondrá, también, un equilibrio entre el sector doctrinal que rechaza que el Derecho penal castigue los meros accesos ilícitos y el que, siendo partidario de lo anterior, demanda un mayor rigor punitivo[624].

3.5.2.3 Consideración del *hacking* como conducta lícita

La aceptación del *hacking*[625] o intrusión blanca como conducta lícita parte de una base errónea no desde un punto de vista conceptual, sino terminológico. Ya he explicado que las características que se atribuyen al intrusista blanco corresponden, en realidad, al *hacker*, no siendo necesario ningún adjetivo para definir una conducta como el *hacking* que es, por sí

---

general, estaríamos ante la obligación de apreciar un concurso medial con otro delito posterior, ya que el menor delincuente suele ir más allá del mismo. Es reveladora, en este sentido (aunque no esté específicamente relacionada con el art. 197 bis 1 del CP), la SAP de Soria 5/2018, de 7 de febrero (ECLI:ES:APSO:2018:37), en la que el menor de edad va más allá de la intrusión en el sistema de información y realiza modificaciones en el contenido del mismo, de manera que, habiendo incurrido en el tipo delictivo previsto en el art. 197.2 del CP, se le impone una medida de cien horas de prestación de servicios en beneficio de la comunidad. No obstante, la solución a esta clase de ciberdelincuencia prematura estriba en la educación y en la prevención, especialmente en lo que respecta a enseñar a distinguir entre aquellas conductas admisibles que evidencian una gran capacidad de actuación en relación con los ordenadores y las que constituyen un delito, objetivo sin duda alcanzable mediante la creación de asignaturas adaptadas a cada nivel educativo.

624 C.M. Romeo Casabona, *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las nuevas tecnologías de la información*, Madrid, Editorial Fundesco, 1988, citado en M. Barrio Andrés, *Ciberdelitos: amenazas criminales del ciberespacio*, 1ª ed., Madrid, Reus Editorial, 2017, p. 131. Otro aspecto que he tenido en cuenta al establecer esta pena abstracta es el reconocimiento unánime por parte de la doctrina de la incapacidad de motivación del cibercriminal, que convierte a las medidas preventivas en las más eficaces por encima de la amenaza penal. Y es que tanto los técnicos en ciberseguridad como los criminólogos o los penalistas coinciden en la necesidad de abogar por medidas de seguridad preventivas en la lucha frente a este tipo de delincuencia, siendo preferible una razonable medida disuasoria *ex ante* que evite brechas de seguridad que un instrumento de fiscalización *ex post*. Se trata, en suma, de intentar prevenir las intrusiones en sistemas de información, en lugar de reprimirlas con un rigor punitivo desmedido.

625 A.T. Keenlyside et al., “El *hacking* desde una perspectiva legal, criminológica y técnica”, *Revista Aranzadi Doctrinal,* no. 6, 2021, p. 1. La existencia del *hacking* era previsible atendiendo al nivel de innovación y evolución de la tecnología digital y a la manera en que se ha incorporado poco a poco a nuestra sociedad.

misma, acorde a la legalidad en su actual configuración. El Derecho penal no debe intervenir en conductas que no suponen una lesión para la ciberseguridad, como el estudio y la investigación de las vulnerabilidades de una red o sistema informáticos a título personal por parte de un *hacker*, siempre que su conducta quede dentro de los márgenes de la ley.

Es el caso de las pruebas de penetración (*pentesting*), consistentes en la realización de ataques contra un sistema de información por parte de un *hacker* con la finalidad de descubrir sus posibles vulnerabilidades, contando siempre con el consentimiento (o, más común aún, con la petición previa) de su propietario, lo que las convierte en atípicas[626] (pues no hay que olvidar que el art. 197 bis 1 exige al sujeto activo actuar en ausencia de la debida autorización, autorización que debe entenderse otorgada cuando existe un acuerdo extrapenal en este sentido), o, como mínimo, en fácilmente defendibles esgrimiendo el art. 20.7 del CP, que exime de responsabilidad criminal a quien, como en el caso del *hacker*, obre en cumplimiento de un deber o en el ejercicio legítimo de un derecho, oficio o cargo.

No puede abordarse esta conducta de otra manera en un escenario en el que se está generalizando la contratación de los servicios de los *hackers* por parte de empresas privadas para que, como profesionales de la informática, analicen específicamente las vulnerabilidades de las redes y sistemas informáticos de quien les ha contratado. En este caso, la clave estará en la existencia de un contrato que refleje la voluntad del contratante, quien, asesorado a nivel técnico en la redacción del mismo por sus propios especialistas en informática, acepta que el *hacker* lleve a cabo una serie de maniobras informáticas orientadas a poner a prueba y analizar las vulnerabilidades de sus redes y sistemas informáticos, permitiendo la elaboración posterior de técnicas de mejora. La actuación por parte del *hacker* dentro de los márgenes de la legalidad en el primer caso, o de acuerdo a lo establecido en el contrato en el segundo, impide que sus actuaciones

[626] Pérez Bes et al., *Memento Experto en Ciberseguridad*, pp. 271 – 272.

puedan encuadrarse dentro del delito de *cracking*, por los motivos técnicos expuestos en el párrafo anterior.

Más complejo es el escenario en el que el *hacker,* sin intención de lesionar la seguridad de las redes y sistemas informáticos, incurre en la conducta típica, bien porque ha ido demasiado lejos en sus investigaciones, en el primer caso, o porque se ha excedido del acuerdo establecido en el segundo (y, por lo tanto, accede igualmente a una parte de un sistema de información sin estar debidamente autorizado para ello). En este caso, habrá que analizar la conducta del *hacker*, quien deberá informar inmediata y directamente a los administradores o a los encargados de garantizar la ciberseguridad con el objetivo de reducir al máximo la lesión a este nuevo bien jurídico[627] [628]. Cumplido dicho requisito, y comprobados por especialistas el alcance y las consecuencias de la intrusión, especialmente en lo concerniente al deber de cuidado del profesional de la informática[629] [630], el resultado no puede ser otro que la absolución, ya que lo contrario, sobre todo

[627] J. Antón Oneca, *Obras. Tomo I,* 1ª ed., Santa Fe, Rubinzal – Culzoni, 2000, pp. 138 – 142.

[628] E. Garro Carrera y A. Asúa Batarrita, *Atenuantes de reparación y de confesión. Equívocos de la orientación utilitaria. A propósito de una controvertida Sentencia del Juzgado de lo Penal no. 8 de Sevilla*, 1ª ed., Valencia, Tirant lo Blanch, 2008, p. 69. Si acudimos al Derecho comparado, en el ordenamiento jurídico austríaco la valoración del esfuerzo por reparar el daño tiene cabida en la atenuante genérica del parágrafo 34.1.15 de su StGB y, sobre todo, en el aumento de posibilidades de derivar el caso a una respuesta extrapenal, como creo que debe suceder cuando el *hacker* informe con rapidez sobre lo sucedido.

[629] A. Daunis Rodríguez, *La graduación de la imprudencia punible*, 1ª ed., Navarra, Aranzadi, 2020, pp. 69 – 72. La estandarización del deber de cuidado en relación con el *hacking* es fundamental, y ello puede conseguirse mediante reglas o normas técnicas que expresen formas de conducta aparejadas a peligros característicos de las mismas, así como las medidas idóneas para evitarlos. Como reitera la SAP de Navarra 131/2000, de 16 de octubre (ECLI:ES:APNA:2000:1235), resultará esencial la labor de individualización judicial; solo así podrán valorarse las características propias de cada caso en particular y diferenciarlos.

[630] J. Cerezo Mir, *Temas fundamentales del Derecho Penal. Tomo I*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2001, p. 396. Reitero que esta vía tendría un escaso recorrido, ya que es imposible encuadrar al autor imprudente de este delito en la categoría desarrollada por Welzel, quien exigía para poder considerar autora de un delito culposo a una persona que esta infringiese a través de una acción el cuidado exigible en el tráfico y causase en forma no dolosa un resultado típico. Nadie supera medidas de ciberseguridad complejas sin proponérselo, y si estas no son complejas, no pueden considerarse medidas adecuadas.

en el caso de los especialistas, conduciría a entorpecer de manera innecesaria las actividades informáticas y a la creación de una sensación de incertidumbre legal incompatible con un mundo en el que los *hackers* colaboran, incluso, en las investigaciones penales[631], y en el que ya existe la tecnología capaz de encontrar y reparar en segundos las brechas de ciberseguridad que un ser humano tardaría meses o años en detectar[632] [633].

3.5.3 La creación de un nuevo título en el CP para los delitos contra la ciberseguridad

Basándome en el desorden estructural de la actual redacción del CP en relación con los delitos que afectan a la ciberseguridad, considero necesaria la creación de un nuevo título en el mismo no para todos, sino exclusivamente para algunos de ellos, siempre que se cumplan dos requisitos: primero, que la ciberseguridad pueda ser considerada como un bien jurídico protegido autónomo; segundo, que exista un delito genérico contra la ciberseguridad, como el de intrusión, para que pueda encabezar este título de nuevo cuño, siendo su tipo delictivo principal y dotando de coherencia no solo a su propia existencia, sino a la conveniencia, o ausencia de ella, de trasladar otros delitos al mismo. Estos dos aspectos, en los que profundizaré a continuación, son los dos pilares sobre los que debe

---

631 R. López Picó, "Investigación tecnológica en el proceso penal: *hacking* legal", en F. Bueno de Mata (dir.), *Fodertics 7.0: estudios sobre derecho digital,* Granada, Comares, 2019, p. 349. Más que establecer distinciones entre los distintos tipos de *hacking*, procede realizar una separación conceptual entre las conductas legales y las delictivas, y la manera más clara es la utilización de los términos *hacking* y *cracking.*

632 D. Brumley, "The White-Hat Hacking Machine: Meet Mayhem, winner of the DARPA contest to find and repair software vulnerabilities", *IEEE Spectrum*, vol. 56, no. 2, 2019, p. 35. Aunque la llamada ciberdefensa autónoma aún necesita desarrollarse en muchos sentidos, se la considera el principio de una revolución tecnológica en el ámbito de la seguridad informática, y ya se está utilizando por el gobierno estadounidense y por importantes empresas tecnológicas y aeroespaciales. En la actualidad, esta tecnología advierte de problemas de seguridad relacionados con el *software* que, posteriormente, solventan expertos en la materia. Aunque esta colaboración entre los seres humanos y las máquinas continuará durante algún tiempo, se espera que en el futuro la IA trabaje sola no solo detectando, sino también arreglando los déficits de ciberseguridad. Esto nos obligará a plantearnos de nuevo todas estas cuestiones desde el Derecho penal.

633 Rueda Martín, *La adaptación del derecho penal al desarrollo social y tecnológico,* pp. 373 – 376.

descansar la creación de este nuevo título, motivo por el cual resulta tan importante llevar a cabo un análisis minucioso y detallado que evidencie su importancia y los consolide.

Los delitos que debe contener el nuevo título son los delitos contra la ciberseguridad, es decir, aquellos que lesionan de cualquier manera la seguridad física o lógica de las redes o sistemas informáticos, afectando así a su disponibilidad, integridad o confidencialidad. Deben incluirse en el mismo, tras un análisis en profundidad de los mismos, algunos de los tipos delictivos que recogen conductas idóneas para este resultado y que no encajen mejor en otra ubicación, descartando aquellos otros que, por sus características, no lo hacen.

No obstante, no creo adecuado, en ningún caso, el traslado al nuevo título de todos los delitos que afectan a la ciberseguridad analizados en esta investigación. Después del análisis, considero apropiada su división en tres categorías tomando como criterio la adecuación de su inclusión en el CP de acuerdo a la actual redacción del texto: primera, delitos cuya ubicación es adecuada y cuyo traslado al nuevo título resulta innecesario, como en el caso de los delitos contenidos en los arts. 238.3 (descubrimiento de claves para la sustracción del contenido), 238.4 (uso de llaves falsas) y 238.5 (inutilización de sistemas específicos de alarma o guarda), puesto que no solo son inseparables del art. 238 del CP, dedicado al robo con fuerza en las cosas, sino que se han adaptado por completo al desarrollo tecnológico resultando idóneos para la protección de las víctimas frente al quebrantamiento de las medias de ciberseguridad como medio para hacerse con ciertos bienes, siendo suficiente para su actualización alguna revisión ocasional del tipo o, cuando procedan, nuevas interpretaciones jurisprudenciales más acordes al estado de la tecnología en un momento determinado; segunda, delitos cuya inclusión es inadecuada y cuyo traslado al nuevo título resulta necesario, siendo este el caso de artículos como el 270.5, párrafos c) y d), del CP o el 270.6, que no solo tienen una escasa aplicación jurisprudencial sino que suponen la tipificación de conductas muy alejadas de la concreta lesión de los derechos de propiedad intelectual que pretende proteger el art. 270, y

conducen a desequilibrios como castigar con una pena similar a la del tipo básico unos actos preparatorios de posteriores comportamientos recogidos en el mismo, y que bien podrían encuadrarse en un artículo dedicado a los actos preparatorios dentro del nuevo título; tercera, delitos cuya inclusión es inadecuada pero cuyo traslado al nuevo título no resulta necesario, puesto que lo que procede es su traslado a otro distinto, siendo el caso del art. 277, que se encuentra recogido entre los delitos relativos a la propiedad industrial cuando sería más adecuado utilizar como criterio sistematizador el bien jurídico protegido para trasladarlo junto a los delitos de traición y contra la paz o la independencia del Estado y relativos a la Defensa Nacional, toda vez que la divulgación prevista debe cumplir el requisito típico de perjudicar a esta última.

CAPÍTULO IV

CIBERSEGURIDAD Y DERECHO PENAL EN TECNOLOGÍAS EMERGENTES SANITARIAS

4.1 Las nuevas tecnologías como elemento instrumental para la ciberseguridad en el ámbito sanitario

El avance de la tecnología en el ámbito de las TIC[634] conlleva, a causa de sus diversas aplicaciones en el ámbito sanitario, un escenario completamente nuevo a nivel criminológico y político-criminal en el que es posible apreciar un salto no solo cuantitativo, sino también cualitativo, al ser los medios para cometer los ciberataques muy variados en lo que concierne a sus niveles de riesgo y a su escala de impacto potencial[635]. Además de los bienes jurídicos protegidos ya analizados en anteriores capítulos de esta investigación, las nuevas tecnologías permiten, a un tiempo, que se vean amenazados y defendidos otros indiscutiblemente relevantes que, hasta ahora, no han tenido relación con la misma, como la vida humana independiente. Ante la enorme importancia del riesgo existente para viejos y nuevos bienes jurídicos protegidos, incluyendo la propia ciberseguridad, es imperativo que nazca junto a este nuevo escenario un interés más decidido que nunca de dotar a las redes y sistemas informáticos de las infraestructuras críticas sanitarias de un nivel lo más elevado posible de seguridad física y

634 J.M. Palma Herrera, "Inteligencia artificial y lucha contra la delincuencia. Potencialidad y peligros en el mundo global", en F.H Llano Alonso y J. Garrido Martín (eds.), *Inteligencia artificial y Derecho. El jurista ante los retos de la era digital,* Cizur Menor, Navarra, Aranzadi, 2021, p. 286. Aunque en el Derecho penal siempre se han utilizado datos para la persecución de los delincuentes, la novedad de la IA radica en que, por primera vez, el tratamiento de los datos lo lleva a cabo un sistema dotado de una capacidad de análisis que multiplica de manera extraordinaria la de un analista humano. Como expondré en este capítulo, en materia de ciberseguridad en el ámbito sanitario, la IA también complementa o mejora las medidas de seguridad que hasta ahora ideaban y estructuraban solo seres humanos, aumentado esto su eficiencia.

635 D. Fernández Bermejo, "Algunas cuestiones jurídico penales sobre la ciberdelincuencia", en E. Monterroso Casado (dir.), *Inteligencia Artificial y Riesgos Cibernéticos. Responsabilidades y Aseguramiento,* Valencia, Tirant lo Blanch, 2019, p. 329. Esto conllevará inevitables cambios legales.

lógica, siendo este un desafío en el que las nuevas tecnologías serán tanto una nueva amenaza como una oportunidad[636] de perfeccionar las medidas de ciberseguridad existentes o, incluso, de crear otras inéditas y mucho más avanzadas.

Los hospitales y los centros sanitarios mantienen, por supuesto, la importancia que les adjudiqué en el anterior capítulo de esta investigación, toda vez que la mayor parte de las conductas a analizar se desarrollarán en su interior. No obstante, las características de las nuevas tecnologías, como la tecnología ponible, vestible, o tecnología corporal (lamentable traducción de *wearable technology*[637]), así como la especialización de ciertos establecimientos (como los biobancos[638]), me obligan a ir más allá de sus muros en mi análisis. Las medidas de ciberseguridad, para ser efectivas, deberán poder desplegarse dejando atrás muchas de las limitaciones que imponían estadios tecnológicos ya obsoletos.

Aunque, por motivos de orden, dedicaré un apartado a cada una de estas nuevas tecnologías, es importante aclarar que la IA, la robótica, los drones, los hospitales inteligentes, el IdCM, la nube sanitaria, la salud electrónica, la tecnología corporal y los demás dispositivos externos al cuerpo humano están íntimamente ligados entre sí: no es posible entender la robótica

---

[636] M.J. De la Calle, "IA: Problema y solución de la Ciberseguridad"*, Contact Center Call Center & IP Solutions,* no. 87, 2017, pp. 32 – 33. Aunque se admite que la IA está llamada a producir una revolución como herramienta que permitirá impulsar campos como el sanitario, también supondrá la creación de nuevos riesgos, como la dependencia para su buen uso respecto de los algoritmos y del entorno en que funcionará. Coincido con esta idea: no hay una correlación entre la utilización de más tecnología y la mejora en el nivel de ciberseguridad, sino que ante la existencia de una nueva tecnología aumentan los beneficios y los riesgos. La manera en que esto afecte a la ciberseguridad dependerá de la adecuada gestión de los mismos.

[637] M. Barrio Andrés, *Internet de las cosas,* 1ª ed.*,* Madrid, Reus, 2018, p. 45. Los datos obtenidos a través de esta tecnología tienen una importancia jurídica innegable, puesto que la información almacenada permite determinar la localización geográfica de un individuo, así como si ha sido lesionado a causa de un accidente.

[638] J. Kaye et al., *Governing biobanks: understanding the interplay between law and practice,* 1ª ed., Oxford, Hart Publishing Ltd., 2012, pp. 30 – 48. Los avances en las investigaciones genéticas introdujeron nuevos desafíos para los marcos regulatorios a nivel mundial. Hoy, la ciberseguridad es un desafío adicional que, siguiendo dicha tendencia, también deberá adaptarse a las necesidades de la ciencia y a su metodología.

sin entender la IA, y no es posible la existencia de hospitales inteligentes sin, al menos, IdCM. Se trata, por lo tanto, de tecnologías interdependientes que, muchas veces, interactúan. Todas ellas comparten, además, una característica que permite establecer un patrón común: su carácter instrumental respecto de las medidas de ciberseguridad, a las cuales se ensamblarán para elevar el grado de seguridad de redes y sistemas informáticos, pero tratándose en todos los casos de meras herramientas.

Como expondré muy brevemente, el estado de la tecnología actual impide atribuir a cualquiera de estas nuevas tecnologías la autoría dolosa directa, la autoría dolosa mediata o la responsabilidad por imprudencia respecto a un hecho delictivo tipificado en el CP.

Ya desde principios de siglo existía un enorme optimismo en relación con la utilización de las nuevas tecnologías en el ámbito sanitario. Sobre todo, el objetivo era resolver problemas prácticos, como la distancia que en ocasiones separaba al médico de sus pacientes. Incluso entonces, cuando la ciberseguridad se encontraba en una etapa de desarrollo casi embrionaria, la doctrina recalcó la importancia de desarrollar de forma paralela a la implementación de estos avances unas medidas de seguridad informática avanzadas, considerando que, de otro modo, los nuevos sistemas sanitarios no resultarían viables[639]. No fue necesario que pasasen muchos años antes de que tecnologías como los programas de diagnóstico médico basados en el análisis probabilístico alcanzasen un nivel de rendimiento equiparable a los de un facultativo experto, superando las expectativas de los especialistas más exigentes y preparando el terreno para, una vez desarrollada la regulación legal necesaria, implementar un sistema sanitario basado en las nuevas tecnologías[640]: una verdadera medicina digital[641] necesitada de avanzadas

[639] J. Kaiser, “Blueprint for cyber health care”, *Science*, vol. 287, no. 5458, 2000, p. 1551.

[640] S.J. Rusell y P. Norvig, *Inteligencia Artificial. Un Enfoque Moderno*, 2ª edición, Madrid, Pearson Educación, 2004, p. 32. A pesar de esto, sus niveles de ciberseguridad no se desarrollaron en la misma medida.

[641] A. Coravos et al., “Digital Medicine: A Primer on Measurement”, *Digital Biomarkers,* vol. 3, no. 2, 2019, p. 33. La medicina digital llegará a estar tan implantada que se la conocerá, sencillamente, como medicina.

medidas de seguridad para las redes y sistemas informáticos sobre las que se está construyendo.

Con objeto de comprenderla, es necesario analizar de manera individual estas nuevas tecnologías, las avanzadas e innovadoras medidas de ciberseguridad que permitirán crear o el modo en que adaptarán las ya existentes, y la manera en que dichas medidas influirán en los delitos que afectan a la ciberseguridad recogidos en el CP español.

4.2 Inteligencia Artificial

4.2.1 Desafíos para la IA en relación con los delitos que afectan a la ciberseguridad

La IA es una nueva tecnología que pone a prueba nuestro ordenamiento jurídico-penal[642]. Es un *software* codificado con capacidad para tomar decisiones que puede ejecutar cualquier tarea y acción igual que un ser humano, pero con una capacidad de computación superior a la biológica. Su funcionamiento puede estructurarse en tres fases: primero, capta información o datos a través de captadores y sensores; segundo, lleva a cabo su interpretación y tratamiento mediante procesadores; tercero y último, toma una decisión.

Los algoritmos son secuencias lógicas que ejecutan una tarea o actividad mediante el cálculo, resolviendo problemas. Es esencial comprender que, en la actualidad, solo existe la IA débil[643], orientada a la

[642] F. Miró Llinares, "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología. Tercera época,* no. 20, 2018, p. 89. Uno de los principales problemas en relación con la IA es la confianza excesiva e irresponsable que cierto sector de la doctrina tiene en los algoritmos, cuando estos pueden no solo no ser objetivos, sino reflejar las dudas y los prejuicios de sus programadores. Coincide con este criterio I. Lledó Benito, "Visión del Derecho penal en relación con la robótica, IA y la ciberdelincuencia", en F. Lledó Yagüe, I. Benítez Ortúzar y O. Monje Balmaseda (dirs.), *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0. Los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes,* 1ª edición, Madrid, Dykinson, 2021, pp. 156 – 162.

[643] E. Iñigo Corroza, P. Sánchez-Ostiz, y M.M. Pereira Garmendia, "Cibercriminalidad", en E. Valpuesta Gastaminza y J.C. Hernández Peña (coords.), *Tratado de Derecho*

resolución de problemas muy concretos, reactiva y escasamente flexible. Si bien computa, no razona, y aprende gracias a ejemplos que le permiten desarrollar operaciones repetitivas, estando frecuentemente orientada a una sola tarea. A día de hoy, la IA fuerte, en teoría proactiva, capaz de resolver problemas abiertos, de programarse a sí misma y de adaptarse a nuevos escenarios existe solo en la imaginación de algunos científicos, motivo por el cual ninguna IA puede ser penalmente responsable, al no tener el dominio del hecho[644]. De acuerdo con esta teoría, la IA sería un mero instrumento en manos del autor doloso directo, que la utilizaría para la comisión de un delito. Se descarta, por el mismo motivo, la posibilidad de atribuir una autoría dolosa mediata a una IA, e incluso queda excluida del tipo imprudente. La IA es, reitero, una herramienta, la cual, por sus características, es idónea para ser utilizada en el ámbito de la ciberseguridad y, por extensión, influenciar en gran medida a los delitos que afectan a la misma en el CP español.

Si se tiene en cuenta que la Comisión Europea estimó una inversión total en Europa en I+D dedicada a la IA de 20.000 millones de euros anuales en el periodo comprendido entre los años 2021 y 2027[645], y que alrededor del 47% de todos los puestos de trabajo habrán sido sustituidos por la IA en el año 2033, es posible hacerse una idea de la cantidad de operaciones que esta realizará a diario, y, por ende, de la cantidad de ocasiones que existirán para que los ciberdelincuentes actúen en su perjuicio[646]. Aunque considero que sus características (y, sobre todo, su proyección de futuro) se han exagerado enormemente, puesto que no ha quedado demostrado que vaya a poder imitar la complejidad de la formación de ideas humana o aspectos exclusivamente humanos como la inspiración, es indudable que la IA tiene un

digital, 1ª ed., Madrid, Wolters Kluwer, 2021, p. 685. En la actualidad, los sistemas de IA vinculados a la materia penal pertenecen a la IA débil.

644 Velasco Núñez, *Delitos tecnológicos*, p. 625 – 627.

645 N. Oliver, "Hacia una inteligencia artificial por y para la sociedad", *Temas para el debate,* no. 299, 2019, p. 38. Aunque coincido con la idea práctica de actualizar el marco legal para prever el previsible uso ubicuo de los sistemas de IA, también considero que esto supone una rendición poco reflexiva y muy prematura.

646 M. Barrio Andrés, *Manual de Derecho Digital,* 1ª ed., Valencia, Tirant lo Blanch, 2020, p. 55.

formidable potencial para la ciberdefensa, toda vez que permite una detección temprana de las ciberamenazas y una respuesta instantánea[647]. Tanto es así que incluso el Consejo de Europa ha reconocido su valor para la prevención de delitos[648].

Al añadir la IA a la ecuación ya existente de la ciberseguridad, se unen a los desafíos expuestos en anteriores capítulos de esta investigación otras nuevas directamente relacionadas con esta nueva tecnología. Así, además de los accesos no autorizados a datos, o de la manipulación o de la transferencia no autorizada de los mismos, encontramos conductas nuevas como la contaminación de datos en el aprendizaje automático (*machine learning*) o la puesta en peligro o la limitación de los resultados obtenidos mediante IA[649].

No obstante, y sintetizando lo que ya desarrollé de manera extensa en el capítulo tercero de esta investigación, sólidos principios del Derecho penal como el de mínima intervención o *ultima ratio* o el de subsidiariedad impiden su intervención directa y obligan a respetar la clásica cadena en tres fases compuesta en primer lugar por la autorregulación (es decir, debe tratar de regularse el asunto en el ámbito privado); en segundo lugar por el control administrativo; y en tercer lugar, y solo ante la imposibilidad de regular una materia a través de los dos anteriores, el control penal, o la aplicación del *ius puniendi* estatal[650].

---

[647] G. Karapilafis, "Artificial Intelligence in Cyber Defense", en N. J. Daras (edit.), *Cyber-Security and Information Warfare,* 1ª ed., Nueva York, NY, Nova Science Publishers, 2019, p. 196. Esto es posible gracias a que la IA puede monitorizar en tiempo real de manera constante y proactiva toda una red informática.

[648] Consejo de Europa, *Artificial Intelligence and Data Protection*, Estrasburgo, Consejo de Europa, 2019, p. 7. Además de su utilidad en la lucha contra el crimen, también se menciona lo útil que será para la sanidad.

[649] Agencia de la Unión Europea para la Ciberseguridad, *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence,* Atenas, Agencia de la Unión Europea para la Ciberseguridad, 2020, p. 29.

[650] J. Valls Prieto, *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial,* 1ª ed., Madrid, Dykinson, 2017, p. 149. Al igual que Romeo Casabona, el autor es partidario de perseguir, tras un análisis cuidadoso de los bienes jurídicos protegidos lesionados, los sistemas que utilicen IA sin haber cumplido con la pertinente evaluación de riesgos.

Con la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se Establecen Normas Armonizadas en Materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se Modifican Determinados Actos Legislativos de la Unión, de 21 de abril de 2021, la UE ha tratado de resolver una difícil situación equilibrando dos intereses en juego: por un lado, necesitaba un texto legal que defendiese los derechos de sus habitantes en lo concerniente a la IA; por otro, no podía permitir que una legislación demasiado exigente supusiese un freno a la innovación tecnológica relacionada con la misma, ya que considera la IA uno de los pilares del desarrollo de la economía digital[651]. Aun así, es posible encontrar referencias específicas a la ciberseguridad en varios de sus considerandos y artículos.

La mayoría de ellos son una descripción de los fuertes requisitos que los sistemas de IA de alto riesgo deben cumplir para ser permitidos[652], como los que se imponen a sus proveedores, fabricantes, importadores, distribuidores y usuarios. El considerando 43 sostiene que, además, deben cumplir requisitos de ciberseguridad que mitiguen de manera efectiva los riesgos para la salud y la seguridad, atendiendo a la finalidad prevista del sistema; el considerando 49 obliga a garantizar un nivel adecuado de ciberseguridad; el 51 destaca el papel fundamental de la ciberseguridad frente a las actuaciones intencionadas de terceros que, aprovechando las

[651] Oxford Commission on AI & Good Governance, *Harmonising Artificial Intelligence: The role of standards in the EU AI Regulation,* Oxford, Oxford Commission on AI & Good Governance, 2021, pp. 6 – 9.

[652] S. García García, "Una aproximación a la futura regulación de la inteligencia artificial en la Unión Europea", *Revista de Estudios Europeos,* vol. 79, 2022, p. 321. Entre los sistemas de alto riesgo se encuentran los sistemas de identificación biométrica remota, que estarán prohibidos con carácter general y solo podrán implementarse de manera excepcional y después de obtener una autorización previa por parte de una autoridad judicial o de una autoridad administrativa independiente, y estarán siempre sometidos a controles especiales de transparencia. Como expondré en este mismo capítulo, la biometría parece ser una de las tecnologías de las que más va a depender la ciberseguridad en el futuro cercano, de manera que la regulación en este sentido no podría ser más oportuna. No obstante, y como ya ha sucedido en otras ocasiones en las que se ha generalizado el uso irresponsable de una tecnología, será difícil que las personas comprendan la importancia de proteger sus datos biométricos si se populariza su uso inadecuado.

vulnerabilidades del sistema, traten de alterar su uso, conducta o funcionamiento o de poner en peligro sus propiedades de seguridad. Además, y para recalcar su importancia una vez más, se extiende en una explicación sobre los ciberataques, aclarando que pueden dirigirse contra elementos específicos de la IA, como los conjuntos de datos de entrenamiento (como sucede en la contaminación de datos) o los modelos entrenados (como en los ataques adversarios), o aprovechar las vulnerabilidades de los elementos digitales del sistema de IA o la infraestructura de TIC subyacente.

Considero que el artículo más importante es el 14.1, toda vez que recalca la supremacía del ser humano sobre la IA al imponer la vigilancia humana sobre la misma.

El art. 15.1 obliga a diseñar y desarrollar los sistemas de alto riesgo de manera que alcancen un nivel adecuado de ciberseguridad que deberán mantener a lo largo de todo su ciclo de vida. El art. 15.4 establece el deber de adoptar soluciones técnicas encaminadas a garantizar su ciberseguridad adecuadas a las circunstancias y los riesgos pertinentes.

En último lugar, y quizá para remarcar la importante vinculación entre ciberseguridad e IA para el legislador comunitario, el art. 42.2 aclara la manera de cumplir los requisitos de ciberseguridad exigidos en el art. 15, dando por sentado que cumplen los mismos los sistemas de IA de alto riesgo que hayan sido certificados o para los que se haya expedido una declaración de conformidad con arreglo a un esquema de ciberseguridad en virtud del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) no. 526/2013 (Reglamento sobre la Ciberseguridad), siempre que sus referencias hayan sido publicadas en el Diario Oficial de la Unión Europea.

Es indudable que la UE pretende garantizar la ciberseguridad de los sistemas de IA de alto riesgo mediante este texto legal comunitario sin acudir, al menos en una primera etapa, al *ius puniendi* de los Estados miembros. Y

es que, si se analiza el ámbito comunitario en busca de regulaciones específicamente penales en esta materia, se pone de manifiesto que no ha trascendido ningún documento oficial por parte de fuentes comunitarias, a excepción de modestas aportaciones como las del Comité Europeo de Problemas Penales (CDPC), que ha centrado sus planteamientos legislativos en ámbitos distintos al sanitario, por mucho que en sus últimas reuniones haya propuesto ampliarlos a otras temáticas.

A nivel estatal, Alemania no ha incorporado aún la IA a su Derecho penal sustantivo (StGB), al igual que sucede en la gran mayoría de Estados miembros de la UE[653], incluyendo a España y su CP, si bien esta nueva tecnología sí ha comenzado a utilizarse de manera paulatina para auxiliar en decisiones judiciales (es decir, en el ámbito del Derecho procesal penal[654 655]), como sucede en lo relativo a las medidas de seguridad, en relación con las cuales la IA ayuda a determinar la probabilidad de reincidir o la peligrosidad criminal del individuo[656].

---

[653] F. Pérez Bes, "Soft-law, Self-regulation and Compliance in AI", en P. García Mexía y F. Pérez Bes (eds.), *Artificial Intelligence and the Law,* 1ª ed., Madrid, Wolters Kluwer, 2021, p. 94. En ocasiones, cuando la tecnología se desarrolla con demasiada rapidez, el legislador opta por esperar hasta analizar su impacto y si es posible su adaptación a los principios y valores imperantes. Así lo han hecho Estonia, Finlandia y Lituania en relación con la IA, desarrollando sus propias estrategias nacionales antes de implementarla.

[654] En C.M. Romeo Casabona, "Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad", *Revista Penal,* no. 42, 2018, p. 179, encontramos un ejemplo del uso de la misma como herramienta auxiliar para la adopción de decisiones judiciales (caso *State v. Loomis* (2016) 881 N.W.2d 749), reconociendo sus numerosas limitaciones, debilidades e inconvenientes. Es importante, en consecuencia, apoyar el punto de vista del autor y recalcar el mero papel auxiliar o complementario de la IA en tareas de Derecho procesal penal, como sucede en las gestiones relativas a la previsión de la peligrosidad criminal, las cuales deben estar siempre sometidas a la decisión final de un ser humano que pueda imponerse al sistema automatizado inteligente y adoptar con autonomía sus decisiones dentro del marco de la libre apreciación de la prueba. En este sentido, sí es posible encontrar textos legales a nivel comunitario, como la Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales.

[655] A mayor abundamiento, M.D. García Sánchez, "Retos del uso de la inteligencia artificial en el proceso: impugnaciones con fundamentación algorítmica y derecho a la tutela judicial efectiva", en F. Bueno de Mata (dir.), *Fodertics 9.0: estudios sobre tecnologías disruptivas y justicia,* Granada, Comares, 2021, p. 233.

[656] Velasco Núñez, *Delitos tecnológicos*, p. 643.

En ausencia de nuevos artículos del CP que analizar, creo conveniente estudiar la manera en que la IA se está adaptando a los tipos delictivos ya encuadrados en el mismo, como complemento al análisis realizado en el capítulo tercero de esta investigación.

Como evidencia la propia normativa comunitaria, una de las principales preocupaciones para la ciberseguridad es la contaminación de datos algorítmicos, entendida como ataques externos a la gobernanza informática de la IA, cuando la actividad del ciberdelincuente incida sobre su programación o su fase de aprendizaje, como sucedería en el caso del algoritmo de un robot quirúrgico que, en lugar de operar al paciente de acuerdo con su programación, le provoca lesiones o, incluso, la muerte[657]. En casos como este, al haber un acceso inconsentido y un ataque a la seguridad de la información, podría optarse por aplicar el art. 197 bis 1 del CP, si bien, como ya he reiterado en el capítulo tercero de esta investigación, la actual localización de este artículo en el CP, entre los delitos de descubrimiento y revelación de secretos, dificulta la persecución de un delito que, en este caso, y como es evidente, no ataca a la intimidad ni a los datos reservados de carácter personal, sino a la propia seguridad informática. Alternativamente, sería posible aplicar el art. 264 bis 1 b) del CP, por haber obstaculizado o interrumpido el sujeto activo el funcionamiento de un sistema informático ajeno mediante la introducción de datos, y haber producido unos daños informáticos. En cualquiera de los dos casos, al verse afectados bienes jurídicos diferentes, procedería un concurso de delitos cuyas características dependerán de lo que finalmente le haya sucedido al sujeto pasivo (lesiones de distinta gravedad, o muerte)[658].

El art. 248.2 a) del CP determina que comete el delito de estafa quien, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. En la actualidad, existen aplicaciones de IA

[657] H. Lüttger, *Medicina y Derecho penal*, 1ª ed., Argentina, Olejnik, 2021, pp. 81 – 82.
[658] Velasco Núñez, *Delitos tecnológicos*, p. 648.

que permiten reunir datos de voz de una persona para imitarla con posterioridad haciéndose pasar por ella para dar una orden que encaje con la descripción típica. Resulta posible subsumir esta clase de innovaciones tecnológicas si no dentro de la manipulación informática, sí del amplio término de artificio semejante[659].

4.2.2 Aplicaciones para la IA como herramienta de ciberseguridad en el ámbito sanitario

Uno de los ámbitos esenciales donde se integrará la IA en el ámbito sanitario es la ciberseguridad, sobre todo en lo concerniente a la protección de los datos médicos. Además, la doctrina ya adelante la posibilidad de cometer crímenes de gran trascendencia en ausencia de la misma, como la manipulación de un algoritmo con objeto de, por ejemplo, proporcionar grandes dosis de insulina a pacientes diabéticos[660]. Ante una presencia cada vez mayor de la IA tanto en la asistencia clínica como en la investigación biomédica[661], y entendiendo que ya salva vidas donde los facultativos no pueden llegar no por falta de conocimientos o experiencia, sino por las limitaciones inherentes a la condición humana[662], es necesario analizar la

[659] Velasco Núñez, *Delitos tecnológicos*, p. 649.

[660] E.J. Topol, "High-performance medicine: the convergence of human and artificial intelligence", *Nature Medicine*, vol. 25, no. 1, 2019, p. 52. El autor, cuya opinión comparto, considera que, siempre en el mejor interés de los pacientes, deben realizarse más estudios antes de utilizar la IA de manera generalizada en el ámbito sanitario, y esta tecnología debe ser puesta a prueba en casos reales de manera progresiva.

[661] Fundación Instituto Roche, *Informe Anticipando Inteligencia artificial en salud: retos éticos y legales*, Madrid, Fundación Instituto Roche, 2020, p. 21. En este documento se han plasmado las principales ideas relativas a la IA en salud: su carácter instrumental, de herramienta, para ayudar al médico y simplificar sus tareas sin llegar nunca a reemplazarle; la necesidad de analizar el caso de cada paciente de manera individual y personalizada antes de adoptar una decisión; y, sobre todo, el deber de pensar en la ciberseguridad para proteger los datos de los pacientes, deidentificándolos (eliminando de los datos aquella información que permita identificar al sujeto fuente) o anonimizándolos para salvaguardar su privacidad.

[662] E. J. Topol, *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again,* 1ª ed., New York, NY, Hachette Book Group, 2019, pp. 4 – 5. Sirva como ejemplo el caso de un recién nacido que, tras ser enviado sano a casa, necesitó ser atendido en urgencias solo cinco días después al estar sufriendo crisis epilépticas. Tras realizar pruebas que descartaron la posibilidad de infecciones, y ante la ineficacia de los fármacos recomendados y el aumento de la frecuencia de las crisis epilépticas, se

manera en que la IA va a propiciar la creación de medidas de ciberseguridad innovadoras y tecnológicamente avanzadas que impidan o, al menos, dificulten al máximo las actividades de los ciberdelincuentes[663] en el ámbito sanitario.

Con este objetivo, creo conveniente estudiar cinco escenarios en los que la IA puede mejorar las medidas de ciberseguridad tradicionales para elevar el grado de seguridad de las redes y sistemas informáticos en el ámbito de la sanidad: primero, la protección de los hospitales y de los centros sanitarios frente al correo no deseado; segundo, la protección frente a los accesos indebidos cuyo objetivo es el descubrimiento y la revelación de secretos sanitarios; tercero, la protección frente a daños informáticos sufridos por las redes y sistemas informáticos de centros sanitarios; cuarto, la protección frente a los ataques contra la propia ciberseguridad, cuyo objetivo es disminuir o destruir por completo el nivel de seguridad informática de dichos centros, en ocasiones para cometer después un delito fin; y, por último, la protección durante una cirugía robótica como ejemplo de la adaptación de la IA a un esquema jurídico-penal clásico. Incluso teniendo en cuenta su complejidad, esto es solo una muestra seleccionada de las posibilidades para la mejora de la ciberseguridad que ofrece la IA, las cuales, bien aprovechadas, abarcarán mucho más, y merecerán ser analizadas según se vayan implantando al tiempo que la propia tecnología de IA sigue desarrollándose.

---

decidió utilizar una muestra de sangre para realizar una secuenciación completa del genoma del menor. La colosal cantidad de información fue gestionada mediante IA y algoritmos de aprendizaje automático hasta dar con una variante en el gen ALDH7A1 que afecta a menos del 0,01% de la población y causa un defecto metabólico, origen de las crisis epilépticas. Al poder ser contrarrestados sus efectos con suplementos dietéticos, la introducción de cambios en la dieta del recién nacido provocó que sus crisis epilépticas cesaran repentinamente y pudiese regresar a casa completamente curado solo treinta y seis horas después.

663 E. Raff, S. Lantzy, y E.J. Maier, “Dr. AI, Where Did You Get Your Degree?”, en F. Koch et al. (eds.), *Artificial Intelligence in Health*, 1ª ed., Cham, Springer, 2019, p. 82. El sujeto activo de esta clase de delitos puede pertenecer a categorías tan distintas como las personas adictas a ciertos tipos de medicamentos que buscan ir más allá de las medidas de ciberseguridad para acceder a ellos o, incluso, los grupos organizados específicamente para dañar el sector sanitario o la confianza de los pacientes en la seguridad del mismo.

4.2.2.1 (I) La IA como protección frente al correo no deseado en hospitales y centros sanitarios

Aunque superficialmente pueda parecer que los ataques contra los filtros de correo no deseado no son demasiado importantes, en realidad se encuentran entre las modalidades más relevantes y novedosas de amenazas para la ciberseguridad en lo que respecta a las tecnologías impulsadas por datos, puesto que son una forma de contaminación de datos algorítmicos. Desde una perspectiva teórica, en esta clase de ciberataques el sujeto activo debe tener el control sobre al menos una parte de los datos utilizados para entrenar un algoritmo, siendo su objetivo final la subversión total del proceso de aprendizaje de manera que disminuya el rendimiento total del sistema o se produzcan errores muy específicos. Y es que, si bien es técnicamente posible que los datos recogidos provengan de fuentes de escasa fiabilidad, como sucede en ocasiones con los sensores o los dispositivos, la amenaza principal que puede prever el CP es la introducción del sujeto activo de información generada con el propósito voluntario de contaminar gradualmente el sistema poniendo en peligro su desempeño a largo plazo. Por mucho que los datos contaminados se identificasen y clasificasen de manera correcta por el algoritmo, siempre existiría el riesgo de que su desempeño fuese inferior al posible por haberlos utilizado.

Los hospitales y los centros sanitarios, como tantas otras instalaciones médicas, disponen para defenderse frente a los ciberataques de filtros de correo no deseado. A través de los mismos, los algoritmos de aprendizaje automático clasifican los mensajes recibidos en dos categorías: correo deseado o no deseado. En la decisión influyen, entre otros aspectos, las palabras en el título de los mismos, o las que contienen. Sabiendo esto, una de las tácticas del sujeto activo es la mezcla de palabras adecuadas al contexto sanitario y otras no relacionadas con el mismo pero que evidencian sus verdaderas intenciones, de manera que la clasificación llevada a cabo por los algoritmos de aprendizaje automático sea incorrecta. El objetivo del

ciberdelincuente es la modificación de los criterios de decisión aprendidos por dichos algoritmos con objeto de provocar errores en la clasificación o de aumentar la probabilidad de comisión de ciertos tipos de error específicos o, de manera alternativa, producir una clasificación equivocada solo en relación con ciertas categorías de datos. Es importante comprender que, en el peor de los escenarios, este ataque a la ciberseguridad se traduciría en la incapacidad de los algoritmos para distinguir entre correo deseado y no deseado, convirtiéndolo en inservible y eliminando las ventajas que esta tecnología proporciona a las instalaciones médicas. Por último, aunque menos frecuente, también existe la posibilidad de que el sujeto activo tenga como objetivo que se clasifiquen como correo no deseado mensajes procedentes de una persona en particular, como sucedería en el caso de un paciente al que desea perjudicar y al que impide toda o parte de su comunicación por escrito en línea con un determinado hospital o centro sanitario[664].

Desde una perspectiva jurídico-penal, es posible encuadrar las conductas anteriores en el art. 264 bis 2 del CP, ya que no solo se obstaculiza el funcionamiento de un sistema informático ajeno mediante la introducción o transmisión de datos, sino que concurre una de las circunstancias previstas por el art. 264.2.4ª, que prevé que los hechos afecten al sistema informático de una infraestructura crítica, procediendo la aplicación del tipo agravado. Un detalle a tener en cuenta cuando se analizan conductas encuadrables en estos dos artículos es la gravedad de la conducta típica. En efecto, tanto el art. 264.1 del CP como el 264 bis 1 del CP exigen que el resultado producido sea grave, aspecto ya estudiado en el capítulo tercero de esta investigación, pero que impide la persecución de hechos exentos de la gravedad exigida por el tipo. Esto hace que resulte sencillo vincular este texto legal con la ciberseguridad, ya que, reitero, es imposible alcanzar un nivel absoluto de la

[664] L. Muñoz-González y E.C. Lupu, “The security of Machine Learning Systems”, en L. F. Sikos (edit.), *AI in Cybersecurity*, Cham, Springer, 2019, p. 54. En efecto, la contaminación de datos, a la que haré referencia más adelante, es importante en relación con la capacidad de la IA para filtrar correo no deseado, puesto que alterando sus algoritmos es posible hacerle creer que el correo no deseado sí lo es, y viceversa.

misma, y siempre hablaremos de ella refiriéndonos a sus niveles: a mayores medidas orientadas a su protección y a más medidas legales -como las jurídico-penales- dedicadas a su defensa, mayor será su nivel, y viceversa. Solo cuando la comisión de la conducta típica suponga una grave disminución del nivel de ciberseguridad en un hospital o centro sanitario y, por lo tanto, se traduzca en unos resultados graves para los pacientes, será posible acudir a estos artículos del CP. Para garantizar que concurre este elemento del tipo, recomiendo una monitorización continua de los filtros de correo no deseado, de manera que solo si se detecta un patrón después de haber contrastado un perjuicio para los pacientes (como el envío de muchos de estos correos desde una misma dirección IP, que permitiría atribuir esta conducta a un único individuo y calificarla como grave) procedería acudir a la jurisdicción penal.

4.2.2.2 (II) La IA como protección frente a los accesos indebidos para descubrir secretos

Los datos de carácter personal que revelan la salud de los pacientes contenidos en las bases de datos de los hospitales y de los centros sanitarios resultan especialmente valiosos, de manera que, como explicaré a continuación, han merecido un tratamiento especial por parte del legislador penal en su intento de garantizar su seguridad. Al tratarse de la vertiente lógica de la ciberseguridad, el objetivo es la garantía de su disponibilidad, su integridad y su confidencialidad frente a los accesos indebidos que puedan afectarles[665].

Tradicionalmente, se han utilizado dos técnicas en el ámbito de la detección de accesos indebidos a redes y sistemas informáticos, a saber: la detección basada en firmas y la detección de anomalías. La primera consiste en un análisis de los ataques informáticos que ya se conocen con objeto de construir una base de conocimiento para combinarla con un sistema de alerta

[665] S. Navas Navarro, "Derecho e inteligencia artificial desde el diseño. Aproximaciones", en S. Navas Navarro (coord.), *Inteligencia artificial. Tecnología. Derecho,* Valencia, Tirant lo Blanch, 2017, pp. 68 – 71.

que se dispara al detectar en el tráfico una correspondencia con las firmas incluidas en la misma. Así, el sistema de alerta analiza el tráfico y, cuando detecta en el mismo un ataque informático cuyas características ya constan en la base de conocimiento, emite un aviso. Esta base de conocimiento requiere una actualización constante, si se pretende que sea de utilidad. La segunda de las técnicas, basada en la detección de anomalías, divide el comportamiento del tráfico informático entre normal o, en los casos en que se detecten diferencias en su comportamiento que lo alejen del mismo, anómalo. Los elementos que se tienen en cuenta para adoptar esta decisión son, entre otros, la existencia de patrones de tráfico inesperados, el aumento de tráfico inusual que tenga lugar a horas específicas del día o de la noche, o la ocupación de la red de manera abusiva. Identificadas las anomalías, se desarrollan señales de alarma, poniendo mucho cuidado en una adecuada distinción entre verdaderos y falsos positivos, así como en permitir las novedades en el tráfico informático que, tras un análisis, evidencien no estar asociadas a un comportamiento sospechoso. La introducción de técnicas de IA en el ámbito de la ciberseguridad ha hecho posible la creación de nuevos sistemas de detección de intrusiones basados en el aprendizaje profundo (*deep learning*) y en algoritmos que aprenden de manera tanto supervisada como no supervisada y alcanzan un grado de precisión mayor en la distinción entre el tráfico normal y el anómalo a través de una ordenación de los datos más exacta[666].

Con el tiempo, el modelo tradicional permitía a un hospital o a un centro sanitario construir una base de conocimiento que incluyese tanto los ciberataques más habituales como aquellos con características más peculiares. Ante una nueva detección de uno de los mismos, el sistema de alerta vinculado a la base emitía un aviso que permitía aumentar los esfuerzos de vigilancia informática frente a accesos indebidos a las bases de datos. El problema radica en que esta base de conocimiento necesitaba ser

[666] A. Parisi, *Hands-On Artificial Intelligence for Cybersecurity. Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies,* 1ª ed., Birmingham, Packt, 2019, pp. 125 – 129.

actualizada de manera constante, lo cual se traducía en un gran esfuerzo económico y de personal, e incluso contando con fondos suficientes y profesionales cualificados, siempre existía la posibilidad de que elementos comprensibles del factor humano, como una sobrecarga de trabajo o la lógica imposibilidad de conocer todos los tipos de ciberataques, permitiesen que la base quedase desactualizada o, en el peor de los casos, abandonada en mayor o menor medida.

Las nuevas técnicas de IA, en este sentido, han aumentado el nivel de ciberseguridad, toda vez que la base de conocimiento se actualiza de manera automática, por mucho que siga siendo recomendable, como siempre, la supervisión del proceso por parte de un profesional humano. En cuanto a la detección de anomalías, sin duda estas técnicas de IA también la han perfeccionado aportando una mayor precisión y exactitud en la distinción entre el tráfico informático normal y el anómalo. Así, elementos como una aparente ocupación abusiva de la red de un hospital o de un centro sanitario también pueden ser analizados, yendo más allá de la existencia de una anomalía y permitiendo valorar factores como que la misma se deba a una emergencia sanitaria que empuja a los pacientes a acceder en masa a la misma de manera simultánea sin intención de perjudicar a nadie.

Sea cual fuere la técnica utilizada, la IA ha aumentado el nivel de ciberseguridad de las redes y sistemas informáticos de los hospitales y de los centros sanitarios. En este sentido, no cabe duda de que las nuevas medidas de ciberseguridad permitirán una disminución de los delitos de descubrimiento y revelación de secretos previstos en el CP para este ámbito, aumentando la seguridad de los datos de los pacientes sin necesidad de acudir a la jurisdicción penal. Y es que el art. 197.2 del CP castiga la conducta de quien, sin estar autorizado, accede por cualquier medio a datos reservados de carácter personal o familiar de otro que se hallen registrados, entre otros, en soportes informáticos, mientras que el art. 197.5 del CP obliga a la imposición en su mitad superior de la pena prevista por dicho artículo cuando los hechos descritos en el mismo afecten a datos de carácter personal que

revelen, entre otra información, el estado de salud de quien haya sido víctima de la brecha de ciberseguridad.

4.2.2.3 (III) La IA como protección más eficiente frente a los daños informáticos

Uno de los principales problemas de la IA en relación con la ciberseguridad es que no solo permite, como en el caso anterior, aumentar la complejidad de las nuevas medidas orientadas a garantizarla, sino que los ciberataques también adquieren una mayor complejidad y desafían de manera cada vez más peligrosa a las mismas, provocando la necesidad de someterlas a un proceso de constante innovación y dejando indiscutiblemente obsoletas las medidas tradicionales de protección de las redes y sistemas informáticos. La IA es, en este sentido, y pese a sus desventajas, la herramienta más eficiente frente a la creciente complejidad de las amenazas intrínsecas a la actividad en el ciberespacio[667].

La elevada difusión de *malware*, unida a la velocidad de su mutación polimórfica en diferentes variantes[668] (es decir, de sus cambios de forma), hacen necesario acudir al mecanismo del aprendizaje automático para una filtración más rápida, un triaje de las ciberamenazas, de manera que no se malgasten recursos escasos como las habilidades y los esfuerzos de los analistas humanos. Así, la IA permite distinguir entre los archivos que son inofensivos y los que suponen un peligro potencial para las redes y sistemas

[667] D. Ventre, *Artificial Intelligence, Cybersecurity and Cyber Defense,* 1ª ed, Londres, Wiley, 2020, pp. 157 – 161. Para Ventre, la IA es un arma de doble filo, puesto que, además de para la defensa, también sirve para perfeccionar los ciberataques, como sucede en el caso del *phishing*. Cuando una IA envía correos electrónicos con la intención de hacerse con los datos personales de multitud de sujetos pasivos, es capaz de adaptarlos a ciertas características de los mismos, haciendo así los mensajes más creíbles. Esto puede hacer que las herramientas clásicas de ciberseguridad no puedan detectarlos. En consecuencia, del mismo modo que la IA puede ayudarnos a distinguir lo legítimo de lo ilegítimo, también facilita la conversión de lo ilegítimo en legítimo con fines delictivos, al menos en apariencia, o la creación de contenidos engañosos.

[668] L.F. Sikos, “The Formal Representation of Cyberthreats for Automated Reasoning”, en L.F. Sikos y K. R. Choo (eds.), *Data Science in Cybersecurity and Cyberthreat Intelligence,* 1ª ed*.,* Cham, Springer, 2020, p. 1. El autor coincide en la naturaleza compleja y dinámica de las amenazas que afectan a la ciberseguridad.

informáticos o para los datos que puedan albergar. Esto es doblemente importante si tenemos en cuenta que el *malware* puede esconderse ya en cualquier tipo de archivo, incluso en aquellos archivos no ejecutables que únicamente contienen imágenes o texto.

El mayor peligro del *malware* radica, no obstante, en su división en multitud de clases, y en que constantemente surgen otras nuevas a causa de la gran creatividad de los ciberdelincuentes al desarrollar nuevas estrategias que exploten las debilidades específicas de las redes y sistemas informáticos de sus víctimas. Ya he analizado algunas de las clases tradicionales de *malware* en el capítulo tercero de esta investigación (troyanos, *botnets*, *rootkits*, o una mezcla de todos o de algunos de ellos), pero la complejidad inherente a los más novedosos deja obsoleto cualquier análisis realizado solo por humanos y convierte en indispensable la utilización de algoritmos que automaticen, como mínimo, la fase preparatoria del análisis (o triaje), consistente en una filtración preliminar del *malware* que, con posterioridad, también estudiará un analista humano, permitiendo así una primera respuesta lo más rápida posible y liberando al analista de las tareas más repetitivas, y dejándole tiempo para estudiar los aspectos más peculiares o inusuales de cada caso.

En contraposición a las técnicas útiles para la detección de accesos indebidos, una protección eficiente frente a los daños informáticos requiere unas medidas de ciberseguridad dotadas de un gran dinamismo, capaces de adaptarse a amenazas en relación con las cuales no se dispone de precedentes. Ante tal necesidad, la intervención de la IA resulta indispensable, por mucho que también sea necesario un analista que manipule estas medidas avanzadas para interpretar el comportamiento de los algoritmos y para estudiar las decisiones que se adoptan en cada ocasión con objeto de comprender la lógica seguida por las máquinas en el aprendizaje automático. Tras esto, podrá ajustarlas a su voluntad.

Cada clase de *malware* requiere una estrategia de ciberseguridad propia. Tanto el *malware* como su respuesta en forma de medida de

ciberseguridad son el resultado de la actividad creativa: en el primer caso, del ciberdelincuente; en el segundo caso, del profesional de la seguridad informática. Al ajustarse rara vez el primero a esquemas preestablecidos, el segundo debe recurrir también a su imaginación para proteger las redes y sistemas informáticos y los datos que albergan en una batalla sin final aparente[669]. Se hace necesaria, para garantizar el máximo nivel posible de ciberseguridad, la monitorización continua de las redes y sistemas informáticos que se pretenden proteger. Contenido un ciberataque, el analista debe intentar obtener de manera activa muestras del *malware* para estudiarlo y, con posterioridad, utilizarlo para entrenar los algoritmos en la distinción entre los archivos inofensivos y aquellos que suponen una amenaza para la ciberseguridad[670].

El tráfico de datos sanitarios de los pacientes y de información en general es constante en los hospitales y los centros sanitarios, no ya solo dentro de los mismos sino también cuando se comunican entre sí, así como con terceros ajenos a los servicios de salud. La protección frente al *malware*, que puede ser recibido en casi cualquiera de sus distintas clases en archivos de imagen (piénsese en radiografías o tomografías computarizadas) o de texto (historias clínicas, informes o comunicaciones de otros facultativos), obligan a que la protección frente al mismo sea eficiente, puesto que lo contrario impediría el trabajo diario de los profesionales sanitarios y no haría más lento, sino que prácticamente detendría el proceso de digitalización en el ámbito de la salud. Es importante, en consecuencia, una actitud proactiva en materia de ciberseguridad. Con el tiempo, y aunque en este ámbito de los daños informáticos es más importante la innovación que la creación de bases de conocimiento, sería recomendable un repertorio común del *malware* todavía no catalogado y ya neutralizado por los respectivos analistas de cada hospital o centro sanitario. Aunque no solucionaría todos los problemas, permitiría unificar los conocimientos de cada analista, crear estrategias y,

669 S. Greengard, “Cybersecurity Gets Smart”, *Communications of the ACM*, vol. 59, no. 5, 2016, p. 31.

670 Parisi, *Hands-On Artificial Intelligence for Cybersecurity*, pp. 79 – 101.

sobre todo, tratar de prever amenazas futuras para la ciberseguridad mediante los macrodatos (*big data*) disponibles.

Por mucho que se implementen medidas preventivas de ciberseguridad que reduzcan el número de ataques exitosos para los ciberdelincuentes, la agresividad del *malware* hará siempre necesaria la existencia de herramientas jurídico-penales que protejan a los usuarios frente a los delitos contra el patrimonio y contra el orden socioeconómico y, más específicamente, frente a los daños informáticos. Al igual que en el caso del correo no deseado (si bien esta clase de correo no puede considerarse *malware*, únicamente un medio para la difusión del mismo), el art. 264 bis 2 del CP prevé la obstaculización o interrupción del funcionamiento de un sistema informático ajeno destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica, cuando los hechos afecten, como recoge el art. 264.2.4ª del CP, al sistema informático de una infraestructura crítica. No creo que sea necesario reiterar las consideraciones ya expuestas sobre el requisito típico relativo a la gravedad del resultado presente en ambos artículos. La severidad de las penas propuestas (prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado) dotan a este art. 264 bis 2 del CP, a mi juicio, de un notable valor disuasorio, que unido a las eficientes medidas preventivas basadas en la IA adoptadas en el ámbito extrapenal deberían ser suficientes para proporcionar a los sistemas de los hospitales y de los centros sanitarios un elevado nivel de ciberseguridad frente a los daños informáticos derivados de las distintas clases de *malware*.

4.2.2.4 (IV) La IA como protección de las propias medidas de ciberseguridad

No existe medida más garantista para los activos a defender que proporcionar el mayor grado de protección posible también a las propias medidas de ciberseguridad. A través de esta acción, no protegemos el

continente (las redes y sistemas informáticos) ni el contenido (los datos), sino, simbólicamente, aquello que los circunda para custodiarlos.

La principal motivación para esto es reputacional: supone una ventaja que los ciberdelincuentes sepan que utilizamos la IA para proteger, incluso, las credenciales que permiten a los usuarios el acceso a sus cuentas. En relación con las contraseñas, si bien siempre han sido la principal herramienta para garantizar la protección de las cuentas de usuario, en la actualidad cabe preguntarse si están obsoletas a causa de la pobre protección que ofrecen una vez han mostrado sus límites. Además, también se ven afectadas por el factor humano: a medida que crece la actividad en línea, también aumenta el número de contraseñas que el usuario debe memorizar, y existe una tendencia a utilizar la misma para múltiples cuentas y servicios, de manera que, cuando un ciberdelincuente roba las credenciales de un usuario, hay altas probabilidades de que pueda completar varios accesos indebidos. Al establecer contraseñas, es importante desarrollar una (o permitir que el sistema desarrolle una por defecto) distinta para cada actividad, y en todos los casos debe ser robusta: la robustez de los códigos alfanuméricos elegidos como contraseña es inversamente proporcional a la facilidad de acceso de los ciberdelincuentes que los ignoran.

Ante la posibilidad de fallar de todo lo anterior, la IA permite, a través de una monitorización con procedimientos de detección de anomalías estructurados sobre algoritmos de aprendizaje automático, que la protección de la cuenta de un usuario no se limite a la simple verificación de la corrección de la contraseña introducida y a su correspondencia con la cuenta de referencia, sino que hace posible tener en cuenta los accesos simultáneos desde direcciones IP localizadas en distintas áreas geográficas, el uso de distintos dispositivos y la utilización de sistemas operativos inusuales o nunca utilizados con anterioridad. Además, para garantizar que las credenciales introducidas realmente pertenecen a su legítimo propietario, con el tiempo se han desarrollado diversas formas de verificación, como la autenticación de múltiples factores, entre la que destaca la autenticación en dos pasos o verificación en dos pasos, si bien su fiabilidad depende, a su vez, de la

integridad de los canales utilizados para gestionar estos factores de autenticación.

Los algoritmos de la IA harán posible la implementación progresiva de técnicas avanzadas de ciberseguridad que serán un valioso añadido, si no una sustitución, de las ya existentes. Hay que destacar dos de estas técnicas: la biometría del comportamiento y las pruebas biométricas. La primera se basa en la posibilidad de identificar como patrones comportamientos y hábitos que, además, pueden asociarse a un usuario en particular. Es el caso de la dinámica de pulsaciones de teclas, la cual, como la escritura a mano, puede ayudar a identificar de manera fiable a una persona. Las segundas permitirán reemplazar las contraseñas por procedimientos de autenticación basados en los rasgos biométricos del usuario como el iris, la voz, las huellas dactilares, las facciones del rostro o una suma de todas ellas, toda vez que de manera individual, aunque fiables por sí mismos, son fáciles de burlar aprovechando las limitaciones y las vulnerabilidades de los sensores utilizados para su verificación[671]. Pero es que incluso en relación con estas técnicas tan avanzadas existen ya ciberdelincuentes que utilizan los algoritmos de la IA para sortearlas o neutralizarlas[672].

Considero que la mejor estrategia para garantizar el mayor nivel posible de ciberseguridad consiste en la combinación de distintas medidas. Hay que implementar las más avanzadas desde un punto de vista tecnológico, y eso hace que la IA sea necesaria, pero esto no debe conllevar el desprecio de las tradicionales ya que, en el peor de los casos, hacen perder el tiempo de los ciberdelincuentes disminuyendo sus posibilidades de éxito y, en el mejor de los casos, son un elemento adicional de disuasión frente a los ciberataques.

El único inconveniente que creo que puede existir para los hospitales y los centros sanitarios al implementar esta clase de medidas avanzadas de

[671] Parisi, *Hands-On Artificial Intelligence for Cybersecurity*, pp. 150 – 176.

[672] P.L. Frana, “Biometric Privacy and Security”, en P.L. Frana y M.J. Klein (eds.), *Encyclopedia of Artificial Intelligence: The Past, Present and Future of AI,* 1ª ed., Santa Bárbara, CA, ABC-CLIO, 2021, p. 46.

ciberseguridad, además de lo invasivos que pueden ser (y no es esta una cuestión menor), es su precio. Llegará un momento, antes o después, en que se generalizarán y estarán al alcance de cualquier usuario, pero estoy seguro de que los primeros años serán una tecnología prohibitiva desde un punto de vista económico si se pretende contratar los servicios de empresas de ciberseguridad sólidas, como se debería. Por este motivo, creo que la mayor parte del sector sanitario debería centrarse en perfeccionar la ciberseguridad basada en credenciales y, en la medida de lo posible, tratar de implementar los mencionados procedimientos de detección de anomalías estructurados sobre algoritmos de aprendizaje automático, teniendo su límite en la biometría del comportamiento en los cargos más altos. Las medidas de ciberseguridad basadas en pruebas biométricas, por su coste inicialmente prohibitivo, deberían dedicarse inicialmente a la protección de los datos sanitarios de los pacientes para ir extendiéndose de manera progresiva de las áreas más importantes (como la protección de armarios inteligentes que contienen medicamentos muy específicos) a las de menor importancia a medida que su coste vaya resultando asumible, y su adquisición generalizada aconsejable.

Una de las cuestiones jurídico-penales más importantes en relación con la existencia de nuevas medidas de ciberseguridad basadas en la IA es la manera en que el art. 197 bis 1 se adaptará a las mismas. La conducta típica descrita en el mismo consiste en acceder o facilitar a otro el acceso al conjunto o a una parte de un sistema de información o mantenerse en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, siempre que se vulneren las medidas de seguridad establecidas para impedirlo y se carezca de la debida autorización. Al comenzar el artículo admitiendo que puede incurrirse en esta conducta por cualquier medio o procedimiento, resulta posible encuadrar en el mismo desde el acceso indebido más clásico, como la averiguación de una contraseña débil, al más avanzado, como las pruebas biométricas, siempre que reúnan el resto de requisitos del tipo objetivo, a saber: la existencia de unas medidas de seguridad establecidas para impedir dicho acceso y la actuación en ausencia de la autorización pertinente. En el caso específico de la protección de la ciberseguridad de los

hospitales y los centros sanitarios, resulta parcialmente adecuada, incluso, la localización de este art. 197 bis 1 entre los delitos de descubrimiento y revelación de secretos, puesto que parte de lo que se pretende proteger son los datos sanitarios de los pacientes. Mas digo parcialmente porque, incluso en el ámbito sanitario, como sucede en el caso de los armarios inteligentes, es posible pretender defender el bien jurídico ciberseguridad, no relacionándolo con la intimidad ni con los datos reservados de carácter personal, lo que nos retrotrae a la cuestión jurídico-penal ya tratada en profundidad en el capítulo tercero de esta investigación, relativa a la posibilidad de trasladar este artículo a un nuevo título del CP dedicado solo a la protección del bien jurídico ciberseguridad.

4.2.2.5 (V) La IA y su uso en cirugía como ejemplo de su adaptación a un esquema jurídico-penal clásico

Entre las aplicaciones más prometedoras de la IA está la de las salas de operaciones, en las que se estima que se llevan a cabo 234 millones de operaciones quirúrgicas cada año en todo el mundo. Se espera que esta tecnología ofrezca soluciones que auxilien a los cirujanos y les ayuden a reducir sus errores disminuyendo la cifra de pacientes que experimenta complicaciones durante las mismas, que actualmente asciende al 20%[673]. Los propios cirujanos admiten que esto les obligará a replantearse su profesión,

[673] E. Witkowski y T. Ward, "Artificial Intelligence Assisted Surgery", en A. Bohr y K. Memarzadeh (eds.), *Artificial Intelligence in Healthcare,* 1ª ed., Londres, Elsevier, 2020, pp. 185 – 190. A juicio de los autores, la IA introducirá mejoras en todas las fases quirúrgicas: en la fase preoperatoria, hará posible realizar diagnósticos más precisos, así como ordenar a los pacientes en base a lo avanzado de la patología que sufran; en la fase operatoria, la más susceptible de ser interrumpida por un ciberataque al ser la que más expone las vulnerabilidades del facultativo y del paciente, permitirá la ejecución de cirugías perfectas desde una perspectiva técnica; en el postoperatorio, conllevará un reconocimiento más rápido de posibles complicaciones que permita solventar cualquier problema que surja. A nivel general, esta nueva tecnología traerá consigo la posibilidad de mejorar la formación de los cirujanos. En cualquier caso, Witkowski y Ward definen nuestra época como la de la infancia de la IA en relación con la cirugía, y prevén un incremento progresivo de las medidas de seguridad que protegen a los pacientes durante las intervenciones.

puesto que cambiará la naturaleza de la propia cirugía[674], incluso teniendo en cuenta sus limitaciones actuales (como su ya mencionada dificultad para adaptarse a nuevas situaciones, las limitaciones en su destreza, o su capacidad limitada para integrar e interpretar información compleja)[675]. Y es que la IA se utiliza ya sobre todo para cirugía prostática, colorrectal o pancreática, por permitir métodos menos invasivos además de tener la capacidad de crear escenarios virtuales de entrenamiento o aprendizaje que simulan una intervención real sin arriesgar la vida de ningún paciente, e incluso permiten que la IA adopte el papel de entrenador o mentor docente mediante la realidad aumentada o la virtual[676].

Es en este contexto donde construyo el último de los cinco ejemplos que muestran las aplicaciones de la IA como herramienta para aumentar el nivel de ciberseguridad en el ámbito sanitario, y lo hago adaptando un esquema jurídico-penal clásico en el que el paciente deposita su confianza en el facultativo y se somete a una intervención quirúrgica en la que interviene el binomio ciberseguridad - IA. La doctrina penal ya admite la posibilidad de que se cometan los delitos más clásicos utilizando como medio la informática[677], e incluso se prevén los casos en los que, antes de comenzar la intervención quirúrgica, el ciberataque se dirige contra los elementos indispensables para que se lleve a cabo, como las máquinas de anestesia, susceptibles de funcionar de manera incorrecta o de ser inutilizadas[678].

---

[674] J.R. Adler, "Remote Robotic Spine Surgery", *Neurospine*, vol. 17, no. 1, 2020, p. 122.

[675] J.F. Ávila-Tomás, M.A. Mayer-Pujadas, y V.J. Quesada-Varela, "La Inteligencia artificial y sus aplicaciones en medicina (I): Introducción. Antecedentes a la IA y robótica", *Atención Primaria: Publicación Oficial de la Sociedad Española de Medicina de Familia y Comunitaria*, vol. 52, no. 10*,* 2020, pp. 782 – 783.

[676] J.F. Ávila-Tomás, M.A. Mayer-Pujadas, y V.J. Quesada-Varela, "La Inteligencia artificial y sus aplicaciones en medicina (II): Importancia actual y aplicaciones prácticas", *Atención Primaria: Publicación Oficial de la Sociedad Española de Medicina de Familia y Comunitaria*, vol. 53, no. 1, 2020, pp. 83 – 84.

[677] De la Mata Barranco, "Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal", p. 42. El acceso a los sistemas informáticos de un hospital con objeto de modificar el programa que organiza la distribución de medicamentos entre los enfermos podría dar lugar a un delito de asesinato en grado de tentativa, por mucho que el sujeto activo no haya tocado dichos medicamentos.

[678] J.C. Goldstein y H.V. Goldstein, "Intraoperative cyberattacks: cyberthreat awareness and cyber-resilience strategies in anesthesia", *Canadian Journal of Anesthesia,* vol. 68,

Atendiendo a lo anterior, no es arriesgado proponer un escenario en el que, de un lado, se encuentra el paciente anestesiado[679] y en plena operación desarrollada mediante IA y, del otro, el ciberdelincuente. En primer lugar, para poder cometer el delito contra la vida humana independiente que es su objetivo final, el segundo debería vulnerar las medidas de seguridad establecidas al efecto y acceder sin autorización al sistema de información encargado de la intervención quirúrgica, vulnerando en primer lugar el art. 197 bis 1 del CP. Resulta de la más elevada importancia recalcar, una vez más, que los bienes jurídicos que el sujeto activo lesiona en casos como este no son ya ni la intimidad ni los datos reservados de carácter personal, sino la propia ciberseguridad como medio para la comisión de un delito fin. En consecuencia, es esencial sostener una vez más que, atendiendo al grado del desarrollo de la tecnología informática, este art. 197 bis 1 del CP encontraría una localización más adecuada a su objetivo actual en un título de nuevo cuño dedicado a la protección del bien jurídico ciberseguridad. Traspasadas estas barreras, el ciberdelincuente debe, como continuación de su camino hacia el deseado delito contra la vida humana independiente, hacerse con el control del sistema informático, introduciendo las modificaciones necesarias para que, en lugar de seguir las instrucciones de los facultativos o los técnicos, que obligan a la IA a seguir unas instrucciones prefijadas y orientadas a la consecución de una intervención quirúrgica satisfactoria (o, como mucho, a una toma de decisiones muy limitada dentro de parámetros prefijados que, en todo caso, no incluirían aquellas que pudiesen traducirse en unas lesiones graves para un ser humano), lleve a cabo las acciones necesarias para acabar con la vida del paciente. El ciberdelincuente transgrede, así, el art. 264 bis 2 del CP, que nos remite al

---

no. 12, 2021, p. 1838. Otros posibles objetivos de los ciberataques podrían ser las máquinas que reflejan las constantes vitales del paciente durante la intervención, que podrían ser manipuladas para ocultar contratiempos como las arritmias mientras muestran datos normales a los facultativos para impedirles que intervengan cuando sea necesario.

679 S. Creese, "The threat from AI", en D.J. Baker y P.H. Robinson (eds.), *Artificial Intelligence and the Law. Cybercrime and Criminal Liability*, 1ª ed., Oxfordshire, Routledge, 2021, p. 213. Creese admite que la IA puede utilizarse como un arma, y distingue entre distintas posibles víctimas de su utilización criminal.

art. 264 bis 1 a) para determinar la acción típica (obstaculización de un sistema informático ajeno en ausencia de autorización, y en este caso de manera indiscutiblemente grave, realizando una de las conductas a que se refiere el art. 264.2.3ª, es decir, alteración de un programa informático perjudicando gravemente un servicio público esencial) y al art. 264.2.4ª para confirmar que concurre una circunstancia que permite aplicar este tipo agravado (los hechos afectan al sistema informático de una infraestructura crítica). La IA, alterada por el ciberdelincuente, procedería a cumplir su función meramente instrumental y, mediante la utilización de las herramientas bajo su control en el mundo físico, a cumplir los objetivos de su nueva programación, asestando, por ejemplo, un corte en una vena o arteria principal, o atravesando uno o varios órganos vitales.

Se consumaría, así, el delito fin, el verdadero propósito del ciberdelincuente, para quien todo lo anterior era solo un medio para la consecución de un objetivo. Considero que este delito contra la vida humana independiente, máximo exponente del fracaso de la ciberseguridad en el ámbito sanitario, debería tipificarse como asesinato con alevosía del art. 139.1.1ª del CP. Y lo considero parte de un esquema jurídico-penal clásico porque, si ignoramos por un momento la utilización de la IA como herramienta para su consumación, los elementos que lo componen han sido tradicionalmente estudiados tanto en la doctrina como en la jurisprudencia, y no se requiere la creación de nuevos conceptos, sino que es posible adaptar la utilización de esta nueva tecnología a los ya existentes. Es el caso de la modalidad alevosa utilizada para cometer el asesinato: se trata de la alevosía de desvalimiento por encontrarse el sujeto pasivo anestesiado y, en ocasiones, incluso sin supervisión de un cirujano o de otro facultativo cualificado, puesto que la propuesta es que, poco a poco, estas máquinas puedan realizar intervenciones por sí mismas, reservando la participación de los especialistas a los casos más complejos en los que se prevén complicaciones. Así, la STS 51/2022, de 12 de enero[680], describe la alevosía

[680] ECLI:ES:TS:2022:51.

como un ataque contra la vida sorpresivo y sin capacidad de respuesta por parte de la víctima que es objeto del mismo. La STS 3489/2021, de 23 de septiembre[681], sostiene que esta modalidad alevosa se produce sobre personas indefensas en situación de inferioridad que es aprovechada por el autor al ejecutar su acción, y la STS 3372/2021, de 16 de septiembre[682], aclara que esta situación de desamparo de la víctima impide cualquier reacción defensiva, poniendo el ejemplo de una persona inconsciente. La STS 4188/2020, de 11 de diciembre[683], abunda en la idea del sujeto pasivo dormido, para quien es imposible cualquier reacción defensiva. Por último, la STS 82/2019, de 16 de enero[684], profundiza en esta circunstancia al determinar que consiste en el aprovechamiento de una especial situación de desamparado de la víctima, como acontece cuando se halla accidentalmente privada de aptitud para defenderse, sirviendo esto para personas que se encuentran inconscientes. El sujeto activo se aprovecha de esta especial situación y desamparo de la víctima que impide cualquier reacción defensiva para ejecutar el delito de una manera fácil y a salvo de cualquier defensa de la víctima. El núcleo esencial de la alevosía por desvalimiento radica, por lo tanto, en la anulación de las posibilidades de defenderse de la víctima, algo que resultará cada vez más común si, como se espera, el paciente no solo estará inconsciente durante la operación quirúrgica, sino que, además, estará solo. Una vez más, resulta clara la necesidad de supervisión humana de cualquier tipo de proceso automatizado basado en la IA (en cuyo caso ya no sería de aplicación esta circunstancia, sobre todo ante la presencia de especialistas o de facultativos especialmente cualificados capaces de corregir sus errores) pero, hasta entonces, y atendiendo al entusiasmo de cierto sector doctrinal que confía en la autonomía total de la misma y considera el culmen de su desarrollo la posibilidad de que el paciente quede a su completa

[681] ECLI:ES:TS:2021:3489.
[682] ECLI:ES:TS:2021:3372.
[683] ECLI:ES:TS:2020:4188.
[684] ECLI:ES:TS:2019:82.

merced, considero que la alevosía por desvalimiento del art. 139.1.1ª del CP resulta aplicable al delito antes descrito.

En lo referente a la doctrina, la relación entre médico y paciente y su vinculación con el Derecho penal ha sido objeto de estudio durante muchos años[685], solo que ahora es preciso valorar factores nuevos como la ciberseguridad y la IA. Hoy, el médico ya no tiene el dominio total sobre el tratamiento médico-quirúrgico, sino que confía parte del mismo a una tecnología vinculada a la informática cuyo nivel de seguridad debe ser, como mínimo, suficiente para ofrecérsela sin reservas al paciente en condiciones de igualdad a sus propios servicios.

Esto obliga a replantear el sistema de atribución de responsabilidad penal clásico manteniendo sus elementos originales y añadiendo otros nuevos. Dos son los conceptos que, aunque estrechamente vinculados pese a ser esencialmente distintos, deben diferenciarse cada vez más: la indicación médica terapéutica y la *lex artis*. La primera consiste en la tarea de valoración de los beneficios y los riesgos objetivamente previsibles para la salud del paciente, dependiendo de la cual tradicionalmente el facultativo aplicaba una u otra medida terapéutica. La *lex artis* o reglas del arte médico consiste en, una vez emitida la valoración mencionada, la aplicación adecuada por parte del médico del tratamiento prescrito. Mientras que con la primera se decide si aplicar algún tratamiento y se elige entre varios de ellos cuando sea necesario, la *lex artis* se refiere a la manera en que se aplica el que ha sido seleccionado[686]. Al incorporarse la ciberseguridad y la IA a ciertos tratamientos, la indicación médica terapéutica adquiere un enorme protagonismo en detrimento de la *lex artis*, por mucho que esta siga siendo importante. El facultativo, como antaño, debe valorar las alternativas posibles para reducir una enfermedad, inclinándose siempre por la que sea más liviana

[685] C.M. Romeo Casabona, *El médico y el Derecho Penal. Tomo I. La actividad curativa. Licitud y responsabilidad penal,* 1ª ed., Santa Fe, Rubinzal – Culzoni, 2011 y *El médico y el Derecho Penal. Tomo II – Volumen I. Los problemas penales actuales de la Biomedicina,* 1ª ed., Santa Fe, Rubinzal – Culzoni, 2011.

[686] Romeo Casabona, *El médico y el Derecho Penal. Tomo I*, p. 193.

y menos molesta para el paciente[687], pero decidiendo sobre aspectos nuevos como si el uso de una determinada tecnología es necesario o no y, con posterioridad, decidiendo también dentro de una diversa gama de productos tecnológicos orientados a la curación de una patología, lo que le obliga no ya a conocer los tratamientos por sí mismo, sino a estar familiarizado con ciertos tipos de tecnología sanitaria.

Si el resultado es positivo, y no solo no han surgido inconvenientes en relación con la ciberseguridad o con la IA, sino que además el paciente puede considerar mejorada su salud, no existirá resultado lesivo, puesto que se habrá protegido el bien jurídico incluso teniendo en cuenta las pequeñas molestias derivadas de la intervención. En este sentido, José Antón Oneca consideraba la salud corporal como un bien jurídico que debía ser tomado en su totalidad, mientras que Hans Welzel consideraba que lo fundamental era el resultado favorable de la intervención siempre que las posibles faltas técnicas no produjesen efectos perjudiciales en la salud[688]. Cuando, por el contrario, se produce un perjuicio al bien jurídico porque no se consigue un resultado favorable en la intervención, y puede apreciarse que se da el tipo objetivo de lesiones o el de homicidio, dependiendo del resultado[689], cabe preguntarse a quién corresponde la responsabilidad penal, teniendo en cuenta que ha sido el facultativo quien ha recomendado la tecnología quirúrgica basada en IA. En primer lugar, considero que, como es lógico, no cabe hacer referencia a la *lex artis* en relación con la propia IA, puesto que la máquina, al contrario que el facultativo, no está obligada a regirse por la misma, y solo debe cumplir los objetivos técnicos para los que ha sido programada.

La responsabilidad del médico, por su parte, debe ser analizada desde una doble perspectiva. La primera, relativa a la indicación médica terapéutica, obligará al facultativo a responder solo cuando haya recomendado una tecnología manifiesta e inequívocamente lesiva para la salud del paciente, es

[687] Romeo Casabona, *El médico y el Derecho Penal. Tomo I*, p. 203.
[688] Romeo Casabona, *El médico y el Derecho Penal. Tomo I*, pp. 198 – 204.
[689] Romeo Casabona, *El médico y el Derecho Penal. Tomo I*, pp. 200 – 201.

decir, una IA que aun funcionando de acuerdo con su programación lesione el bien jurídico al ser por completo inadecuada para la patología a tratar. Se tratará de casos extremos que manifiesten un profundo desconocimiento respecto a lo recomendado al paciente, como la utilización de una máquina especializada en cirugía cardíaca para tratar una apendicitis, y en relación con los cuales nada podrá reclamarse a los técnicos que la crearon, puesto que no solo funciona bien sino que el médico fue bien informado en lo concerniente a sus especificaciones técnicas, como su uso adecuado.

La segunda perspectiva es la de la *lex artis*, que obligará al facultativo, una vez recomendada una determinada tecnología basada en IA, a actuar de manera distinta de acuerdo con la información que le haya sido proporcionada respecto a sus características. El médico deberá saber si la máquina puede realizar su función de manera autónoma o si, por el contrario, requiere su supervisión durante toda o parte de la intervención quirúrgica, ya sea por la escasa fiabilidad de la misma o por su dudoso nivel de ciberseguridad que puede traducirse en ciberataques inesperados, exigiendo la presencia de un especialista que pueda corregir una desviación durante la misma. En ningún caso deberá responder ni por las acciones imprevisibles llevadas a cabo por ciberdelincuentes ni por un mal funcionamiento de la máquina, siendo en este último caso los responsables los proveedores, los fabricantes, los importadores o los distribuidores, quienes deberán confirmar que cumplen todos los requisitos de ciberseguridad exigidos a nivel comunitario, siendo aún una propuesta de *lege ferenda* que puedan ser perseguidos en vía penal en caso contrario.

Ya en la perspectiva tradicional existía un deber de cuidado para el facultativo en relación con la utilización de ciertos instrumentos y productos. Así, la STS 2891/1988, de 22 de abril[690], afirmó que los médicos debían extremar las cautelas y precauciones y emplear el instrumental de toda clase que fuese adecuado y se hallase en condiciones óptimas de funcionamiento,

[690] ECLI:ES:TS:1988:2891.

siendo esto extensible a las nuevas tecnologías médicas[691]. El proceso de tecnificación de la práctica clínica continúa, por lo tanto, en la actualidad, siendo el médico, cada vez más, un técnico con gran capacidad no solo para analizar y valorar datos relativos a su paciente cada vez más precisos y complejos, sino también para manejar instrumentos imprescindibles dotados de un elevado grado de sofisticación, como aquellos que se sirven de la IA y para los que la ciberseguridad resultará esencial como condición para utilizarlos[692].

4.2.3 Los peligros de la utilización de la IA en el ámbito sanitario y su influencia sobre el Derecho penal

Como ya he expresado en este mismo capítulo, el hecho de que vaya a hacerse un uso ubicuo de los sistemas de IA no significa que esto sea correcto. Muy al contrario, solo evidencia que, una vez más, los avances tecnológicos se imponen en todo el mundo a la así llamada sociedad moderna, que no puede someterlos al profundo análisis para rechazarlos en caso de considerar que sus desventajas superan a sus aspectos positivos. ¿Cuál será el límite de este obsesivo viaje hacia delante de la modernidad, en el que cualquier disidencia, incluso la más razonable, está proscrita y castigada con el ostracismo académico y social?

En el ámbito sanitario, en el que estos avances tecnológicos han crecido de manera inversamente proporcional a la calidad asistencial y a la cercanía entre médico y paciente a causa de un sistema en declive, masificado y, en ocasiones, deshumanizado[693], se pretende ahora descargar sobre la IA no ya las tareas que le corresponden como tecnología, sino la esperanza de revertir un proceso de decadencia que trasciende los límites de

[691] Romeo Casabona, *El médico y el Derecho Penal. Tomo II – Volumen I*, p. 206.

[692] Romeo Casabona, *El médico y el Derecho Penal. Tomo II – Volumen I*, p. 244.

[693] J.M. Palomino Martín, *Derecho penal y nuevas tecnologías. Hacia un sistema informático para la aplicación del Derecho penal*, 1ª ed., Valencia, Tirant lo Blanch, 2006, p. 113. Palomino Martín advierte del peligro de deshumanización o despersonalización también de la actividad judicial y del Derecho penal ante el avance de las nuevas tecnologías, en lo que parece una indudable y lamentable tendencia generalizada.

lo sanitario y es consustancial a todo un sistema. Ignorando de manera muy conveniente todo lo anterior, no cabe duda de que está previsto que la IA se utilice para todo en el ámbito de la sanidad: desde los bots conversacionales en línea que realizarán un primer cribado de los pacientes para saber a qué especialista remitirles[694], pasando por los análisis de macrodatos sanitarios[695], hasta el abordaje clínico del paciente, incluso en las especialidades[696].

La modernidad se asienta sobre un sinfín de avances tecnológicos que conforman una mescolanza materialista irreflexiva y prematuramente aceptada[697]. Incluso se teoriza, a largo plazo, sobre el advenimiento de una superinteligencia que representaría una singularidad tecnológica sin precedentes, pero no se piensa ni por un momento en lo necesario o bueno de su existencia, ni mucho menos en los aspectos concernientes a la ciberseguridad, cuando existen expertos que advierten sobre la dificultad para controlar una tecnología de estas características[698]. A las desafortunadas, por

---

694 T. Nadarzynski et al., "Acceptability of artificial intelligence (AI)-led chatbot services in healthcare: A mixed-methods study", *Digital Health,* vol. 5, 2019, pp. 4 – 6. De acuerdo con el estudio realizado, parte de los pacientes no tiene problemas con interactuar con una IA en esta fase de la atención sanitaria, si bien muchos de ellos albergan preocupaciones relativas a la ciberseguridad, especialmente a la de sus datos.

695 K. Benke y G. Benke, "Artificial Intelligence and Big Data in Public Health", *International Journal of Environmental Research and Public Health,* vol. 15, no. 12, 2018, p. 7. Los autores evidencian el profundo cambio en la forma de trabajar de los especialistas que supondrán los macrodatos gestionados por la IA.

696 F. Loncaric et al., "La integración de la inteligencia artificial en el abordaje clínico del paciente: enfoque en la imagen cardíaca", *Revista Española de Cardiología,* vol. 74, no. 1, 2021, p. 79. Aunque los autores admiten las dificultades que todavía hay que solventar (como preguntas técnicas, dificultades de aplicación e idoneidad para tareas específicas), también consideran que la IA puede proporcionar más tiempo a los clínicos, redundando esto de manera favorable en lo más valioso: la relación entre médico y paciente.

697 C. Chace, *Surviving AI: The promise and peril of artificial intelligence,* 3ª ed, Three Cs, 2020, pp. 1 – 4.

698 M. Alfonseca et al., "Superintelligence Cannot be Contained: Lessons from Computability Theory", *Journal of Artificial Intelligence Research,* vol. 70, 2021, p. 73. Aunque en la actualidad tampoco tenemos la absoluta certeza de que la utilización de nuestras redes y sistemas informáticos sea totalmente segura, la existencia de una superinteligencia supondría un cambio esencial: teniendo en cuenta la capacidad de los ordenadores para adaptarse utilizando sofisticadas técnicas de aprendizaje automático, no resulta posible prever el comportamiento de una IA superinteligente. Nuestra capacidad para utilizar una IA para controlar otra IA es, además, limitada, de manera que considero que, en este sentido, debería actuarse con toda precaución.

superficiales, lecturas no solo jurídicas, sino incluso (y puede que esto sea más grave) teológicas de los resultados de su implementación, muy alejadas de las profundas reflexiones necesarias en ambas disciplinas[699], se han unido en su entusiasmo tanto expertos como ignorantes, estando permitido demostrar desde un cauto y lacónico entusiasmo hasta un entusiasmo rayano en lo fanático, pero nunca una disidencia auténtica, digna de ser tenida en cuenta con objeto de revertir un progreso que se considera, de nuevo, imparable e inevitable. Los adalides de este progreso a imponer a buenas o a malas parecen ignorar la pesadilla que ha supuesto la implementación en la sociedad de lo que, en apariencia, era una inofensiva telefonía móvil y terminó transformándose en ordenadores de bolsillo cuyas características permiten que todos estemos monitorizados y conectados *in aeternum* a una Red omnipresente y asfixiante, lo deseemos o no lo deseemos, sin posibilidad de abandonar el sistema, ya que incluso apagados, los dispositivos siguen procesando datos sin que nadie pueda escapar.

No incurriré en pensamiento utópico alguno: la IA, al igual que todas las demás nuevas tecnologías, se impondrá en la sociedad, a pesar de todo lo que podamos argumentar en contrario. Así las cosas, solo cabe proponer ideas que suponen, más que una alternativa, un intento de minimizar su efecto negativo para las personas: primero, la obligación de que la IA permanezca siempre bajo el control del ser humano; y segundo, que su utilización sea, siempre que sea posible, meramente auxiliar, y las decisiones finales sean adoptadas siempre por un ser humano. A lo primero responde adecuadamente la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se Establecen Normas Armonizadas en Materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se Modifican Determinados Actos Legislativos de la Unión, de 21 de abril de 2021, en su artículo 14.1, que consagra la imposición de vigilancia humana sobre la IA. Lo segundo, atendiendo a los sesgos de los que se habla con cada vez más frecuencia en su aplicación en el Derecho procesal penal, resulta más

[699] R.M. Geraci, *Apocalyptic AI,* 1ª ed., New York, NY, Oxford University Press, 2010, p. 8.

importante que nunca, e invita a un cuidadoso análisis si alguna vez se pretende trasladar esta nueva tecnología al ámbito del Derecho penal sustantivo.

Como conclusión de este apartado dedicado a la IA en el ámbito sanitario, quisiera exponer tres reflexiones que ponen de manifiesto su influencia sobre el Derecho penal.

Primera, que a pesar de la novedad que suponen innovaciones tecnológicas como los algoritmos, las modificaciones del CP no parecen estar orientadas a incluirlos en tipos delictivos nuevos, como podría parecer lógico tras un análisis superficial, sino que, en muchos casos, estas innovaciones pueden protegerse frente a conductas delictivas mediante artículos ya existentes. Así sucede con la contaminación de datos de los algoritmos, conducta perseguible sin necesidad de propuesta de *lege ferenda* a través del actual art. 264 bis 1 b) del CP, que tipifica la obstaculización o interrupción del funcionamiento de un sistema informático ajeno mediante la introducción de datos que producen unos daños informáticos. El único problema que percibo, en este sentido, es de carácter terminológico: estas suposiciones se basan en la idea de que un algoritmo pueda ser encuadrado dentro de la categoría de sistema informático, y no exista opinión informática experta que asegure que pertenece a una categoría propia o distinta. En este proceso de adaptación del CP será importante, por lo tanto, la existencia de equipos multidisciplinares que incluyan a informáticos para que determinadas conductas no acaben siendo consideradas atípicas por falta de exactitud en la terminología utilizada al unir la informática y el Derecho penal.

El primer artículo nuevo que se añadirá al CP en relación con la IA estará dedicado, muy probablemente, a la inclusión de un tipo delictivo orientado a perseguir a quienes, en la utilización de la misma, no cumplan con los estrictos requisitos exigidos por el articulado de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se Establecen Normas Armonizadas en Materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se Modifican Determinados Actos Legislativos de la Unión, de 21

de abril de 2021, o por la legislación extrapenal vinculante que pudiera desarrollarse en este ámbito en el futuro.

Así, se tipificaría la conducta de quien, teniendo conocimiento del mal funcionamiento o de los defectos de sus productos equipados con IA, no toma medidas para solucionarlos y no previene los resultados nocivos derivados de su uso, ya sea su conducta dolosa o imprudente. No sería posible (ni conveniente) castigar a quien ha seguido de manera rigurosa las normas extrapenales establecidas, debiendo asumir la sociedad de forma colectiva los efectos negativos inevitables, que entrarían dentro del espacio de riesgo permitido[700], entendido como el espacio que equilibra la necesidad de proteger los bienes jurídicos amenazados por la IA y el beneficio social que conlleva su existencia[701].

Segunda, que la adaptación del CP a la IA debe realizarse solo cuando sea necesario tras un estricto análisis de los posibles bienes jurídicos lesionados. Las propuestas de *lege ferenda* en este sentido, si pretenden ser sensatas, deben tener en cuenta los principios del Derecho penal y adaptar preferentemente tipos delictivos ya existentes tomando como referencia la actividad legislativa de países con unas leyes pioneras derivadas de su posición a la vanguardia internacional de la innovación tecnológica. Sobre todo, es importante recordar siempre que la IA son solo algoritmos y técnicas de ingeniería dotados de sus propias fortalezas e inconvenientes que resultan adecuados para la resolución de ciertos problemas, pero que son por

[700] B.J. Feijoo Sánchez, *Homicidio y lesiones imprudentes: requisitos y límites* materiales, 1ª ed., Argentina, Olejnik, 2021, p. 132. Toda conducta social conlleva riesgos para los demás integrantes de la sociedad.

[701] I. Salvadori, "Agentes artificiales, opacidad tecnológica y distribución de la responsabilidad penal", *Cuadernos de Política Criminal. Segunda época,* no. 133, 2021, pp. 171 – 174. En el hipotético caso de que el desarrollo de la IA y del aprendizaje automático diesen lugar a la creación de agentes artificiales capacitados para aprender y para adaptarse al contexto en que operan de manera igual o superior a la de un ser humano, pudiendo además comprender el valor social negativo de su comportamiento, el legislador debería evaluar la posibilidad de atribuir una responsabilidad directa a los agentes artificiales completamente autónomos, reconociendo su capacidad criminal. Únicamente cumplidas dichas condiciones se podría reprochar a los agentes artificiales la comisión de un acto antijurídico y culpable. Comparto este punto de vista, sobre todo, por aceptar como mera hipótesis este elevado nivel futuro de desarrollo tecnológico, el cual considero en exceso optimista y quizá inalcanzable por resultar imposible.

completo inútiles frente a otros[702]. No hay que olvidar que cuando, con el tiempo, la IA quede superada, habrá otras tecnologías futuras que también se relacionarán con el Derecho penal, por lo que su inclusión en el mismo no debe ir más allá de nuestras necesidades jurídico-criminales realistas.

Tercera, que no comparto la propuesta de *lege ferenda* que defiende que el uso de la IA debería poder considerarse una agravante genérica en el CP[703]. A mi juicio, tiene el mismo desvalor de la acción clavar a alguien en la yugular una varilla metálica que manipular la IA de un robot quirúrgico para que clave en la yugular de un paciente una de las varillas metálicas de las que se compone su instrumental. El único riesgo, en este sentido, es que el ordenamiento jurídico-penal se quedase desfasado al no poder establecer una conexión entre el avance tecnológico y el propio lenguaje jurídico-penal, convirtiendo ciertas conductas en atípicas. La progresiva adaptación de los tipos delictivos ya existentes a la IA, como sucede en el caso del mencionado delito de daños informáticos del art. 264 bis 1 b) del CP, hace que los temores por la obsolescencia del CP y por la imposibilidad de perseguir conductas claramente lesivas para bienes jurídicos protegidos sean infundados, convirtiendo esto en innecesaria la existencia de una agravante genérica para el uso de la IA que castigue su uso, cuando este quedará incardinado en los propios tipos delictivos.

Por último antes de abordar la robótica y los drones, hay que recalcar que ni siquiera en la vía civil puede la IA responder por un daño, al no tener

[702] G. Marcus y E. Davis, *Rebooting AI: Building Artificial Intelligence We Can Trust,* 1ª ed., New York, NY, Pantheon Books, 2019, p. 24. Depositar una confianza excesiva en la IA puede provocar graves problemas, toda vez que la misma no está preparada para la amplia variedad de circunstancias del mundo real.

[703] J. Valls Prieto, *Inteligencia artificial, Derechos Humanos y bienes jurídicos*, 1ª ed., Cizur Menor, Aranzadi, 2021, p. 85. Esta propuesta, insinuada por el autor pero no desarrollada aún en profundidad en ninguna de sus publicaciones, se basa en la idea de que la IA tiene un impacto muy genérico al afectar a multitud de bienes jurídicos y delitos, motivo por el cual no resulta recomendable crear un tipo agravado para cada uno, sino que parece más aconsejable la creación de una agravante genérica para los casos en que se utilice la IA. Yo considero que si bien lo primero es cierto, esto no significa necesariamente que lo segundo lo sea.

conciencia de sus propios actos y no poder ser imputable civil[704] [705]. A continuación, es necesario cambiar de perspectiva, puesto que pasamos del ámbito cibernético e intangible propio de la IA y de los algoritmos al ciberfísico[706] de los robots y de los drones. A través de los mismos, la IA se materializa en un continente, ya sea antropomórfico, como sucede en el caso de la robótica más tradicional, o no lo sea por motivos prácticos, como en el de los drones. Ambos interactúan con la realidad en un escenario principalmente físico. Su ciberseguridad, por lo tanto, también tendrá características propias, como una mayor tendencia a ser sujetos pasivos de ataques principalmente físicos y ciberfísicos que merecen un apartado propio en esta investigación.

4.3 Robótica y drones

4.3.1 Robótica

[704] R.M. García Teruel, "El Derecho de daños ante la inteligencia artificial y el *machine learning*: una aproximación desde las recomendaciones del Parlamento Europeo y del Grupo de Expertos de la Comisión Europea", en J. Ataz López y J.A. Cobacho Gómez (coords.), *Cuestiones clásicas y actuales del Derecho de daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón. Tomo II,* Cizur Menor, Navarra, Aranzadi, 2021, pp. 1018 – 1052. El caso *United States v. Athlone Industries, Inc.* (1984) 746 F.2d 977 planteó la posibilidad de que una IA fuese declarada responsable de los daños que había cometido, pero la sentencia dejó claro que, a pesar de los daños devastadores que puedan provocar, no es posible demandar a los robots, incluso cuando existan dificultades para atribuir la responsabilidad de los hechos a una persona.

[705] En contra de esta opinión, S. Díaz Alabart, *Robots y responsabilidad civil,* 1ª ed., Madrid, Reus, 2018, pp. 73 – 74. Hay que aclarar que su defensa de los robots autosuficientes dotados de una personalidad jurídica específica que les obligue a reparar los daños que hayan causado se plantea solo para modelos no actuales, sino mucho más avanzados, y únicamente para aquellos dotados de una mayor autonomía y complejidad.

[706] V. Laptev y V. Fedin, "Legal Awareness in a Digital Society", *Russian Law Journal*, vol. 8, no.1, 2020, p. 157. Para los autores, tanto la IA como los robots deberían poder ser parte de la sociedad, toda vez que, a su juicio, las relaciones que se desarrollan en la misma han perdido su atributo esencial: su humanidad. Así, los humanos deberían poder relacionarse con la IA, los robots, y otros activos del mundo digital. En el apartado siguiente veremos cómo esto, en mi opinión, es especialmente desacertado en lo que respecta a los robots, ya que conduce a alejar a estas tecnologías de su carácter mera y únicamente instrumental.

4.3.1.1 Cuestiones de Derecho penal relativas a la ciberseguridad de la robótica actual

Desde los primeros mecanismos animados que adquirían su capacidad de movimiento a través de ingenios hidráulicos, poleas y palancas hasta las máquinas autómatas, la complejidad de la robótica ha ido creciendo de manera gradual con el paso de los siglos hasta la revolución que supuso la capacidad para tratar la información mediante técnicas de IA en los primeros años del siglo XXI, y que les permitió alcanzar un nivel de razonamiento simbólico. Gracias al mismo, sus algoritmos pueden obtener información más allá de sus sensores y son capaces de trabajar basándose en sus conocimientos mediante la extracción de reglas a partir de principios y la generalización de su aplicación sobre situaciones antes desconocidas, al tiempo que detectan excepciones a dichas reglas y continúan funcionando aunque una parte del sistema haya fallado. En el ámbito sanitario, la robótica ha irrumpido con fuerza, ya que además de aumentar el nivel de precisión de los especialistas les permite acceder con mayor facilidad a áreas de riesgo, y también está presente en la asistencia, en el cuidado y en el proceso de rehabilitación de los pacientes.

En la actualidad, los robots, que son capaces de llevar a cabo desde tareas mínimas hasta prácticamente la totalidad de la cirugía, pueden sistematizarse en tres categorías: robots protésicos y rehabilitados; robots de atención y cuidado y, por último; robots quirúrgicos (para cirugía general, urológica, cardíaca o neurocirugía), que permiten a los cirujanos llevar a cabo intervenciones de exactitud (como las que se desarrollan en el área cerebral) como de fuerza (como las que requieren un corte pero también no dañar ninguna parte sana). Son los robots quirúrgicos los que están más desarrollados y los que plantean los mayores retos al Derecho penal, puesto que la telecirugía asistida y la telerrobótica permiten una profunda interacción

entre el especialista y la máquina[707]. Los robots más avanzados, los de Tipo D (por ser capaces de adquirir datos de su entorno y readaptar sus tareas basándose en ellos) y 3ª Generación (además de estar programados mediante el uso de un lenguaje natural, poseen capacidad para la planificación automática) se utilizan para la práctica quirúrgica y en el ámbito de la salud, pero plantean una serie de interrogantes en lo que concierne a la seguridad, especialmente en el caso de aquellos que no requieren supervisión humana y funcionan de manera completamente autónoma. Por este motivo, existe cierta tendencia hacia lo que se ha denominado seguridad intrínseca, mediante la que se intentan compatibilizar estas nuevas tecnologías con la seguridad de las personas[708].

A pesar de lo anterior, estos robots plantean sus propios retos en lo que respecta a la ciberseguridad, puesto que de manera paralela al desarrollo tecnológico se incrementan también los ataques contra los mismos, incluyendo los procedentes de grupos organizados y altamente cualificados[709]. No obstante, como en el caso de la IA, las cuestiones más acuciantes relativas al Derecho penal se centran no en los robots como sujetos pasivos del delito, aspecto ya tratado en el análisis de, entre otros, el delito de daños informáticos del capítulo tercero de esta investigación, sino en aspectos como la posibilidad de que un robot pueda ser considerado como

[707] R. García Portero, "Los robots en la sanidad", en M. Barrio Andrés (dir.), *Derecho de los Robots*, 2ª ed., Madrid, Wolters Kluwer, 2019, pp. 246 – 250. La telecirugía asistida permite una comunicación permanente entre un experto y un cirujano que realiza una intervención, haciendo posible que el primero guíe al segundo aconsejándole y dirigiendo los gestos que debe hacer en cada momento. La telerrobótica, por su parte, otorga la posibilidad a un cirujano de dar órdenes precisas a un robot para que realice una operación habiendo entre ellos miles de kilómetros: el robot reproducirá en cada momento los movimientos indicados.

[708] J. García-Prieto Cuesta, "¿Qué es un robot?", en M. Barrio Andrés (dir.), *Derecho de los Robots*, 2ª ed., Madrid, Wolters Kluwer, 2019, pp. 33 – 63. Los expertos consideran que los robots irán adquiriendo mayor complejidad en su funcionamiento y en su comportamiento, así como una independencia gradual respecto a sus diseñadores originales. No obstante, no considero creíble la previsión de un punto de singularidad que supondría para los sistemas robóticos alcanzar un nivel de consciencia semejante al de los humanos.

[709] A. Mozo Seoane, "La revolución tecnológica y sus retos: medios de control, fallos de los sistemas y ciberdelincuencia", en C. Rogel Vide (coord.), *Los robots y el Derecho*, 1ª ed., Madrid, Reus, 2018, p. 94.

sujeto activo del mismo. Esta primera cuestión tiene respuesta negativa basándonos en los fundamentos generales del Derecho penal clásico, pues aún los robots más avanzados carecen de voluntad y, al no poder equipararse su nivel de desarrollo al del cerebro humano, resulta imposible para los mismos alcanzar la configuración del hecho por medio de una voluntad de realización que conscientemente lo dirija, tal y como exigía Hans Welzel al autor del delito[710] [711]. En la actualidad, los robots no pueden considerarse, ni siquiera, autores mediatos, ya que lejos de tratarse de personas utilizadas para llevar a cabo la acción típica, no son más que una prolongación de las acciones del sujeto activo, que los utiliza como meras herramientas. Su especialización en tareas limitadas y cercanas entre sí y su carencia de inteligencia múltiple se traducen en que no pueden sentir culpa al llevar a cabo acciones contrarias al Derecho penal, acciones que, en cualquier caso, son el resultado de procesos algorítmicos esencialmente causales muy alejados del libre albedrío. Los seres humanos, de un modo u otro, todavía dominan y controlan los robots, de manera que serán ellos los responsables de sus acciones[712]. En consecuencia, en el caso de robots que delincan por haber sido programados específicamente para ello, será responsable la persona responsable de su programación[713].

No obstante, excepto en el caso anterior, las personas que diseñan o programan robots no encajan en el concepto de autor recogido en el art. 28 del CP, ya que no llevan a cabo la acción típica ni por sí mismos ni, como ya

[710] I. Lledó Benito, *El Derecho penal, robots, IA y cibercriminalidad: desafíos éticos y jurídicos. ¿Hacia una distopía?*, 1ª ed., Madrid, Dykinson, 2022, p. 83. Para Lledó Benito, plantear la responsabilidad penal de los robots resulta del todo absurdo en la actualidad, llegando a considerar esta posibilidad como una aporía.

[711] Lledó Benito, *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, p. 173.

[712] C.M. Romeo Casabona, "Criminal responsability of robots and autonomous artificial intelligent systems?", *Comunicaciones en propiedad industrial y derecho de la competencia*, no. 91, 2020, pp. 175 – 180.

[713] I. Blanco Cordero, "Homo sapiens y ¿machina sapiens?. Un Derecho Penal para los robots dotados de inteligencia artificial", en C. Mallada Fernández (dir.), *Nuevos Retos de la Ciberseguridad en un Contexto Cambiante*, Cizur Menor, Navarra, Aranzadi, 2019, pp. 71 – 72. En los casos en que un programador utilice su conocimiento para desarrollar un robot con el objetivo específico de delinquir, procede esta excepción.

he explicado, por medio de un tercero[714]. En cuanto a sus usuarios, al ser los robots elementos muebles susceptibles de titularidad, tampoco incurren en responsabilidad penal a no ser que no solo conozcan y quieran la acción delictiva, sino que también contribuyan a ella mediante la puesta a disposición del objeto. Una particularidad de los robots médicos es que su elevado coste hace inevitable que en la mayor parte de los casos sean propiedad de personas jurídicas, como hospitales, no habiendo coincidencia, muchas veces, entre titular y usuario. El legislador solo admite la responsabilidad penal de las personas jurídicas[715] en relación con determinados delitos, eximiéndola de la misma o atenuándola dependiendo del grado de implementación de sistemas de control orientados a prevenirlos[716]. Aunque no resulta descabellado prever la comisión de un delito (como el de daños informáticos del art. 264 quater del CP) por parte de una persona jurídica dueña de un robot, considero indudable que esto supone una desnaturalización tanto de la justicia penal y de sus objetivos como de la estructura tradicional de su norma principal, el CP, toda vez que a medida que se han ido añadiendo elementos al mismo se ha llegado a un punto en que la imposición de penas resulta casi simbólica, siendo quizá más conveniente redirigir ciertas acciones a la vía civil o a la normativa extrapenal cuando no resulte posible atribuir una conducta típica a una persona física determinada. Del mismo modo que sucedía en el caso de la IA, en relación con la cual se valoraba la posibilidad de reservar la vía penal para las personas que incumplan los requisitos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se Establecen Normas

[714] E. Fosch-Villaronga, *Robots, Healthcare, and the Law. Regulating Automation in Personal Healthcare*, 1ª ed., Oxfordshire, Routledge, 2020, p. 151. Fosch-Villaronga considera que una actuación del robot distinta a la establecida por quien lo ha diseñado no debería eximir directamente a este de toda responsabilidad.

[715] M. Iglesias Cabero, *Robótica y Responsabilidad. Aspectos legales en las diferentes áreas del Derecho*, 1ª ed., A Coruña, Colex, 2017, p. 121 – 124. Iglesias Cabero hace referencia a las consecuencias accesorias, a las que yo me referiré por resultar adecuadas para los sistemas autónomos inteligentes.

[716] E.M. Domínguez Peco, "Los robots en el Derecho penal", en M. Barrio Andrés (dir.), *Derecho de los Robots*, 2ª ed., Madrid, Wolters Kluwer, 2019, pp. 181 – 186. Domínguez Peco considera también que existen herramientas jurídicas suficientes en el ámbito penal para controlar la robótica en su estado actual.

Armonizadas en Materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se Modifican Determinados Actos Legislativos de la Unión, de 21 de abril de 2021, sería conveniente dilucidar si también sería posible perseguir mediante la misma los incumplimientos relativos a robots que se valen de IA para funcionar, o si, por el contrario, sería conveniente desarrollar normas extrapenales especializadas para la robótica que permitiesen proceder del mismo modo: ante el incumplimiento de la norma extrapenal, y cuando haya una lesión a un bien jurídico protegido por el Derecho penal, quedaría abierta la vía penal para perseguir preferentemente a una persona física o, en su defecto, a una persona jurídica, pero en ningún caso a un robot, que no deja de ser una simple máquina.

4.3.1.2 Desafíos jurídico-penales para la ciberseguridad de los sistemas autónomos inteligentes

Distintos de los robots cuyo nivel de desarrollo conocemos actualmente son los sistemas autónomos inteligentes[717], hipotéticamente capaces de tomar decisiones y de lesionar de manera intencionada un bien jurídico protegido por el Derecho penal. Ni sus diseñadores, ni sus creadores, ni sus propietarios los dominan ni controlan por completo[718].

A pesar de esta ausencia de dominio o control totales, resulta esencial como medida de ciberseguridad preventiva el mantenimiento de cierto control sobre estos sistemas por parte de seres humanos, de manera que se mantenga siempre el dominio sobre los mismos y puedan ser sometidos a las consecuencias jurídicas del delito cuando cometan una transgresión en el ámbito penal. Y utilizo una expresión tan alejada de la pena no por casualidad, sino porque considero que carece de sentido pretender castigar a los

[717] A. Van Wynsberghe, *Healthcare Robots: Ethics, Design and Implementation*, 1ª ed., Burlington, VT, Ashgate, 2015, p. 56. La autonomía no se refiere a la capacidad del robot para sentir, sino a su capacidad para interpretar los datos que recibe desde su entorno y actuar en un sentido tras juzgar en consecuencia.

[718] Romeo Casabona, "Criminal responsability of robots and autonomous artificial intelligent systems?", p. 175.

sistemas autónomos inteligentes de manera tradicional, al ser incapaces de sentir culpa moral y no tener la pena un efecto retributivo en ellos. Mucho más inteligente, aunque no por completo fiable, parece la introducción en su programación de mecanismos inalterables y eficientes de abstención de la comisión de hechos tipificados como crímenes[719], y esto porque donde carece de sentido castigar por la imposibilidad de educar y reinsertar, parece más lógico intentar, al menos, prevenir. La introducción de consecuencias accesorias al delito, mediante la creación, incluso, de una categoría específica en el CP adaptada a las necesidades de respuesta de los sistemas autónomos inteligentes, y que se basaría en la verificación de la existencia de peligrosidad objetiva en relación con los mismos, sería la manera más adecuada de garantizar su ciberseguridad mediante las normas penales. En última instancia, el dominio del ser humano sobre la máquina se garantiza a través de la posibilidad de bloquearlas, o de destruirlas en los casos más graves[720], extendiéndose esta posibilidad, a causa del riesgo, a todos los modelos de una misma serie cuando la lesión al bien jurídico protegido por el Derecho penal haya tenido lugar sin variación o modificación de la programación del sistema autónomo inteligente. Otras medidas no tan drásticas serían su retirada del mercado o, en los casos en que esto sea posible, su reprogramación[721], pues no se trata, en ningún caso, de equiparar a los sistemas autónomos inteligentes con las personas físicas ni con las personas jurídicas, sino de garantizar la supremacía del ser humano sobre, incluso, las máquinas más avanzadas, a través del Derecho penal.

---

[719] Romeo Casabona, "Criminal responsability of robots and autonomous artificial intelligent systems?", p. 179.

[720] G. Quintero Olivares, "La robótica ante el derecho penal: el vacío de respuesta jurídica a las desviaciones incontroladas", *Revista Electrónica de Estudios Penales y de la Seguridad: REEPS*, no. 1, 2017, p. 10. Quintero Olivares reconoce la destrucción del robot como una posible consecuencia del perjuicio causado a humanos, pero sostiene que esto no se trataría de una condena penal, toda vez que en el Derecho penal es necesario que los hipotéticos futuros transgresores de una norma conozcan *ex ante* las consecuencias de desobedecerla. Si bien se posiciona, mediante esta afirmación, en contra de la responsabilidad penal de los robots, advierte que no todo lo que estos hagan habrá de ser considerado necesariamente irrelevante.

[721] Romeo Casabona, "Criminal responsability of robots and autonomous artificial intelligent systems?", p. 175 – 181.

Estas consideraciones adquieren mayor importancia, si cabe, en el ámbito sanitario, en el que ya existen sistemas robóticos autónomos que efectúan intervenciones quirúrgicas complejas como la radiocirugía estereotáctica, capaz de eliminar tumores a través de un haz de láser en la zona afectada mediante un procedimiento indoloro de unos treinta minutos de duración que no daña tejidos adyacentes sanos y en la que el robot actúa con plena autonomía. En el futuro, los robots quirúrgicos irán asumiendo funciones que, en la actualidad, corresponden en exclusiva a los cirujanos, y cobrarán cada vez mayor protagonismo en lo que concierne al cuidado de los pacientes. Por ello, uno de los principales retos de su regulación jurídico-penal es el equilibrio entre un grado adecuado de permisividad frente a la innovación tecnológica que no la coarte de manera innecesaria y la ausencia de riesgos irracionales para la salud y para la seguridad de los pacientes[722].

4.3.2 Drones

4.3.2.1 Ciberseguridad como protección de los drones médicos y sanitarios frente a delitos

Los drones médicos y sanitarios están expuestos a distintas clases de ataques, tanto en el ámbito físico como en el virtual. Cuando se generalice su uso, estas aeronaves resultarán un objetivo prioritario para los ciberdelincuentes a causa de la relevancia y del valor económico de sus misiones[723], que van desde la entrega y recogida de muestras de sangre u orina y fármacos hasta el transporte de material médico como los desfibriladores.

[722] García Portero, *Derecho de los Robots*, pp. 253 – 258.

[723] J. Alonso Lecuit, "Drones, seguridad y ciberseguridad", en M. Barrio Andrés (dir.), *Derecho de los drones*, 1ª ed., Madrid, Wolters Kluwer, 2018, p. 379. La gestión del riesgo en relación con la ciberseguridad de los drones es especialmente compleja, teniendo en cuenta los distintos vectores de ataque existentes.

Y es que, incluso en la actualidad, cuando es necesario el transporte de insumos o de materiales médicos a poblaciones rurales de difícil acceso o, al revés, el traslado desde estos de muestras que solo puedan ser analizadas en hospitales o laboratorios especializados, la utilización de un dron reduce en un 38% el tiempo de desplazamientos con respecto al vehículo a motor, pudiendo realizar un total de seis vuelos diarios con un máximo de dos kilos de carga por viaje. Además de ser una solución frente al desabastecimiento, los drones hacen posible enviar una muestra y recibir poco tiempo después tanto los resultados como los medicamentos recomendados para el tratamiento propuesto para una patología en particular. Por otro lado, permiten alertar de una emergencia médica mediante una aplicación en el teléfono móvil y solicitar material médico específico para contrarrestarla, como un desfibrilador, cuadruplicando esto en rapidez al tiempo de respuesta de las ambulancias convencionales. Al tratarse de sistemas ciber-físicos, su navegación es el resultado de las continuas interacciones entre sus elementos físicos (*hardware*) y sus elementos computacionales (*software*), dependiendo su seguridad no solo de su vulnerabilidad frente a ataques cibernéticos, sino también de tipo físico.

A causa de lo anterior, los vectores de ataque pueden clasificarse en vectores físicos y vectores lógicos: los primeros tienen como objetivo neutralizar físicamente el dron interceptándolo a través de medios mecánicos (como proyectiles) o electrónicos (como un pulso electromagnético); los segundos buscan obtener su control total o parcial, o extraer información del mismo, mediante interferencias basadas en procedimientos electrónicos o informáticos[724]. Las medidas de ciberseguridad tienen, en relación con los drones, un doble objetivo, puesto que deben proteger tanto la seguridad de terceros como la actividad objeto del vuelo. Solo teniéndola en cuenta desde la fase de diseño de sus distintos componentes y profundizando en objetivos como proporcionarles unos canales de comunicación dotados de un cifrado robusto será posible conseguir este objetivo, sin olvidar la necesidad de

[724] Alonso Lecuit, *Derecho de los drones*, pp. 379 – 383.

regular legalmente en el ámbito extrapenal aspectos relacionados con el riesgo y la seguridad[725].

En cuanto al Derecho penal, la naturaleza ciber-física de los drones conlleva relacionar inevitablemente los ataques contra los mismos con el delito de daños del art. 263 del CP y de daños informáticos de los arts. 264 y siguientes del mismo texto legal. El vector de ataque elegido por el ciberdelincuente determinará la selección de uno u otro. No obstante, al ser el objetivo principal de los drones médicos y sanitarios el transporte de insumos o de materiales médicos que no por ser inferiores a los dos kilos de peso deben considerarse de escaso valor económico. Para valorar su destrucción o los daños que hayan podido sufrir, es importante enfocarlo desde las características de la carga, que estará estrechamente relacionada con las intenciones del ciberdelincuente. Su principal objetivo será siempre, ya se decante por un vector de ataque físico o lógico para atacar el dron, la destrucción o el deterioro de la carga física que transporta este, debiendo añadir a los daños de distinto tipo sufridos por la aeronave unos daños siempre físicos (pues tal es la naturaleza de la carga) del art. 263 del CP. En segundo lugar, es posible, aunque menos probable, que el ciberdelincuente esté interesado en interceptar la carga no por el valor intrínseco de la misma desde una perspectiva económica, que sería exiguo, pero que sí podría resultar valioso por otros motivos como contener datos reservados de carácter personal, como en el caso de las muestras de sangre o de ADN susceptibles de ser sustraídas y analizadas.

El problema, en este sentido, radica en que ni está generalizado el envío a través de drones de cargas tan valiosas como los órganos para trasplantes ni la lógica aconseja que se generalice en un futuro, puesto que esta clase de intervenciones quirúrgicas requieren una planificación pausada y rigurosa que hace recomendable el traslado no del órgano, sino del paciente al centro hospitalario donde vaya a tener lugar la intervención. Al llevarse a cabo tanto la extracción de los órganos como la implantación de los mismos

[725] Alonso Lecuit, *Derecho de los drones*, p. 388.

en hospitales dotados de buenos accesos por carretera o incluso comunicados, en ocasiones, por helicóptero, optar por un dron para transportar un órgano no parece lo más aconsejable en la actualidad, si bien no debe excluirse esta posibilidad cuando avance la tecnología.

Esta clase de ataques sí tendría sentido si la pretensión del ciberdelincuente fuese la de evitar que el dron entregase tipos de medicamentos muy específicos, como la insulina, a personas que hubiesen manifestado necesitarlos de manera urgente (o que, en ausencia de lo anterior, los hubiesen venido necesitando de manera crónica), y en cuyo caso podría darse un delito contra la vida humana independiente. No cabe duda, en cualquier caso, de que la principal motivación de los ataques contra los drones médicos y sanitarios es la comisión de delitos contra el patrimonio y contra el orden socioeconómico, debiendo acudirse a la figura concursal adecuada en cada caso que permita englobar tanto los daños sufridos por el dron como los de la carga que este transportaba en el momento del ataque.

4.4 Hospitales inteligentes

Los hospitales inteligentes[726] (*Smart Hospitals*) son centros sanitarios destinados al diagnóstico y al tratamiento de enfermos que se caracterizan por depender de procesos optimizados y automatizados basados en un entorno de TIC interconectadas (sobre todo, IdCM), y cuya finalidad es la mejora de los procedimientos de atención al paciente, así como la

[726] A. Holzinger, C. Röcker, y M. Ziefle, "From Smart Health to Smart Hospitals", en A. Holzinger, C. Röcker, y M. Ziefle (eds.), *Smart Health. Open Problems and Future Challenges*, 1ª ed., Cham, Springer, 2015, p. 4. La pretensión inicial es que esta clase de hospitales mejoren el cuidado de los pacientes, puesto que, a través de sensores y tecnologías basadas en la interacción entre las personas y las máquinas, podrán recibir asistencia personalizada, incluyendo ayuda para llevar a cabo actividades diarias o la monitorización de su estado de salud, y proporcionándoles, además, un mayor nivel de ciberseguridad. No obstante, también es muy importante no dejarse cegar por las promesas tecnológicas cuya factura se paga con la pérdida de privacidad y de dominio sobre los datos reservados de carácter personal. En la actualidad, los hospitales funcionan, en muchos aspectos, de manera excelente, de manera que la introducción de nuevas tecnologías sanitarias estaría justificada únicamente en aquellos ámbitos en los que, tras sopesar los argumentos a favor y en contra, supongan una indudable mejora para los intereses generales del paciente.

introducción de nuevas capacidades[727]. Las nuevas tecnologías hacen posible que, a nivel interno, sea posible conocer en tiempo real las personas trabajando en cada tarea y las necesarias ante una emergencia específica, o las unidades de medicamentos y material sanitario de los que se dispone; y a nivel externo, coordinar distintos hospitales inteligentes basándose en un cálculo de su ocupación y desplegar los recursos de cada uno, como las ambulancias, de la manera más beneficiosa para los intereses de los pacientes.

No obstante, al tiempo que aumentan los beneficios, también se multiplican los riesgos para la ciberseguridad, puesto que, de no establecer las medidas de seguridad informática adecuadas, sería posible para un ciberdelincuente llevar a cabo una intrusión en la red informática de uno o varios hospitales inteligentes para manipular sus datos en tiempo real, con consecuencias tan graves como provocar el envío en medio de una emergencia de ambulancias llenas de heridos a un hospital que, en teoría y de acuerdo con los datos falseados, dispondría de capacidad suficiente para atenderles, pero que en realidad se encontraría saturado, dejando al mismo tiempo las urgencias hospitalarias de otros centros completamente vacías. Figuras clásicas como la modificación indebida de historias clínicas adquieren una nueva naturaleza, ya que la inmediatez con la que pueden llevarse a cabo harían posible que un facultativo prescribiese medicamentos que pusiesen en peligro a un paciente, como sucedería de ignorar las advertencias relativas a sus alergias por haber sido eliminadas de la historia clínica por un ciberdelincuente con el objetivo de perjudicarle.

[727] P. Llaneza González, *Seguridad y responsabilidad en la Internet de las cosas (IoT)*, 1ª ed., Madrid, Wolters Kluwer, 2018, pp. 243 – 268. Para proteger un hospital inteligente es necesaria una combinación de buenas prácticas de seguridad organizativas y técnicas. Dentro de las técnicas se encuadran la ciberseguridad y las medidas de protección, como la implantación de mecanismos de prevención de intrusiones, los cifrados robustos o los cuidadosos controles de acceso. Para implementar medidas de seguridad de vanguardia, además de un elevado coste económico, es necesario tratar solo con proveedores de atención médica que incluyan entre sus objetivos la garantía de unos altos estándares de ciberseguridad.

La multitud de objetivos posibles una vez el ciberdelincuente ha conseguido acceder a la red o sistema informáticos de un hospital inteligente hace que, desde una perspectiva jurídico-penal, se vean amenazados bienes jurídicos tan distintos como la intimidad, los datos reservados de carácter personal, el patrimonio, o la vida humana independiente.

La diferencia respecto a los hospitales tradicionales radica en la profunda interconexión entre los elementos que los componen, ya que todo está conectado, como mínimo, a la red interna del propio centro sanitario, pero muy frecuentemente también a Internet (la Red), ocasionando, por ejemplo, que la infección por *malware* suponga un perjuicio mucho más grave por la multitud y heterogeneidad de dispositivos a los que puede afectar, e introduciendo amenazas nuevas contra la ciberseguridad como los llamados *medjack* (secuestro de dispositivos médicos con objeto de abrir puertas traseras en las redes hospitalarias) y *skimming* (obtención ilegal de información de los dispositivos RFID, muy utilizados para etiquetar objetos). Los ataques DoS suponen, por el mismo motivo, un peligro mucho más elevado, ya que la indisponibilidad de un sistema informático derivado de un ciberataque puede traducirse en la imposibilidad de atender a multitud de pacientes[728], pudiendo verse lesionados a causa de esta eventualidad una pluralidad de bienes jurídicos.

Los hospitales inteligentes están especialmente expuestos a diversas modalidades de ciberataque, de entre las que hay que destacar las siguientes, las cuales, por sus variadas características, merecen una respuesta individualizada y distinta por parte del Derecho penal: primera, ataques de ingeniería social dirigidos contra personal del hospital, a través de los cuales se pretende recopilar información y sentar las bases para posteriores ataques, en ocasiones instalando algún tipo de *malware* (dependiendo de la acción típica y, sobre todo, de si el sujeto activo consigue hacerse con una contraseña que le proporcione acceso a un sistema

[728] Llaneza González, *Seguridad y responsabilidad en la Internet de las cosas (IoT)*, pp. 254 – 255.

informático, arts. 197 bis 1 del CP, o 197 y sucesivos del mismo texto legal, o art. 264 del CP en caso de utilizar éste cualquier tipo de *malware*); segunda, alteración intencionada de dispositivos médicos (dependiendo de si se trata de un ataque contra el *hardware* o contra el *software*, y en ausencia de una valoración más profunda de los ataques mixtos como la ya realizada en el capítulo tercero de esta investigación, arts. 263 o 264 del CP, respectivamente); tercera, sustracción de equipo hospitalario (el elevado valor económico de distintos componentes del equipo de un hospital inteligente, como los ya referenciados robots quirúrgicos, los convierten en un objetivo previsible para los ciberdelincuentes, ya estén protegidos, o no, por sus propias medidas de ciberseguridad, circunstancia que será esencial valorar al aplicar alguno de los apartados del art. 238 del CP); cuarta, ataques de *ransomware* a los sistemas informáticos del hospital, evitando su correcto funcionamiento o cifrando su contenido e impidiendo su acceso (al tratarse de un *malware* de rescate, y, por lo tanto, de una modalidad de *malware*, el art. 264 del CP protege los hospitales inteligentes frente al *ransomware*); y quinta, ataques DDoS dirigidos específicamente contra los servidores del hospital inteligente (de nuevo, es de aplicación el art. 264 del CP, si bien esta clase de ataques, y más teniendo en cuenta el objetivo específico, pertenecen al ámbito exclusivo de lo lógico, de lo inequívocamente digital[729]).

Atendiendo a la importancia de la ciberseguridad en los hospitales inteligentes y de los desafíos cada vez más novedosos, siempre análogos al avance de las nuevas tecnologías sanitarias, es esencial contar con al menos un ECS en cada hospital o centro sanitario que atienda a una cantidad suficiente de pacientes como para necesitarlo tras una evaluación objetiva. A él le corresponderán los deberes de identificar las brechas de seguridad informática presentes o futuras y de planificar respuestas para las mismas. Es indudable, en todo caso, que su preocupación principal serán los datos reservados de carácter personal que pertenecen a los pacientes (de ahí la importancia en este ámbito de los arts. 197 y sucesivos del CP), si bien

[729] Llaneza González, *Seguridad y responsabilidad en la Internet de las cosas (IoT)*, pp. 258 – 259.

deberá prever cualquier modalidad de ciberataque, aplicando tras cada uno de los mismos los conocimientos extraídos con objeto de fortalecer las medidas de ciberseguridad orientadas a la protección del hospital o centro sanitario[730].

4.5 Internet de las Cosas Médicas (IdCM)

El Internet de las Cosas Médicas o IdCM (*Internet of Medical Things*, o *IoMT*) es solo unas de las modalidades de Internet de las Cosas o IdC (*Internet of Things*, o *IoT*), pero se trata de una de las más importantes porque los dispositivos conectados al mismo pertenecerán a la categoría de dispositivos críticos, constituyendo su utilización incorrecta grandes riesgos[731]. Y es que todo aquello que se conecta a Internet es inevitablemente susceptible de convertirse en objetivo de un ciberataque[732]. No obstante, dando por sentado siempre que existirán las medidas de ciberseguridad adecuadas, en este caso los argumentos a favor sí parecen superar a los argumentos en contra, y la posibilidad de monitorizar el estado de salud sobre todo de pacientes ancianos o con enfermedades crónicas, así como de asesorarlos en su propio domicilio, se traduce, sin duda, en un aumento de su calidad de vida. Existen muy distintas innovaciones tecnológicas conectadas al IdCM, que van desde dispositivos móviles algo más clásicos a la nueva tecnología ponible, vestible, o tecnología corporal, y que permite la monitorización de constantes vitales y medir diversos parámetros fisiológicos (como la temperatura corporal, la respiración, el nivel de oxígeno en sangre,

[730] R. Guillén, "Retos a la Hora de Proteger la Ciberseguridad de los Hospitales Conectados", *Revista de la Sociedad Española de Informática y Salud*, no. 134, 2019, p. 40. En la práctica, garantizar este nivel de ciberseguridad hace necesario aplicar tecnologías como el cifrado o el escaneo de vulnerabilidades.

[731] L. Joyanes Aguilar, *Internet de las Cosas. Un futuro hiperconectado: 5G, Inteligencia Artificial, Big Data, Cloud, Blockchain y Ciberseguridad*, 1ª ed., Barcelona, Marcombo, 2021, p. 22. Existe una gran falta de seguridad en muchos dispositivos conectados, aumentando esto los factores de riesgo para los mismos.

[732] R.H. Weber y E. Studer, "Cybersecurity in the Internet of Things: Legal aspects", *Computer Law & Security Review*, no. 32, 2016, p. 715. Sirva como ejemplo el caso seleccionado por los autores, un ciberataque cuyo objetivo fue entregar dosis equivocadas de medicamentos con el objetivo de dañar a los pacientes.

la actividad muscular o cerebral o los patrones de movimiento del paciente). Esto, además, aumenta la independencia del paciente, que se ve liberado para acudir con menor regularidad al hospital o centro sanitario, aspecto doblemente positivo por suponer una descongestión de los mismos, y con el que estoy de acuerdo siempre que esta tecnología nunca invada el cuerpo humano (es decir, que cumplan siempre el requisito de poder ser considerados no invasivos) y la disminución de las visitas no suponga una excusa para disminuir la calidad de los servicios sanitarios, especialmente los públicos.

Los desafíos que el IdCM enfrentará en el futuro continúan siendo, sobre todo, los relativos a la seguridad y a la privacidad[733], que no son sino sus desafíos tradicionales. Los dispositivos médicos conectados a Internet siempre han corrido un triple riesgo vinculado a la ciberseguridad: primero, un ataque contra su disponibilidad podría afectar a la seguridad de un paciente a causa de la imposibilidad de acceder a información esencial para adoptar decisiones clínicas; segundo, un ataque contra su integridad que conlleve la alteración maliciosa de datos podría llevar al paciente a ser víctima de decisiones clínicas incorrectas; y tercero, un ataque a su confidencialidad podría suponer una transgresión no solo de normas penales, sino también de la abundante legislación extrapenal en esta materia[734].

La dependencia de los dispositivos conectados al IdCM respecto de redes informáticas poco fiables, unido a la ocasional ausencia de medidas de ciberseguridad, hace posible que un ciberdelincuente pueda interceptar datos entrantes o salientes. Para evitarlo, es necesario combinar medidas de seguridad técnicas y no técnicas. Las primeras suponen la aplicación de tecnologías ya mencionadas en apartados anteriores de este capítulo, como

[733] C. Kotronis et al., "Evaluating Internet of Medical Things (IoMT)-Based Systems from a Human – Centric Perspective", *Internet of Things,* vol. 8, 2019, pp. 3 – 15. De nuevo, y al igual que sucedía con los drones, el cuidado desde el diseño y el respeto por las regulaciones y por el marco legal existentes en relación con la protección de los datos sanitarios resulta fundamental, especialmente en lo concerniente al RGPD.

[734] P.A.H. Williams y A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem", *Medical Devices: Evidence and Research*, vol. 8, 2015, p. 309.

la autenticación de múltiples factores, o la biometría del comportamiento y las pruebas biométricas; mientras que las segundas se centran en la formación del personal sanitario[735].

Desde una perspectiva jurídico-penal, y a causa del tipo de datos en riesgo (principalmente, datos de tipo sanitario enviados a o recibidos desde dispositivos médicos), será de aplicación, sobre todo, el art. 197.5 del CP en relación con alguno de los apartados anteriores del mismo artículo, que el legislador incluyó específicamente para la protección de datos de carácter personal que revelen, entre otros, el estado de salud de la víctima, y que prevé la imposición de las penas previstas en otros apartados en su mitad superior.

Por último, en lo concerniente a la tendencia a conectar a Internet cada vez más elementos, creo que es necesario, por mucho que suponga ser una voz discordante, evidenciar la locura que supone pretender conectar a la Red no dispositivos externos al cuerpo humano, sino partes o la totalidad del cuerpo humano. El avance de la tecnología y las escasas críticas a un progreso desmesurado harán, sin duda, que todo objeto material susceptible de serlo acabe siendo conectado a Internet, pero supondría un tragedia inconmensurable la conexión al mismo, como ya se propone y se experimenta, de cuerpos humanos. Aunque la conexión generalizada puede considerarse asfixiante sin importar las medidas de ciberseguridad existentes (pues incluso un funcionamiento óptimo supone un flujo de datos e información exagerados e innecesarios), considero que el límite indiscutible en este sentido deben ser los dispositivos externos al cuerpo humano, o no

[735] J.A. Yaacoub et al., "Securing internet of medical things systems: Limitations, issues and recommendations", *Future Generation Computer Systems*, vol. 105, 2020, pp. 586 – 598. Aunque los datos reservados de carácter personal son el principal objetivo de los ciberdelincuentes en este ámbito, son posibles otras muchas modalidades de ciberataque frente a las que deben establecerse medidas de ciberseguridad adecuadas. La introducción de *software* malicioso en un dispositivo médico puede conllevar lesiones físicas para los pacientes que los utilizan, un cambio mortal en la dosis de medicamentos que necesitan, o un ataque a implantes conectados, motivo por el cual existen ya medidas de prevención como el bloqueo de su manejo a distancia para evitar lesiones ocasionadas voluntariamente por parte de terceros. El deber de establecer medidas de seguridad informática físicas y lógicas en los dispositivos médicos recae principalmente, como en el caso de otras nuevas tecnologías ya mencionadas, sobre sus fabricantes.

invasivos, no debiendo conectarse a Internet mediante una conexión invasiva cuerpo humano alguno. Y esto porque ni existe necesidad de que así sea, ni existen garantías, como en el caso de los dispositivos externos, de la posibilidad de volver a separarse de la Red cuando lo desee su portador. Sus contras, todos ellos de suma gravedad, no han sido suficientemente debatidos. Estas pretensiones podrán no transgredir, ni ahora ni en el futuro, norma jurídico-penal alguna, pero plantean una serie de cuestiones religiosas de la mayor profundidad, puesto que son el principio de una modificación del ser humano que no le reportará ningún beneficio y solo abrirá la puerta a un transhumanismo opuesto a su verdadera naturaleza. Debemos esforzarnos por mejorar la salud del ser humano sin transformar al ser humano.

4.6 La nube sanitaria

La nube (*Cloud Computing*) es un modelo de acceso remoto que utiliza una red de comunicaciones para permitir, bajo demanda, un rápido acceso a un conjunto compartido de recursos configurables de carácter informático con una mínima intervención del proveedor del servicio. Se trata de una opción que será cada vez más utilizada en el ámbito sanitario por su capacidad masiva de almacenamiento de datos y por la posibilidad de acceder a la misma de manera remota, lo que ofrece grandes posibilidades a los profesionales de la salud, quienes ya no se encuentran atados a un *hardware* localizado en una ubicación física específica para el acceso a la información o a distintos tipos de *software*, suponiendo esto un importante avance, sobre todo, para la atención de emergencias extrahospitalarias, en los que estos se ven obligados a alejarse del hospital o del centro sanitario que, hasta ahora, albergaba de manera exclusiva esta clase de contenidos.

El Derecho penal ha protegido la nube a través de los datos contenidos en la misma, no existiendo un contenido jurídico-penal unitario relacionado con ella, sino una protección parcial y disgregada a través de distintos tipos delictivos, como el art. 197 del CP para particulares y el art. 278 del CP en el caso de que la información protegida consista en secretos de empresa.

Además, desde la reforma del año 2015 se protegen también el propio servidor de accesos no deseados (es decir, de brechas en las medidas de ciberseguridad[736]) y el proceso de transmisión de datos hacia el mismo, el primero a través del art. 197 bis 1 del CP (toda vez que la nube encaja en la descripción de sistema de información exigida por el tipo), y el segundo mediante el art. 197 bis 2 del mismo texto legal, que ampara todo proceso de transmisión no pública de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, sobre todo si se trata de datos de tipo sanitario[737].

Corresponde al usuario averiguar la localización de los servidores que utilizará para saber si su ubicación se encuentra dentro del territorio de la UE, de modo que, en caso contrario, y de haber una transferencia internacional de datos, se asegure de que el país en el que se encuentran ofrece unas garantías jurídicas adecuadas antes de enviarlos[738]. A causa de la complejidad de este trámite, resulta aconsejable la utilización de servicios en la nube previamente investigados y aprobados por especialistas en ciberseguridad sanitaria, so riesgo para los profesionales de hospitales y centros sanitarios de enfrentarse, en caso de litigio, a procesos penales en

[736] C. Serrano Durbá, "Garantías de seguridad en los servicios de computación en nube", en D. Canals Ametller (dir.), *Ciberseguridad: un nuevo reto para el Estado y los Gobiernos Locales*, 1ª ed., Madrid, Wolters Kluwer, 2021, pp. 329 – 332. Aunque la nube proporcione una mayor facilidad para implantar medidas de ciberseguridad, también aumenta en ella la exposición a las actividades de los ciberdelincuentes. Entre sus principales objetivos está la obtención ilegal de datos mediante el robo de los mismos, ya sea aprovechando las vulnerabilidades de una aplicación o las malas prácticas de ciberseguridad, y abarcando las modalidades de información sustraída, incluso, hasta los datos sanitarios.

[737] M.I. Montserrat Sánchez-Escribano, "La protección penal del servidor de Cloud Computing y de los datos almacenados en él o en proceso de transferencia hacia él", en Apolònia Martínez Nadal (dir.), *Big Data, Cloud Computing y otros retos jurídicos planteados por las tecnologías emergentes*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2019, pp. 105 – 119. En el caso del art. 197 bis 2, el hecho de que las comunicaciones en relación con la nube suelan ser unidireccionales (técnicamente, el usuario se envía archivos a sí mismo) no supone un problema jurídico, pero, a juicio de Montserrat Sánchez-Escribano, sí podría considerarse contrario al verdadero espíritu de la norma, que pretende proteger la comunicación entre distintos usuarios.

[738] A. Postigo Palacios, *Seguridad informática,* 1ª ed., Madrid, Paraninfo, 2020, p. 304.

los que las normas se fijen desde el extranjero, con los costes económicos que ello supone, especialmente si no se elige el lugar donde litigar[739].

4.7 Salud electrónica

La salud electrónica (*e-Health*) es la combinación de la informática médica y de la salud pública orientada a mejorar la atención en los servicios de salud mediante el uso de tecnología de la información y de la comunicación. Al menos en su concepción teórica, se entiende como un medio para expandir, ayudar, o mejorar las actividades humanas, y en ningún caso como un sustituto de la acción humana[740], aspecto con el que coincido del todo y que espero que no varíe, con independencia del nivel de desarrollo de esta tecnología.

Dentro de la salud electrónica, que no debe confundirse con la salud móvil (*m-Health*, consistente en la interacción con fines sanitarios mediante el teléfono móvil llevada a cabo, sobre todo, a través de aplicaciones) se engloban la telemedicina (suministro de servicios de atención sanitaria utilizando las TIC para intercambiar información) y los sistemas informáticos de salud (*software* que permite a los hospitales o centros sanitarios llevar un control de los servicios prestados a los pacientes, obtener datos epidemiológicos o acceder a las historias clínicas electrónicas). A nivel normativo, la salud electrónica se encuentra escasamente regulada, existiendo muy pocas disposiciones legales relacionadas con la misma. De hecho, no existe en España ninguna norma explícita sobre la misma, lo que no impide una proliferación cada vez mayor de ordenadores y dispositivos

[739] J.L. González Cussac, "Computación en nube: la verificación de los ordenamientos internos en los países de localización como garantía de la seguridad y la confidencialidad de la información", en R. Martínez Martínez (edit.), *Derecho y Cloud Computing*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2012, pp. 289 – 307.

[740] S. Ferrer Gelabert, "E-salud: la tecnología al servicio de la salud", en C. Gil Membrado (dir.), *E-salud, autonomía y datos clínicos. Un nuevo paradigma*, 1ª ed., Madrid, Dykinson, 2021, p. 15. La definición de la salud electrónica es enormemente reciente. Tanto es así, que para desarrollarla sintetizando las más comúnmente citadas hubo que llevar a cabo una revisión sistemática de la literatura médica contenida en diversas bases de datos bibliográficas que consistió en el análisis individual de 1209 resúmenes y 430 citas.

portátiles y una implantación progresiva de innovaciones como la historia clínica electrónica[741]. Esta investigación ya ha dado respuesta jurídico-penal a otras como la necesidad de garantizar la ciberseguridad de la robotización de las instalaciones quirúrgicas, desafío al que, con el tiempo, se unirán la posibilidad de acceso a resultados diagnósticos desde cualquier parte, los sistemas de monitorización avanzada de pacientes o el uso de sistemas de videoconferencia para las consultas con los facultativos, por plantear todas ellas serios problemas en relación con la ciberseguridad y la protección de datos que podrían llevar a reconsiderar la redacción de los arts. 197 y sucesivos del CP, y especialmente del 197.5.

La adecuada gestión de la información y de la asistencia médicas resulta, por otro lado, esencial a medida que las TIC avanzan permitiendo un nivel cada vez mayor de participación de los pacientes en los asuntos relacionados con su propia salud. Y es que las barreras entre médico y paciente se difuminan cada vez más, como sucede en el caso de, entre otras, las personas contagiadas del virus de la inmunodeficiencia humana, cuyas búsquedas de información en línea suponen un riesgo de recurrir al autodiagnóstico[742], cuyo rechazo de las aplicaciones y dispositivos inteligentes en el ámbito sanitario evidencia un temor a la ausencia, justificada en cierto modo, de una atención médica especializada humana que evidencie que estas tecnologías se tratan de un mero complemento, y no de una sustitución, de la misma[743], y cuya persistente desconfianza en la seguridad de la recopilación de datos sanitarios hace más compleja la implantación de

[741] González et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 – 2021*, pp. 395 – 407.

[742] C. Jacomet et al., "E-health. Patterns of use and perceived benefits and barriers among people living with HIV and their physicians. Part 1: Information retrieval on the Internet and social networks", *Médecine et Maladies Infectieuses*, vol. 50, no. 7, 2020, p. 579. Casi la mitad de las personas que buscaron datos sobre su enfermedad en Internet cambiaron la manera de cuidar su salud como consecuencia de los resultados.

[743] C. Jacomet et al., "E-health. Patterns of use and perceived benefits and barriers among people living with HIV and their physicians. Part 2: Health apps and smart devices", *Médecine et Maladies Infectieuses*, vol. 50, no. 7, 2020, p. 587. Estas reticencias disminuirían si los facultativos demostrasen que, en caso de no saber o no querer utilizar el IdCM, los pacientes pueden seguir siendo atendidos sin complicaciones.

la salud electrónica[744]. En este último caso, y con independencia de la valoración que merezcan estos avances cuando se juzgan desde otras perspectivas, resulta lamentable que su implantación se frene por la percepción, muchas veces acertada, de que no van acompañados de medidas de ciberseguridad suficientes para garantizar los derechos de los pacientes. En este sentido, desde el Derecho penal solo cabe respaldar y reforzar las mismas y las posibles normas extrapenales existentes en este ámbito mediante la persecución de los accesos ilícitos y la protección de los datos sanitarios a través de la aplicación del art. 197.5 del CP, cuando se considere que bienes jurídicos como la intimidad o los datos reservados de carácter personal han sido vulnerados por el ciberdelincuente[745].

4.8 Los avances tecnológicos obligan a ir más allá de las clásicas cuestiones de *lege lata* y *lege ferenda*

A pesar de todo lo expuesto en esta investigación, en el año 2021 el INCIBE reportó 109.126 incidentes de seguridad, cifra que evidencia la necesidad de continuar trabajando para mejorar los niveles de ciberseguridad de nuestras redes y sistemas informáticos. Resulta por completo imposible, sobre todo desde una perspectiva material, pretender perseguirlos en vía penal, máxime cuando, con el tiempo, se espera un crecimiento progresivo de la cantidad y de la complejidad de los mismos. Un estudio[746] realizado en

[744] C. Jacomet et al., "E-health. Patterns of use and perceived benefits and barriers among people living with HIV (PLHIV) and their physicians. Part 3: Telemedicine and collection of computerized personal information", *Médecine et Maladies Infectieuses*, vol. 50, no. 7, 2020, p. 595. La propuesta para conseguir que los pacientes no teman por sus datos se basa en una legislación más robusta y fiable en este ámbito.

[745] V. Sanchini y L. Marelli, "Data Protection and Ethical Issues in European P5 eHealth", en G. Pravettoni y S. Triberti (eds.), *P5 eHealth: An Agenda for the Health Technologies of the Future*, 1ª ed., Cham, Springer, 2020, p. 186. Se plantea, también en relación con la salud electrónica, la necesidad de alcanzar el equilibrio planteado en el análisis de la IA: por un lado, deben protegerse los derechos de las personas, pero por otro, esta protección no debe impedir el desarrollo de innovaciones tecnológicas verdaderamente beneficiosas.

[746] Emergency Care Research Institute, "Cybersecurity attacks top ECRI list of health technology hazards for 2022", *Reactions Weekly*, vol. 1892, no. 1, 2022, p. 1. Estos peligros han sido seleccionados por un grupo multidisciplinar compuesto por médicos,

Pensilvania, EE. UU., identificó como principales peligros para la ciberseguridad de hospitales y centros sanitarios en 2022, destacando entre ellas la posibilidad de que la IA ofrezca diagnósticos erróneos, los dispositivos equipados con IdC con medidas insuficientes de ciberseguridad y que la ausencia de wifi provoque retrasos, lesiones o incluso la muerte al paciente. Todos ellos son peligros susceptibles de impedir la atención debida a los pacientes, constituyendo un verdadero peligro para su bienestar físico. Todos los hospitales y los centros sanitarios corren el peligro de sufrirlos, hasta el punto de que la pregunta que plantean los expertos no es si serán atacados, sino cuándo serán atacados. Para responder a estos peligros es necesario un programa de seguridad robusto, de lo que se deduce que en este nuevo siglo no solo se espera de los hospitales y de los centros sanitarios que curen a las personas, sino que también les ofrezcan garantías desde el punto de vista de la ciberseguridad, incluyendo la de los dispositivos médicos conectados a una red que podrían formar parte de un determinado tratamiento o del proceso de recuperación de un paciente.

Las consecuencias de ignorar esta nueva e inexcusable faceta de la atención sanitaria son el caos en el sistema de citas o de organización de intervenciones quirúrgicas, la utilización incorrecta de vehículos de emergencia, el cierre preventivo de unidades de cuidados intensivos o, incluso, de hospitales y centros sanitarios enteros, dependiendo de la gravedad que lleve aparejada un determinado peligro para la seguridad de los pacientes.

En lo que respecta a la UE y a España, otro estudio[747] basado en entrevistas a los principales expertos de los centros públicos y de las

ingenieros biomédicos y expertos en gestión sanitaria tras un estricto proceso de selección de la información obtenida a partir del análisis de incidentes en este ámbito.

[747] U. Von der Leyen et al., “Cómo evolucionarán los ciberataques en 2022”, *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, vol. 31, no. 148, 2022, pp. 94 – 144. De manera específica, Von Der Leyen, cuya aportación ha sido extraída de su discurso sobre el estado de la Unión de 15 de septiembre de 2021, destaca la naturaleza cambiante de las ciberamenazas, destacando entre ellas los ataques híbridos, así como la importancia de la interoperabilidad. Hoy, no puede haber defensa sin ciberseguridad.

empresas de ciberseguridad más destacados sostuvo que, aunque en 2022 no se esperan cambios revolucionarios, la ciberdelincuencia seguirá evolucionando e innovando, adaptándose con rapidez a nuevos escenarios y centrándose en las infraestructuras críticas sanitarias mediante acciones como una intensificación de los ataques dirigidos contra las mismas, sobre todo mediante *ransomware*. Este estudio coincidió con el de sus homólogos estadounidenses en su preocupación por los dispositivos equipados con IdC, puesto que resulta muy difícil dotarlos de una seguridad informática suficiente. Por último, el gran volumen de trabajadores en este sector que disponen de acceso a datos sanitarios de pacientes con un carácter valioso y altamente comercializable recogidos y almacenados en cantidades colosales los convierte en objetivos prioritarios de nuevas modalidades de ciberataques orientados a sustraerlos.

Pero es que, además del crecimiento progresivo en la cantidad de ciberataques, las amenazas contra la seguridad informática también crecerán en complejidad, hasta el punto de empujarnos a una profunda reflexión en relación con la conveniencia de proporcionar protección jurídica a ciertas conductas. Es el caso, en la actualidad, de un Internet cada vez más innecesariamente invasivo del cuerpo humano bajo falsas promesas, o, en el futuro, de los úteros artificiales que se servirán de la IA y de la robótica para hacer viables embarazos externos al cuerpo de la mujer humana. Ambos harán posible que el cuerpo humano sea objeto material del delito en ciertos tipos de ciberataques, el primero por el carácter transhumanista derivado de su unificación de tecnología y cuerpo humano, y el segundo por vincular el desarrollo de la vida humana hasta niveles innecesarios a las tecnologías avanzadas que he mencionado, haciéndola dependiente de las mismas de manera antinatural. Ante casos como estos, considero que debemos adoptar una actitud pasiva y defender que no todo el desarrollo científico-tecnológico es deseable, y mucho menos inevitable. La clave está en analizar cada una de estas innovaciones y determinar si merecen ser protegidas o si, por el contrario, son las personas las que merecen protección jurídica frente a ellas. En el ámbito de las ciencias de la salud, la historia ya nos ha demostrado

cómo incluso cuando en los ordenamientos jurídico-penales occidentales prohibimos la manipulación genética (arts. 159 y sucesivos del CP), en países como China se han completado experimentos aparentemente exitosos valiéndose de la misma. Por mucho que finalmente se condenase a tres años de prisión al autor de los hechos, la transgresión tecnológica, y con ella el grave atropello al bien jurídico, ya no podrá deshacerse jamás.

La naturaleza poliédrica de la ciberseguridad exige unas respuestas frente a los peligros que la amenazan que también estén dotadas de dicha característica[748]. No todas deben ser jurídico-penales y ni siquiera legales, sino que tras una atención cotidiana y permanente es necesario plantear distintos escenarios de respuesta. Para ello, es necesaria la creación de nuevas figuras, como el Especialista en Ciberseguridad Sanitaria[749] (ECS), a quien yo atribuyo una doble función: primera, actuar como primer filtro analítico de la realidad cotidiana de los hospitales y de los centros sanitarios en materia de ciberseguridad, realizando estadísticas o estudios generales de los casos más comunes y profundizando en los más novedosos o extraños cuya complejidad lo requiera; segunda, servir de apoyo como asesor jurídico en el desarrollo legislativo (entre ellos, el específicamente jurídico-penal) relativo a la ciberseguridad. Y es que la innovación en ciberseguridad no debe tener lugar solo en centros tecnológicos, sino que también debe considerarse como parte de la misma el desarrollo de novedades legislativas, sin las cuales no sería posible alcanzar los objetivos de I+D+i y sería muy difícil, ante la falta de confianza en el ordenamiento jurídico-penal de uno de los potenciales socios, colaborar en proyectos o iniciativas tecnológicas a nivel comunitario o

[748] J.J. Fernández Rodríguez, "Ciberseguridad: ¿Desafío insuperable? En búsqueda de escenarios de respuestas adecuados", en C. García Novoa y D. Santiago Iglesias (dirs.), *4ª Revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital*, Cizur Menor, Aranzadi, 2018, pp. 76 – 77. La capacidad de los aplicadores del Derecho para realizar su labor interpretativa en el mundo digital resulta esencial, puesto que de la misma se derivan las posibles actualizaciones normativas.

[749] P.A.H. Williams et al., "Working as a Health Cybersecurity Specialist", en K. Butler – Henderson, K. Day, y K. Gray (eds.), *The Health Information Workforce: Current and Future Developments*, Cham, Springer, 2021, p. 225. Esta especialidad, de gran importancia y múltiples aplicaciones, ya está caracterizada, y es previsible que se vaya implementado a medida que se adquiera conciencia sobre lo necesaria que es.

internacional. Con este objetivo, en lugar de formular directamente una propuesta de *lege ferenda*, creo necesaria la creación de un sistema de tres niveles que obligue al legislador a profundizar en relación con cada innovación tecnológica relacionada con la ciberseguridad antes de proponer incluirla en nuestro ordenamiento jurídico-penal, que sería la cúspide del mismo, pero exigiría unos requisitos para llegar a dicho tercer nivel.

Primero, un análisis de amenazas a la ciberseguridad en el ámbito extrapenal que incluya no solo a la ENISA o al INCIBE, sino a nuevas figuras como el ECS que permitan conocer la realidad diaria de los hospitales y de los centros sanitarios con objeto de hacer frente al crecimiento progresivo de la cantidad y de la complejidad de los ciberataques de manera activa. A nivel intelectual, la valoración más importante a este nivel, que requiere un profundo juicio de valor, es la decisión sobre si se va a proteger mediante novedades legislativas la ciberseguridad en relación con una determinada innovación tecnológica o si, por el contrario, lo que procede es prohibirla para proteger a las personas de la misma.

Segundo, un análisis que responda a tres cuestiones fundamentales: si la innovación tecnológica es cibersegura en sí misma, si resulta posible protegerla mediante la legislación frente a los ciberdelincuentes y, por último, el planteamiento sobre la adecuación de regularla en el ámbito privado, en el administrativo o, ante la imposibilidad de hacerlo en los dos anteriores, de aplicar el *ius puniendi* estatal y acudir al Derecho penal. En este nivel deben tenerse en cuenta las implicaciones a corto, medio y largo plazo de esta actividad legislativa, de manera que las limitaciones que se establezcan no se conviertan en trabas para la libertad de las personas en el futuro y, *a contrario sensu*, que lo que se permite en un momento determinado no degenere en un riesgo para otros bienes jurídicos en el futuro.

Tercero, realización de una propuesta jurídico-penal clásica de *lege ferenda*.

4.9 El futuro jurídico-penal de la ciberseguridad en el ámbito sanitario

La principal amenaza es lo que se ha llamado popularmente “el gran apagón”: la caída, provocada o no, de Internet a nivel mundial, que supondría un riesgo para la ciberseguridad de primer orden de muy difícil control. Iría mucho más allá de los estragos del art. 346 del CP, puesto que, si se tratase del resultado de la acción dolosa de un individuo o de un colectivo, lesionaría la práctica totalidad de bienes jurídicos que se pretenden proteger mediante este texto legal. Incluyo aquí este desafío, que quizá debería ser el último, por ser el más grave pero también el más improbable, salvo escenarios bélicos internacionales, ya que quiero destacar su importancia: sin un qué o un dónde, no hay un cómo: solo podemos proporcionar seguridad a aquello que existe. El gran apagón supone el ataque definitivo: la ausencia de disponibilidad de toda red y sistema informático sobre la faz de la tierra, o, de acuerdo con previsiones más comedidas, en zonas específicas de la misma. Haría posible, además, poner a cero los contadores de la banca o pérdidas de datos masivas en sectores específicos, siendo imposible calcular la cuantía o la gravedad de los daños. Además, por su carácter internacional, daría lugar a complejas cuestiones de aplicación de la ley penal en el espacio, dando por hecho el mantenimiento del orden social.

Descartando escenarios como el anterior, el futuro de la ciberseguridad en el ámbito sanitario se sostiene sobre tres pilares: la ciberbioseguridad, la computación cuántica y el metaverso. Antes de analizar cada uno de ellos es necesario aclarar una serie de conceptos.

El núcleo de la protección continuarán siendo los datos sanitarios de los pacientes[750], de manera que no solo estén protegidos[751] sino que puedan ser utilizados para ayudarles[752]. De manera que por mucho que el art. 197 bis

[750] Supervisor Europeo de Protección de Datos, *Shaping a Safer Digital Future. The EDPS Strategy 2020 - 2024*, Bruselas, Supervisor Europeo de Protección de Datos, 2021, p. 10. El objetivo es encontrar un justo equilibrio entre garantizar la salud pública y asegurar la protección y la privacidad de los datos personales.

[751] J. Whitfill, “Data Security and Patient Privacy”, en B.F. Branstetter IV (edit.), *Practical Imaging Informatics: Foundations and Applications for Medical Imaging*, 2ª ed., Cham, Springer, 2021, pp. 119 – 120.

[752] A. Herrero González, “The value of data and its applicability in the Health Sector”, *Revista Española de Medicina Nuclear e Imagen Molecular*, vol. 41, no. 1, 2022, p. 40. Estos datos hacen posible, por ejemplo, la detección de ciertas características en las

1 del CP se traslade a un nuevo título dedicado a la protección del bien jurídico ciberseguridad, los arts. 197 y sucesivos del CP seguirán teniendo una gran trascendencia, por mucho que sea ya casi un clásico la recomendación de dotar de una redacción menos enrevesada y de una nueva estructura más lógica al propio art. 197 del CP. El principal objetivo de los profesionales de la ciberseguridad en el ámbito sanitario será mantenerse a la altura de los ciberdelincuentes, para lo que será necesario contar con profesionales especializados capaces de realizar previsiones a largo plazo[753], como el ya mencionado ECS. Como ya señalé en el apartado de este capítulo dedicado a la IA, si bien se utilizará en la mayoría de especialidades médicas[754], empezará a pasar a un segundo plano en favor de la computación cuántica, siendo necesario un nivel cada vez mayor de ciberseguridad para evitar los ciberataques. Por último, es previsible el surgimiento de cada vez más nuevos campos científicos, como la incipiente informática biomédica[755].

Entre los mismos, el más destacable será el de la ciberbioseguridad, que integrará tres conceptos clave, dos de ellos pertenecientes a la definición de ciberseguridad de esta investigación: ciberseguridad física, ciberseguridad lógica y bioseguridad. Con el tiempo, lo que se espera de la misma es que proporcione la posibilidad al usuario de encriptar y desencriptar un dispositivo personal mediante el ADN, siendo esta una medida de seguridad que blindará una red o sistema informático, si bien planteará nuevas cuestiones, como la seguridad del propio ADN humano. No hay que olvidar los peligros señalados por los profesionales estadounidenses y europeos en relación con los

arterias de los pacientes que están asociadas a síntomas tempranos de enfermedades cardiovasculares, permitiendo la prevención de muchos ataques al corazón.

[753] Agencia de la Unión Europea para la Ciberseguridad, *Foresight Challenges: A study to enable foresight on emerging and future cybersecurity Challenges,* Atenas, Agencia de la Unión Europea para la Ciberseguridad, 2021, p. 47. Además, los métodos y herramientas utilizados deben adecuarse al objetivo.

[754] J.A. Vallejo Casas y E. Rodríguez Cáceres, “Inteligencia Artificial y Medicina Nuclear. Hoy ya es futuro”, *Revista Española de Medicina Nuclear e Imagen Molecular*, vol. 41, no. 1, 2022, pp. 1 – 2.

[755] J.J. Cimino et al., “The Future of Informatics in Biomedicine”, en E.H. Shortliffe y J.J. Cimino (eds.), *Biomedical Informatics*, 5ª ed., Cham, Springer, 2021, p. 987. Este campo científico interdisciplinario utiliza los conocimientos existentes en el ámbito de la informática para mejorar el cuidado de la salud humana.

dispositivos conectados a IdCM, y que podrían verse solucionados mediante esta nueva tecnología. La información contenida en un dispositivo electrónico pasaría a estar protegida por la información personal contenida en un elemento biológico, como una célula. En todo caso, la fusión del mundo biológico con el digital planteará, por supuesto, nuevos retos y amenazas para la ciberseguridad[756]. Será el caso del proceso de transformación digital de los laboratorios actuales a los modernos laboratorios inteligentes del futuro, en los que se deberá poder garantizar un elevado nivel de ciberbioseguridad porque se usará la realidad virtual, especialmente para entrenar al personal que trabaje con materiales biológicos sensibles. Incluso se plantea el uso de *blockchain* para dejar constancia de cada paso de los experimentos realizados en el mismo[757], y la convergencia de las ciencias de la vida con la ciberseguridad en lo concerniente a la digitalización de la información de los pacientes[758].

La ciberbioseguridad permitirá también analizar el impacto humano de las nuevas tecnologías informáticas, como el controvertido 5G, cuyo impacto económico para 2030 ascenderá a 530.000 millones de dólares en relación con la sanidad y con la atención sociosanitaria. En teoría, más de la mitad del impacto del 5G en el mundo se producirá por su aplicación en el sector de salud y de atención sociosanitaria en los próximos diez años. En este sentido, sus defensores sostienen que resulta necesario, ya que la telemedicina es el

[756] F. Ruiz Domínguez, "Ciberbioseguridad: implicaciones técnico-jurídicas para la perfecta desconocida en seguridad y defensa", *Bie3: Boletín IEEE*, no. 22, 2021, pp. 662 – 674. Aunque todavía existen criterios dispares en EE. UU. y aún no ha habido un pronunciamiento específico por parte de su Corte Suprema, en el caso *Maryland v. King* (2013) 569 U.S. 435 ésta dictaminó que el ADN es comparable con las huellas dactilares a efectos identificativos. Un criterio que, con el tiempo, y si no hay oposición, podría reinterpretar el papel del ADN en lo relativo a la garantía de la seguridad de las redes y de los sistemas informáticos.

[757] J. C. Reed y N. Dunaway, "Cyberbiosecurity Implications for the Laboratory of the Future", *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 182, 2019, p. 13. La identificación biométrica se presenta como una propuesta para aumentar el nivel de ciberseguridad cuya aplicación se entiende que es solo cuestión de tiempo, sin reflexionar adecuadamente sobre sus profundas consecuencias para las personas.

[758] L.C. Richardson et al., "Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape", *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 99, 2019, p. 4. Como ya ha sucedido antes, los autores de este artículo señalan a los dispositivos médicos como uno de los objetivos potenciales de los ciberataques.

futuro de la atención médica. La atención remota será una de las áreas sanitarias en las que el 5G podrá permitir un mayor ahorro de costes y mejores resultados para la salud. Acompañado de los avances en robótica, IdCM e IA, el 5G podrá dar lugar al surgimiento de una nueva atención médica conectada, pero no hay que olvidar la opinión de sus detractores, quienes aseguran que esta tecnología es lesiva para el cuerpo humano y que las futuras redes 6G, 7G y sucesivas harán enfermar a las personas, yendo sus hipotéticas implicaciones, por lo tanto, y siempre de ser ciertas estas inquietantes afirmaciones, hasta el ámbito de los delitos contra la vida humana independiente recogidos en el CP.

El segundo de los pilares mencionados es la computación cuántica, capaz de destruir la seguridad del actualmente imbatible *blockchain*, así como de todo aquel elemento no encriptado cuánticamente: claves, contenido codificado, 5G, wifi, bluetooth, GPS, teléfonos, páginas web, e incluso armas estratégicas[759]. En la actualidad, se sabe que China está aumentado sus inversiones para avanzar más rápidamente en sus investigaciones en este ámbito y podría llevar la delantera a los países occidentales[760]. Mediante la aplicación de complejos números y matrices[761], la computación cuántica podría desafiar el *statu quo* de la Red, puesto que será capaz de entrometerse en comunicaciones supuestamente seguras y, además, de desencriptar todas las comunicaciones llevadas a cabo en el pasado.

Así, y a pesar de que esta tecnología no esté aun plenamente operativa, los consejos de los expertos son; primero, formalizar alianzas entre países afines para cooperar en este ámbito; segundo, desarrollar una autonomía suficiente llevando a cabo investigaciones propias; tercero, hacerse un hueco a nivel internacional en lo que respecta a las

[759] M.A. Caballero Velasco y D. Cilleros Serrano, *Ciberseguridad y transformación digital: Cloud, Identidad Digital, Blockchain, Agile, Inteligencia Artificial*, 1ª ed., Madrid, Anaya Multimedia, 2020, p. 303.

[760] M. McGuire, *Nation States, Cyberconflict and the Web of Profit*, Palo Alto, CA, HP Inc., 2021, p. 17.

[761] S. Kurgalin y S. Borzunov, *Concise Guide to Quantum Computing: Algorithms, Exercises and* Implementations, 1ª ed., Cham, Springer, 2021, p.1. Esto conlleva el uso del cúbit, es decir, del bit cuántico.

comunicaciones basadas en la computación cuántica; cuarto, financiar centros de investigación especializados en la materia; y quinto, proponer la posibilidad de compartir centros de investigación y laboratorios con países afines que también deseen colaborar[762]. Uno de los objetivos primordiales de estas alianzas es conseguir unas comunicaciones más seguras[763], así como garantizar un elevado nivel de ciberseguridad a los propios ordenadores cuánticos, los cuales, en la actualidad, son imposibles de trasladar a un hospital o centro sanitario, toda vez que requieren una temperatura casi criogénica que lo expone a ciberataques físicos y ciberfísicos muy específicos. Tanto los cambios de temperatura como las más mínimas vibraciones se convierten, así, en amenazas a su ciberseguridad[764]. Estos equipos son tan sensibles como necesarios, puesto que la criptografía que hasta ahora se utilizaba para proteger la práctica totalidad de comunicaciones a través de Internet, incluyendo las del ámbito sanitario, están obsoletas, con lo que ello implica para los datos[765].

¿Cómo se legisla en relación con aquello que es capaz de destrozar cualquier medida de ciberseguridad? Las consecuencias de la irrupción de la computación cuántica para los artículos 197 y sucesivos del CP, así como para el delito de daños informáticos, requerirá de profundas investigaciones y debates jurídicos en los que, indudablemente, el bien jurídico ciberseguridad cobrará un nuevo protagonismo si se pretenden proteger otros como la intimidad[766], los datos reservados de carácter personal, el patrimonio o la vida.

---

[762] R. Clark et al., *The impact of quantum technologies on secure communications*, Canberra, ACT, Australian Strategic Policy Institute, 2021, pp. 9 – 32. Los autores destacan como un hecho positivo que los EE. UU., Canadá, el Reino Unido y los países europeos hayan realizado ya inversiones en computación cuántica.

[763] J. Vos, *Quantum Computing in Action*, Shelter Island, NY, Manning Publications, 2020, pp. 142 – 168.

[764] R.L. Amoroso, “Imminent Advent of Universal Quantum Computing (UQC)”, en L.M. Caligiuri (edit.), *Frontiers in Quantum Computing*, Hauppauge, NY, Nova Science Publishers, 2020, pp. 269 – 270.

[765] J.D. Hidary, *Quantum Computing: An Applied Approach*, 1ª ed., Cham, Springer, 2019, p. 14.

[766] F.J. Aranda Serna, *Derecho y Nuevas Tecnologías. La influencia de Internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento*

Por último, el tercero de los tres pilares será el metaverso. Presentado e introducido de manera casi tímida como una magnífica oportunidad para entrenar al personal sanitario o de laboratorios biomédicos encargado de las tareas más complejas y peligrosas, se trata no del sustituto, sino de la evolución de Internet: un mundo virtual que va más allá de la realidad virtual y que, como su predecesor, revolucionará todos los ámbitos de la sociedad, incluyendo el sanitario[767]. Aunque incluso sus más fervientes defensores[768] admiten que también hará que aumenten los riesgos[769] para los usuarios, es indudable que permitirá asistir a una consulta médica virtual desde cualquier lugar y recibir toda aquella parte de la asistencia sanitaria que no requiera interacción física entre médico y paciente (resolución de dudas, entrega de recetas digitales, o análisis visual de signos y síntomas mediante fotografías y videocámara de alta definición). Esto, que plantea ya de por sí serias dudas en relación con la protección de los datos sanitarios de los pacientes, y que obligará a abordar desde una perspectiva nueva artículos como el 197 y sucesivos del CP, se une a un defecto de la propia tecnología que podría acabar trasladándose al ámbito sanitario. El metaverso es una cuestión científica de primer orden. Ahora mismo, existe la posibilidad mediante video y audio de engañar al cerebro, como sucede con el creciente número de personas que, en lugar de no escuchar ningún sonido artificial ni escuchar

jurídico español, 1ª ed., Madrid, Dykinson, 2021, p. 115. La protección de la intimidad trasciende hoy las barreras físicas, y debe abarcar todos los ámbitos de la vida de las personas por las profundas huellas digitales personales que imprimen.

[767] M. Ball, *The Metaverse: And How It Will Revolutionize Everything*, 1ª ed., Nueva York, NY, Liveright Publishing Corporation, 2022, p. 19. El metaverso supone una revolución equiparable a la que hizo posible navegar por Internet en los teléfonos móviles, aunque mucho más inmersiva e insegura a muchos niveles.

[768] K. Roth, "Implications for Virtual Worlds: A Comparative Study of United Kingdom, United States and Australia on Networks Readiness, Government Investment and Cyber-security", *Journal of Virtual Worlds Research*, vol. 2, no. 5, 2010, p. 10. En ocasiones, las precauciones relativas a la ciberseguridad de un determinado ámbito, como el metaverso, resultan prematuras. Es el caso de esta investigación, que se adelantó más de doce años a su tiempo previendo una inminente llegada del metaverso que no tuvo lugar.

[769] J. Bailenson, *Experience on Demand: What Virtual Reality Is, How It Works, and What It Can Do*, 1ª ed., Nueva York, NY, W. W. Norton & Company, 2018, pp. 24 – 25. Los errores resultan inocuos en la realidad virtual, que proporciona el entorno necesario para entrenar a expertos cirujanos sin riesgo para el paciente. También es posible utilizarla en el ámbito de la rehabilitación, pues evita ejercicios tediosos y repetitivos.

música, optan por sumergirse mediante la tecnología en sonidos naturales relajantes como las olas del mar o la lluvia golpeando el tejado de una casa donde también se oye el crepitar del fuego. Esto es una evidente vía de escape de los agobios y la cacofonía del mundo moderno. A medida que la situación en el mundo real se ha ido degradando, estos espacios, aunque completamente falsos, son cada vez más solicitados, y las personas desean pasar en ellos cada vez más tiempo. ¿Por qué ahora? Porque hasta ahora no existía alternativa a la realidad y era necesario afrontar los problemas. Pero ahora, la tecnología ofrece una mentira cada vez más elaborada. Si realmente llega un momento en que la tecnología haga indistinguible la diferencia entre un mundo real hostil y enfermizo y una realidad virtual idílica, el problema de personas que preferirían "vivir" su vida en la segunda en detrimento del primero podría alcanzar niveles de gravedad parecidas a las de las epidemias de heroína españolas de los años ochenta, con la diferencia de que esta trajo secuelas principalmente físicas, mientras que el metaverso las traerá mentales (aumento de las esquizofrenias, incapacidad para distinguir la realidad de la ficción, y, derivado de lo anterior, aumento de la alegación de causas de atenuación de la responsabilidad criminal durante los procesos penales…)

Por todo esto, considero que lo más recomendable sería, mientras estemos a tiempo, limitar el uso de esta tecnología a través de su precio para cuestiones sanitarias al alcance de todos los pacientes pero exclusivamente en hospitales y centros sanitarios, y dándole un uso exclusivamente clínico, como en el mencionado caso de la IA y las operaciones quirúrgicas, tecnología que se usa para salvar vidas pero que permanece en manos de personas jurídicas que regulan su utilización y garantizan que sea la correcta.

Un sencillo ejemplo de la locura que ya está despertando el metaverso es la de aquellos autores que proponen la existencia de un ordenamiento jurídico (incluso jurídico-penal) para el mismo[770], diferenciado del CP aplicable a los hechos cometidos en la así llamada "vida real". ¿Cómo

[770] Aranda Serna, *Derecho y Nuevas Tecnologías*, p. 122.

afectaría al comportamiento en la realidad de las masas el hecho de que posiblemente se podrían llevar a cabo ciertas acciones típicas en el mismo, pero no fuera? No se trata ya de la guerra o de la violencia vistas como un juego, o de la pornografía más depravada, sino del verdadero acto de asesinar o de violar con un nivel de realismo indistinguible al de la realidad. ¿Cómo afectará esto a la mente de sus usuarios? ¿Podrá alegarse, algún día, la confusión entre estos dos mundos? ¿En qué patología, probablemente ya existente en el DSM-5, encajaría? En cualquier caso, si las únicas ventajas que puede ofrecer actualmente el metaverso en el ámbito sanitario son los beneficios para los profesionales sanitarios y su entrenamiento y los avances que llevaría aparejados en telemedicina (que podrían suplirse con otras tecnologías menos invasivas esta vez no para el cuerpo humano, pero sí para la vida de las personas), creo que el riesgo que supone para artículos del CP como el 197 y sucesivos es demasiado elevado, y requerirá una vigilancia muy atenta por parte de los especialistas en Derecho penal.

Considero, por todo lo anterior, que la misión del penalista en relación con estas nuevas tecnologías será la de permanecer vigilante en lo que se ha venido a llamar "la frontera digital"[771], que yo defino como el límite en constante expansión del alcance de los avances científico-tecnológicos. Cuando, tras invadir y recorrer progresivamente y con carácter previo otras áreas del Derecho en las cuales se regulen, choque con el límite propio del Derecho penal, será cuando debamos volver a desarrollar esta evaluación desde el principio: realización de un análisis lo más detallado posible de la

[771] S. Milivojevic, *Crime and Punishment in the Future Internet. Digital Frontier Technologies and Criminology in the Twenty-First Century*, 1ª ed., Oxfordshire, Routledge, 2021, pp. 119 - 136. Para Milivojevic, cuyas líneas de investigación se encuentran precisamente en la vanguardia de dicha frontera digital, las preocupaciones más acuciantes para el Derecho penal en relación con las nuevas tecnologías son las llamadas tecnologías de frontera, como el aprendizaje automático, el *blockchain*, la IA, el IdCM, el uso de macrodatos o la robótica y los drones. Avances tecnológicos, todos ellos, analizados desde la perspectiva de la ciberseguridad, el Derecho penal y la salud en este cuarto y último capítulo de esta investigación. Así, y habiendo abarcado desde la conceptualización de la ciberseguridad hasta sus modalidades más avanzadas, y siendo este el límite del desarrollo científico-tecnológico actual a juicio de los expertos más destacados, considero esta cita en particular el cierre idóneo para esta investigación.

nueva tecnología desde una perspectiva objetiva pero jurídicamente comprensible, encaje en un tipo delictivo ya existente o, en caso de no ser posible, desarrollo de una propuesta de *lege ferenda* preferentemente para la modificación o la creación de uno nuevo. Lo mismo en relación con las mejoras en ciberseguridad: seremos testigos de cómo los algoritmos podrán ayudar a resistir el empuje de la computación cuántica, y del nacimiento de estrategias para crear algoritmos a prueba de la misma que permita pervivir los criptosistemas clásicos. En este sentido, la existencia de un capítulo en el Código Penal dedicado al bien jurídico protegido ciberseguridad resultará esencial, así como la existencia de un tipo delictivo dedicado en exclusiva a la protección de esta barrera que será enriquecido en base a los desafíos que imponga (la elección de este verbo no es fortuita) el desarrollo científico-tecnológico.

CONCLUSIONES (CASTELLANO)

A partir de la investigación realizada, he llegado a las siguientes doce conclusiones:

I

La ciberseguridad se define como la seguridad física y lógica de las redes y sistemas informáticos que abarca tanto su *hardware* como su *software*, y cuyo objetivo es garantizar el mayor nivel de seguridad posible mediante la protección de la disponibilidad, la integridad y la confidencialidad tanto de estas como de los datos informáticos que contienen.

II

A excepción de detalles como la actual ubicación del artículo 197 bis 1 en el Título X del Código Penal, que protege principalmente la intimidad y los datos reservados de carácter personal y solo proporciona una protección secundaria y limitada a la ciberseguridad, el Derecho penal español se encuentra adecuadamente adaptado tanto a las exigencias del principal tratado de Derecho penal internacional en este ámbito (Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001) como de las normas de Derecho penal comunitario (Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión, o Directiva NIS, y Reglamento (UE) 2019/881 relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación).

III

A nivel internacional y comunitario, se pueden apreciar tres grandes categorías de regulación del delito de acceso ilícito a un sistema informático: primera, la regulación del delito en normas penales especiales (EE.UU., Reino Unido, Francia); segunda, la regulación del delito en un título o capítulo propio y diferenciado (Bélgica); y tercero, la regulación del delito junto a otros delitos ya existentes, vía elegida por la mayoría de países de nuestro entorno (Austria, Alemania y España, si bien, en este último caso, reitero mi crítica a la ubicación del artículo 197 bis 1 del Código Penal en su Título X, puesto que está dedicado principalmente a defender la intimidad y los datos reservados de carácter personal, mientras que otorga una defensa secundaria y limitada a la ciberseguridad como bien jurídico).

IV

Los aspectos del Derecho penal comparado relativos a la ciberseguridad susceptibles de ser tenidos en cuenta en el Derecho penal español son: primero, la iniciativa danesa de crear y financiar una unidad de ciberseguridad asignada a cada uno de los sectores críticos para la sociedad, como el sanitario, y que permite el desarrollo de una estrategia específica adaptada a sus vulnerabilidades; segunda, la decisión belga de dotar de autonomía a los delitos informáticos otorgándoles un título o capítulo propio y diferenciado, de tal manera que se pudiese tipificar con detalle el delito de acceso ilícito y proteger la ciberseguridad como bien jurídico protegido autónomo; tercero, la manera en que el Reino Unido tipifica en la actualidad el delito de acceso ilícito, sobre todo teniendo en cuenta la distinguida

posición que este país ocupa en las clasificaciones sobre ciberseguridad; cuarto, no incurrir en los mismos fallos que países como EE.UU o la Federación Rusa, que han cometido errores o en la ubicación o en la calidad de la tipificación del delito de acceso ilícito; quinto, siempre teniendo en cuenta el irrenunciable principio de legalidad, comprender que las nuevas tecnologías avanzan con rapidez y que la única manera de poder garantizar una adaptación eficaz del Derecho penal a las mismas es imbuir de algo de la versatilidad del sistema jurídico-penal anglosajón al español, sin que esto suponga la necesidad de apartarnos de nuestra tradición jurídica europea continental.

V

En el Código Penal resulta posible distinguir, dentro de la categoría más amplia de los ciberdelitos, delitos que afectan a la ciberseguridad, es decir, que lesionan de cualquier manera la seguridad de una red o sistema informáticos, afectando así a su disponibilidad, a su integridad o a su confidencialidad. El acceso no autorizado, considerado como elemento nuclear del tipo, tiende a ser solo un medio que permite al ciberdelincuente cometer un delito fin susceptible de lesionar bienes jurídicos distintos, motivo por el cual los delitos que afectan a la ciberseguridad se encuentran dispersos en el Código Penal, contándose entre los mismos desde artículos como el 197 (ubicado en el Título X, dedicado a la protección de la intimidad y de los datos reservados de carácter personal) hasta otros como el artículo 598 (cuya ubicación se encuentra en el Título XXIII, y que protege otra clase completamente distinta de información). Pese a su incorrecta ubicación actual, e incluso teniéndola en cuenta, el artículo 197 bis 1 constituye el paradigma de delito que afecta a la ciberseguridad, aunque se encuentra limitado por los bienes jurídicos protegidos en el Título X en el que se ubica

actualmente, a saber: la intimidad y los datos reservados de carácter personal.

VI

Además de la doctrina, una interpretación objetiva de los artículos 19, 27.1 y 28 de la Declaración Universal de los Derechos Humanos y de los artículos 17.1, 18.3 y 18.4 de la Constitución española de 1978, además del artículo 82 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales justifican que la ciberseguridad se convierta en un bien jurídico autónomo protegido por el Derecho penal español.

VII

Existe una necesidad político-criminal de criminalizar los accesos ilícitos a los sistemas de información. La función social esencial que la ciberseguridad desempeña, y la dependencia respecto de la misma sobre todo en ámbitos como el sanitario, hacen que necesite una protección adicional a la que puede proporcionarle el Derecho administrativo. Además, mediante la elevación de esta clase de comportamientos a la categoría de delito aumentaría el nivel de armonización de nuestra legislación penal tanto en lo concerniente al Derecho penal internacional y al Derecho penal comunitario como a las de otros Estados miembros de la Unión Europea, como Alemania. Estos accesos ilícitos están dotados, por último, de un importante efecto criminógeno, puesto que pueden tener graves repercusiones sobre distintos bienes jurídicos protegidos por los delitos fin que, en ocasiones, son el verdadero objetivo del ciberdelincuente que accede ilícitamente a un sistema de información.

VIII

Es necesaria la creación de un nuevo título en el Código Penal para los delitos contra la ciberseguridad que haga posible remediar el desorden estructural actual en relación con los mismos, solo donde corresponda. El delito de acceso ilícito a un sistema de información, actualmente el artículo 197 bis 1 ubicado en el Título X de dicho texto legal, constituiría, por sus características, el primero en ser trasladado al mismo. No obstante, en lo concerniente a los demás delitos que afectan a la ciberseguridad analizados, no procedería el traslado de todos ellos al nuevo título, sino que, dependiendo de sus características, se dividirían en tres categorías que determinarían la adecuación, o no, de este traslado: en primer lugar, los delitos cuya ubicación actual es adecuada, y cuyo traslado al nuevo título resulta innecesario (por ejemplo, ciertos párrafos relacionados con la ciberseguridad del delito de robo con fuerza en las cosas correspondiente al artículo 238 del Código Penal); en segundo lugar, los delitos cuya ubicación actual es inadecuada, y cuyo traslado al nuevo título resulta necesario (por ejemplo, el ya mencionado delito de acceso ilícito a un sistema de información recogido en el artículo 197 bis 1 del CP); y en tercer y último lugar, los delitos cuya ubicación actual es inadecuada, pero cuyo traslado al nuevo título no resulta necesaria porque lo que en realidad procede es su traslado a un título distinto no relacionado específicamente con la ciberseguridad (por ejemplo, la divulgación intencionada de una invención objeto de una solicitud de patente secreta tipificada en el artículo 277 del Código Penal, delito que, aunque mal ubicado en base a un criterio sistematizador erróneo, no puede considerarse relacionado con la ciberseguridad, y cuyo traslado a este nuevo título no procede).

IX

Actualmente, la ciberseguridad se ha visto desafiada en el ámbito sanitario por nuevas tecnologías como la inteligencia artificial, la robótica, los drones, los hospitales inteligentes, el Internet de las cosas médicas, la nube sanitaria o la salud electrónica, planteando cada una de ellas cuestiones muy complejas relacionadas con el Derecho penal. Resulta destacable el hecho de que la influencia de las nuevas tecnologías sobre la ciberseguridad y sobre el Derecho penal vaya a manifestarse de manera distinta a la esperada, toda vez que, previsiblemente, el primer delito en este ámbito no estará relacionado de manera directa con la seguridad de las mismas, como sucede con la contaminación de datos de los algoritmos, que es perseguible aplicando la legislación penal actualmente vigente, sino con aspectos exclusivamente jurídicos como el incumplimiento de las normas extrapenales relacionadas con las nuevas tecnologías por quien deba cumplirlas.

X

A la vista de las consecuencias tan variadas y, en ocasiones, tan lesivas a las que puede dar lugar la utilización de las nuevas tecnologías, sobre todo en aquellos casos en que se trata de la siempre intolerable tecnología invasiva del cuerpo humano, podemos sostener que no todos los avances tecnológicos deben ser aceptados *per se*. A partir de la premisa de que no todo el desarrollo científico-tecnológico es deseable ni inevitable, resulta esencial someter a un profundo análisis cada uno de ellos para determinar si merecen ser protegidos por el Derecho penal o si, por el contrario, son las personas las que deben ser protegidas mediante las herramientas legales jurídico-penales para garantizar su bienestar.

XI

El futuro de la ciberseguridad se construirá sobre la ciberbioseguridad, la computación cuántica y el metaverso: la primera, por hacer posible la fusión de la ciberseguridad física, la ciberseguridad lógica y la bioseguridad, permitiendo que un usuario encripte y desencripte un dispositivo mediante su ADN, blindando con ello una red o sistema informático; la segunda, por su capacidad para contrarrestar la seguridad de todo elemento no encriptado cuánticamente mediante la aplicación de complejos números y matrices; y el tercero, por tratarse de la evolución de Internet, una herramienta idónea para el entrenamiento del personal encargado de las tareas más complejas y que, sin embargo, plantea serias dudas de índole no solo legal, como la forma que deben adquirir las normas jurídico-penales por las que se regirá, o su enorme potencial para provocar adicciones.

XII

Ante los desafíos que impone el progresivo desarrollo científico y tecnológico, el especialista en Derecho penal que pretenda influir en la legislación que lo regule debe permanecer vigilante en la *frontera digital*, o el límite en constante expansión del alcance de los avances científico-tecnológicos para, ante la detección de una nueva tecnología susceptible de lesionar bienes jurídicos tradicionales o nuevos, analizarla con el mayor nivel de detalle posible no exclusivamente jurídico-penal sino también, en la línea de lo expuesto en la conclusión décima, mediante un análisis en profundidad de la propia tecnología; tratar de encajarla en un tipo delictivo ya existente y, en caso de no ser posible, desarrollar una propuesta de *lege ferenda*

orientada preferentemente a la modificación de la redacción del actual Código Penal y, solo en última instancia, a la creación de un nuevo delito.

CONCLUSIONS (ENGLISH)

On the basis of the research carried out, I have reached the following twelve conclusions:

I

Cybersecurity is defined as the physical and logical security of networks and information systems, encompassing both their hardware and software, which aims to ensure the highest possible level of security by protecting the availability, integrity and confidentiality not only of the systems but also the computer data they contain.

II

With the exception of details such as the current position of Article 197 bis 1 under Chapter X of the Spanish Criminal Code which mainly protects privacy and reserved personal data and only provides secondary and limited protection for cybersecurity, Spanish Criminal Law is adequately adapted not only to the requirements of the main international criminal law treaty in this field - the Convention on Cybercrime of 23 November 2001, Budapest - but also EU criminal law provisions including the Directive (EU) 2016/1148 on measures to ensure a high common level of security of networks and information systems within the Union; the NIS Directive; and Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification.

III

At international and EU level, three main categories regulating the criminal offence of unlawful access to a computer system can be identified: the first one regulates the criminal offence in special criminal regulations (the USA, the UK and France); the second category involves the regulation of the criminal offence in a separate and distinctive Chapter or Section (Belgium); and thirdly, the criminal offence is regulated together with other existing criminal offences, which is the route chosen by most of the countries in our environment (Austria, Germany and Spain; although, in the latter case, I reiterate my criticism of the position of Article 197 bis 1 of the Criminal Code under Chapter X, since it is mainly devoted to defending privacy and reserved personal data, while it grants secondary and limited defence to cybersecurity as a legally protected interest).

IV

The following aspects of comparative Criminal Law related to cybersecurity could be taken into account in Spanish criminal law: firstly, the Danish initiative to create and finance a cybersecurity unit assigned to each of the critical sectors for society, such as the health sector, and which allows the development of a specific strategy adapted to its vulnerabilities; secondly, the Belgian decision to give computer crimes autonomy by granting them a separate and distinct Chapter or Section, so that the criminal offence of unlawful access could be categorised in detail, and cybersecurity protected as an autonomous legally protected interest; thirdly, the way in which the UK currently categorises the criminal offence of unlawful access, particularly considering the UK's prominent position in cybersecurity crime classification;

fourthly, not to repeat the same mistakes as countries such as the USA or the Russian Federation, which have made mistakes regarding the position or categorisation quality to the criminal offence of illicit access; and in fifth place, always bearing in mind the inalienable principle of legality, understand that new technologies are advancing rapidly and the only way to guarantee an effective adaptation of Criminal Law to them is to imbue Spanish Law with some of the versatility of the Anglo-Saxon penal legal system, without implying the need to move away from our continental European legal tradition.

V

Within the broader category of cybercrimes, the Criminal Code allows the differentiation of criminal offences affecting cybersecurity, i.e., criminal offences that damage the security of a network or information system in any way, thus affecting its availability, integrity or confidentiality. Unauthorised access, envisaged as the core element of the criminal offence type, tends to be only a means that allows the cybercriminal to commit an end criminal offence that is likely to damage legally protected interests. For this reason, criminal offences affecting cybersecurity are scattered throughout the Criminal Code, ranging from articles such as Article 197 (located in Chapter X, dedicated to the protection of privacy and reserved personal data) to others such as Article 598 (located in Chapter XXIII, which protects a completely different kind of information). Despite its current incorrect position in the arrangement of headings, and even taking this into account, Article 197 bis 1 is the paradigm of a criminal offence affecting cybersecurity, although it is limited to the legal interests protected under Chapter X where it is currently located, i.e.: privacy and reserved personal data.

VI

In addition to the legal doctrine, an objective interpretation of Articles 19, 27.1 and 28 of the Universal Declaration of Human Rights and Articles 17.1,18.3 and 18.4 of the Spanish Constitution of 1978, in addition to Article 82 of the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights, justifies that cybersecurity shall become an independent legal interest protected by Spanish Criminal Law.

VII

There is a political-criminal need to criminalise unlawful access to computer systems. The essential social role that cybersecurity plays and the dependence on it especially in areas such as the health sector, mean that additional protection compared to the protection which can be provided by Administrative Law, is needed. Furthermore, elevating this type of behaviour to the status of a criminal offence would increase the level of harmonisation of our criminal legislation both with regard to International Criminal Law and EU Criminal Law, as well as with legislation of other Member States of the European Union, such as Germany. Finally, the aforementioned unlawful accesses cause a major criminogenic impact, as they can have serious repercussions on various interests endangered by the end criminal offences, which are sometimes the real target of the cybercriminal who unlawfully accesses an information system.

VIII

There is a need to create a new Chapter in the Criminal Code for cybersecurity criminal offences that would make it possible to remedy the current structural disarrangement in relation to cybersecurity criminal offences, only where appropriate. The criminal offence of unlawful access to an information system, currently Article 197 bis 1 located in Chapter X of the aforementioned legal text, would, due to its characteristics, be the first to be transferred to it. Nevertheless, with regard to the other criminal offences affecting cybersecurity analysed, it would not be appropriate to transfer all of them to the new Chapter, but rather, depending on their characteristics, they should be divided into three categories that would determine the appropriateness or otherwise, of such transfer: (i) criminal offences which are currently in the suitable position in the arrangement of headings and whose transfer to the new Chapter is unnecessary (e.g., certain cybersecurity-related paragraphs of the criminal offence of burglary under Article 238 of the Criminal Code); (ii) criminal offences which are currently in an unsuitable position in the arrangement of headings, and whose transfer to the new Chapter is necessary (e.g., the aforementioned criminal offence of unlawful access to an information system under Article 197 bis 1 of the Criminal Code); and finally, (iii) criminal offences which are currently in an unsuitable position in the arrangement of headings and whose transfer to the new Chapter is unnecessary because what would be really appropriate is their transfer to a different Chapter not specifically related to cybersecurity (e.g., intentional disclosure of an invention that is the subject of a secret patent application under Article 277 of the Criminal Code; an criminal offence which, although misplaced on the basis of an erroneous systematising criterion, cannot be considered related to cybersecurity, and whose transfer to this new Chapter is not appropriate).

IX

Currently, cybersecurity has been challenged in the healthcare sector by new technologies such as Artificial Intelligence, robotics, drones, smart hospitals, the Internet of Medical Things (IoMT), the healthcare cloud or e-health, and each of them raises very complex issues regarding Criminal Law. It is worth highlighting that the influence of new technologies on cybersecurity and Criminal Law may materialise differently than expected, given that the first crime in this field will not be directly linked with their security, as in the case of data contamination in algorithms, which can be prosecuted under current criminal law, but rather to exclusively legal aspects such as breaching regulations outside the scope of criminal law related to new technologies by those who are bound to comply with them.

X

In view of the wide-ranging and sometimes very harmful consequences that may result from the use of new technology, particularly in those cases involving the always intolerable invasive technology for the human body, we can argue that not all technological breakthroughs should be accepted *per se*. Based on the premise that not all scientific-technological breakthroughs are desirable or inevitable, it becomes essential to subject each development to an in-depth analysis to determine whether they deserve to be protected by Criminal Law or on the contrary, it is people who should be protected by means of the legal tools of criminal legal systems to guarantee their wellbeing.

XI

The future of cybersecurity will be built on cyberbiosecurity, quantum computing and the Metaverse: the first, as it facilitates the fusion of physical

cybersecurity, logical cybersecurity and biosecurity, allowing a user to encrypt and decrypt a device through its DNA, thereby shielding a network or computer system; the second, by its capacity to counter the security of any non-quantum encrypted element through the application of complex numbers and matrices; and the third, because it is the evolution of the Internet, an ideal tool for the training of personnel in charge of the most complex tasks, and which nonetheless raises serious doubts not only of a legal nature, such as the form which legal-criminal rules governing it should take, but also its huge potential to cause addiction.

XII

Considering the challenges imposed by progressive scientific and technological progress, any Criminal Law specialist who intends to influence the legislation governing such breakthrough, must remain vigilant on the *digital frontier*, or the constantly expanding scope of scientific-technological developments, so that when a new technology likely to damage traditional or new legally protected interests is identified, it can be analysed with the highest possible level of detail not exclusively in terms of criminal law but also along the lines of that set out in the tenth conclusion, through an in-depth analysis of the technology itself; attempting to fit it into an existing criminal offence type and if this is not possible, developing a *lege ferenda* proposal preferably aimed at amending the wording of the current Criminal Code and only as a last resort, creating a new offence.

BIBLIOGRAFÍA

Abad Quintanal, G., “El concepto de seguridad: su transformación”, *Comillas Journal of International Relations,* no. 4, 2015, pp. 41 – 51.

Abadías Selma, A., Fernández Albesa, N., y Leal Ruiz, R., *Ciberdelincuencia. Temas prácticos para su estudio*, 1ª ed., A Coruña, Colex, 2021.

Aboso, G.E., “Delitos contra la intimidad y la privacidad: acceso indebido a comunicaciones electrónicas, datos sensibles y sistemas informáticos”, *Revista de Derecho Penal y Criminología,* no. 7, 2017, pp. 3 – 31.

Adler, J.R., “Remote Robotic Spine Surgery”, *Neurospine*, vol. 17, no. 1, 2020, pp. 121 – 122.

Agencia de la Unión Europea para la Ciberseguridad, *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence,* Atenas, Agencia de la Unión Europea para la Ciberseguridad, 2020.

Agencia de la Unión Europea para la Ciberseguridad, *Foresight Challenges: A study to enable foresight on emerging and future cybersecurity Challenges,* Atenas, Agencia de la Unión Europea para la Ciberseguridad, 2021.

Alastuey Dobón, C., “Delitos contra el patrimonio y contra el orden socioeconómico I. Hurtos. Robos. Extorsión. Robo y hurto de uso de vehículos. Usurpación”, en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho Penal, Parte Especial*, 2ª ed., Granada, Comares, 2022, pp. 343 – 372.

Alcoceba Gil, J.M., “Contraterrorismo en el siglo XXI: de *seguridad* a *defensa*”, en V. Moreno Catena y A. Arnáiz Serrano (dirs.), *El estado de derecho a prueba: seguridad, libertad y terrorismo*, 1ª ed., Valencia, Tirant lo Blanch, 2017, pp. 119 – 150.

Alfonseca, M. et al., “Superintelligence Cannot be Contained: Lessons from Computability Theory”, *Journal of Artificial Intelligence Research,* vol. 70, 2021, pp. 65 – 76.

Almenar Pineda, F., *Ciberdelincuencia. Teoría y práctica*, 1ª ed., Porto, Juruá Editorial, 2018.

Almenar Pineda, F., *El delito de hacking,* 1ª ed., Cizur Menor, Navarra, Aranzadi, 2018.

Alonso Lecuit, J., “Relanzamiento del Plan de Ciberseguridad de la UE”, *Análisis del Real Instituto Elcano (ARI),* no. 97, 2017, pp. 1 – 9.

Alonso Lecuit, J., “Drones, seguridad y ciberseguridad”, en M. Barrio Andrés (dir.), *Derecho de los drones*, 1ª ed., Madrid, Wolters Kluwer, 2018, pp. 349 – 388.

Álvarez de Neyra Kappler, S., “Doctrina del Tribunal Supremo con relación a la protección de la relación de confidencialidad abogado-cliente”, en L. Bachmaier Winter (coord.), *Investigación penal, secreto profesional del abogado, empresa, y nuevas tecnologías: retos y soluciones jurisprudenciales,* 1ª ed., Cizur Menor, Navarra, 2022, pp. 171 – 242.

Álvarez Rodríguez, I., “Constitución y Derecho del Ciberespacio”, en C. Mallada Fernández (dir.), *Nuevos Retos de la Ciberseguridad en un Contexto Cambiante*, Cizur Menor, Navarra, Aranzadi, 2019, pp. 21 – 46.

Amoroso, R.L., “Imminent Advent of Universal Quantum Computing (UQC)”, en L.M. Caligiuri (edit.), *Frontiers in Quantum Computing*, Hauppauge, NY, Nova Science Publishers, 2020, pp. 269 – 330.

Andrés Domínguez, A.C., “Artículo 346”, en M. Gómez Tomillo (dir.), *Comentarios prácticos al Código Penal. Tomo IV. Delitos contra el medio ambiente, el patrimonio histórico, la ordenación del territorio y contra la seguridad colectiva. Artículos 319 – 385 ter*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, pp. 241 – 246.

Andrés Segovia, B., *La convergencia de las telecomunicaciones, los medios de comunicación y las tecnologías de la información*, 1ª ed., Navarra, Aranzadi, 2020.

Antón Oneca, J., *Obras. Tomo I,* 1ª ed., Santa Fe, Rubinzal – Culzoni, 2000.

Antón Oneca, J., *Obras. Tomo II*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2002.

Antón Oneca, J., *Obras. Tomo III*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2003.

Aranda Serna, F.J., *Derecho y Nuevas Tecnologías. La influencia de Internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español*, 1ª ed., Madrid, Dykinson, 2021.

Arroyo Guardeño, D., Gayoso Martínez, V., y Hernández Encinas, L., *Ciberseguridad*, 1ª ed., Madrid, CSIC – Catarata, 2020.

Ashley, K.D., "Introduction: Cybersecurity in Pittsburgh", *Pittsburgh Journal of Technology Law and Policy,* vol. 14, no. 2, 2014, pp. 273 – 275.

Ávila-Tomás, J.F., Mayer-Pujadas, M.A., y Quesada-Varela, V.J., "La Inteligencia artificial y sus aplicaciones en medicina (I): Introducción. Antecedentes a la IA y robótica", *Atención Primaria: Publicación Oficial de la Sociedad Española de Medicina de Familia y Comunitaria*, vol. 52, no. 10*,* 2020, pp. 778 – 784.

Ávila-Tomás, J.F., Mayer-Pujadas, M.A., y Quesada-Varela, V.J., "La Inteligencia artificial y sus aplicaciones en medicina (II): Importancia actual y aplicaciones prácticas", *Atención Primaria: Publicación Oficial de la Sociedad Española de Medicina de Familia y Comunitaria*, vol. 53, no. 1, 2020, pp. 81 – 88.

Avilés Farré, J., "Por un concepto amplio de seguridad", en Ministerio de Defensa – Instituto Español de Estudios Estratégicos (eds.), *Revisión de la Defensa Nacional,* 1ª ed., Madrid, Ministerio de Defensa – Instituto Español de Estudios Estratégicos, 2002, pp. 17 – 44.

Ayala, L., *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention,* 1ª ed., Nueva York, NY, Apress Media LLC, 2016.

Ayala, L., *Cybersecurity Lexicon*, 1ª ed., Nueva York, NY, Apress Media LLC, 2016.

Azcona Albarrán, C.D., *Tarjetas de pago y Derecho penal. Un modelo interpretativo del art. 248.2.c) CP*, 1ª ed., Barcelona, Atelier, 2012.

Bachman, R.D. y Schutt, R.K., *The Practice of Research in Criminology and Criminal Justice,* 7ª ed., Thousand Oaks, CA, SAGE Publications, 2020.

Bailenson, J., *Experience on Demand: What Virtual Reality Is, How It Works, and What It Can Do*, 1ª ed., Nueva York, NY, W. W. Norton & Company, 2018.

Bainbridge, D.I., "Hacking. The Unauthorised Access of Computer Systems. The Legal Implications", *The Modern Law Review*, vol. 52, no. 2, 1989, pp. 236 – 245.

Bajo Fernández, M., *Los delitos de estafa en el Código Penal,* 1ª ed., Madrid, Editorial Universitaria Ramón Areces, 2004.

Baldwin, D.A., "The concept of security", *Review of International* Studies, no. 23, 1997, pp. 5 – 26.

Ball, M., *The Metaverse: And How It Will Revolutionize Everything*, 1ª ed., Nueva York, NY, Liveright Publishing Corporation, 2022.

Barbero Bajo, J., "*Phishing* y otros delitos informáticos: el uso ilícito de Internet", *Lex nova: La revista,* no. 53, 2008, pp. 6 – 10.

Barja de Quiroga López, J., Encinar del Pozo, M.A., y Villegas García, M.ª A., *Código Penal. Comentado, con jurisprudencia sistematizada y concordancias,* 8ª ed., Madrid, Francis Lefebvre, 2021.

Barja de Quiroga López, J. et al., *Ley de Enjuiciamiento Criminal. Comentada, con jurisprudencia sistematizada y concordancias,* 8ª ed., Madrid, Francis Lefebvre, 2021.

Barrio Andrés, M., *Ciberdelitos: amenazas criminales del ciberespacio*, 1ª ed., Madrid, Reus, 2017.

Barrio Andrés, M., *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet,* 1ª ed., Valencia, Tirant lo Blanch, 2018.

Barrio Andrés, M., *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos,* 1ª ed., Madrid, Wolters Kluwer, 2018.

Barrio Andrés, M., *Internet de las cosas,* 1ª ed*.,* Madrid, Reus, 2018.

Barrio Andrés, M., *Manual de Derecho Digital,* 1ª ed., Valencia, Tirant lo Blanch, 2020.

Baumard, P., *Cybersecurity in France*, 1ª ed., Cham, Springer, 2017.

Begishev, I.R., Khisamova, Z.I., y Mazitova, G.I., "Criminal legal ensuring of security of critical information infrastructure of the Russian Federation", *Revista Gênero & Direito,* vol. 8, no. 6, 2019, pp. 283 – 292.

Begishev, I.R., Khisamova, Z.I., y Nikitin, S.G., "The organization of hacking community: Criminological and criminal law aspects", *Russian Journal of Criminology,* vol. 14, no. 1, 2020, pp. 96 – 105.

Bell, J. et al., "Balancing Data Subjects' Rights and Public Interest Research: Examining the Interplay between UK Law, EU Human Rights Law and the GDPR", *European Data Protection Law Review,* vol. 5, no. 1, 2019, pp. 43 – 53.

Benetó Santa Cruz, A. y Cachón Marinello, L., "La creciente importancia de proteger los secretos comerciales", en J. Velázquez (coord.), *Cuadernos de*

Derecho para ingenieros: ciberseguridad, Las Rozas, Madrid, Wolters Kluwer, 2017, pp. 229 – 250.

Benke, K. y Benke, G., "Artificial Intelligence and Big Data in Public Health", *International Journal of Environmental Research and Public Health,* vol. 15, no. 12, 2018, pp. 1 – 9.

Bermejo García, R. y López-Jacoiste Díaz, E., *La ciberseguridad a la luz del Jus ad Bellum y del Jus in Bello,* 1ª ed., Pamplona, Ediciones Universidad de Navarra, 2020.

Blanco Cordero, I., "Homo sapiens y ¿machina sapiens?. Un Derecho Penal para los robots dotados de inteligencia artificial", en C. Mallada Fernández (dir.), *Nuevos Retos de la Ciberseguridad en un Contexto Cambiante*, Cizur Menor, Navarra, Aranzadi, 2019, pp. 63 – 80.

Blokland, P.J. y Reniers, G.L., "The Concepts of Risk, Safety and Security: A Fundamental Exploration and Understanding of Similarities and Differences", en C. Bieder y K. Pettersen Gould (eds.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice,* 1ª ed., Cham, Springer, 2020, pp. 9 – 16.

Boldova Pasamar, M.A., "Penas privativas de libertad", en L. Gracia Martín (coord.), *Tratado de las consecuencias jurídicas del delito*, 1ª ed., Valencia, Tirant lo Blanch, 2005, pp. 91 – 122.

Boldova Pasamar, M.A., "Los principios del derecho penal", en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho penal, Parte General. Introducción y teoría jurídica del delito,* Granada, Comares, 2016, pp. 37 – 54.

Bolea Bardón, C., "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en M. Corcoy Bidasolo y S. Mir Puig (dirs.), *Comentarios al Código Penal. Reforma LO 1/2015 y LO 2/2015*, 1ª ed., Valencia, Tirant lo Blanch, 2015, pp. 729 – 762.

Borrajo Valiña, D., “La integración en la seguridad y defensa de la UE: las iniciativas post-Brexit y la futura articulación de la cooperación con el Reino Unido”, *Revista Aranzadi Unión Europea*, no. 4, 2019, pp. 71 – 94.

Brebner, J., “*Breen v. Williams:* A lost opportunity or a welcome conservatism?”, *Deakin Law Review,* vol. 3, no. 2, 1996, pp. 237 – 249.

Brenner, S.W., “Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law”, *Murdoch University Electronic Journal of Law,* vol. 8, no. 2, 2001.

Briera Dalmau, C., “La ciberseguridad: consideraciones y apuntes sobre el régimen jurídico aplicable a la seguridad de las redes y sistemas de la información”, en J. Velázquez (coord.), *Cuadernos de Derecho para ingenieros: ciberseguridad,* Las Rozas, Madrid, Wolters Kluwer, 2017, pp. 265 – 286.

Broadhurst, R., “Cybercrime in Australia”, en A. Deckert y R. Sarre (eds.), *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice*, Londres, Palgrave Macmillan, 2017, pp. 221 – 235.

Brumley, D., “The White-Hat Hacking Machine: Meet Mayhem, winner of the DARPA contest to find and repair software vulnerabilities”, *IEEE Spectrum*, vol. 56, no. 2, 2019, pp. 30 – 35.

Buchanan, B., *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations,* 1ª ed., New York, NY, Oxford University Press, 2016.

Bueno De Mata, F., “Análisis de las medidas de cooperación judicial internacional para la obtención transfronteriza de pruebas en materia de cibercrimen”, en L. Fontestad Portalés (dir.), *La transformación digital de la cooperación jurídica penal internacional*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021, pp. 19 – 48.

Burton, J., “Small states and cyber security: The case of New Zealand”, *Political Science,* vol. 65, no. 2, 2013, pp. 216 – 238.

Caballero Velasco, M.A. y Cilleros Serrano, D., *Ciberseguridad y transformación digital: Cloud, Identidad Digital, Blockchain, Agile, Inteligencia Artificial*, 1ª ed., Madrid, Anaya Multimedia, 2020.

Calle Rodríguez, M.V., "El delito de estafa informática", *La ley penal: revista de derecho penal, procesal y penitenciario,* no. 37, 2007, pp. 40 – 56.

Cámara Arroyo, S. et al., *Cibercriminalidad*, 1ª ed., Madrid, Dykinson, 2019.

Cancio Meliá, M., *Los delitos de terrorismo: estructura típica e injusto*, 1ª ed., Madrid, Editorial Reus, 2010.

Cardona Pastor, J.M., y Cuñat Ferrando, J.S., *Guía Rápida Ciberseguridad para Despachos y Profesionales*, 1ª ed., Madrid, Francis Lefebvre, 2018.

Carlini, A., "Ciberseguridad: un nuevo desafío para la comunidad internacional", *Bie3: Boletín IEEE,* no. 2, 2016, pp. 950 – 966.

Carnevali Rodríguez, R., "Derecho penal como *ultima ratio*. Hacia una política criminal racional", *Ius et Praxis,* vol. 14, no. 1, 2008, pp. 13 – 48.

Carrasco Andrino, M.D.M. y Moya Fuentes, M.D.M., "La ciberdelincuencia dentro de la estrategia de seguridad nacional. Especial referencia a las conductas de introducción en el sistema informático", en J.M. Canales Aliende y A. Romero Tarín (eds.), *La seguridad de los Estados en el contexto de las incertidumbres: una visión poliédrica*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021, pp. 281 – 308.

Carter, D.J. y Hartridge, S., "Mandatory data breach notification requirements for medical practice", *The Medical Journal of Australia,* vol. 209, no. 5, 2018, pp. 204 – 205.

Cartwright, E., Hernández de Castro, J., y Cartwright, A., "To pay or not: game theoretic models of ransomware", *Journal of Cybersecurity*, vol. 5, no. 1, 2019, pp. 1 – 12.

Castells, M., *La Galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*, 1ª ed., Madrid, Areté, 2001.

Castiñeira Palou, M.ª T. y Estrada i Cuadras, A., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en J.M. Silva Sánchez (dir.), *Lecciones de Derecho Penal, Parte Especial*, 7ª ed., Barcelona, Atelier, 2021, pp. 157 – 182.

Cate, F.H. y Cate, B.E., "The Supreme Court and information privacy", *International Data Privacy Law,* vol. 2, no. 4, 2012, pp. 255 – 267.

Cavelty, M.D., *Cybersecurity in Switzerland,* 1ª ed., Cham, Springer, 2014.

Cerezo Mir, J., "El delito como acción culpable", *Anuario de derecho penal y ciencias penales*, vol. 49, no. 1, 1996, pp. 9 – 42.

Cerezo Mir, J., *Curso de Derecho Penal español. Parte General. Tomo II. Teoría Jurídica del Delito*, 6ª ed., Madrid, Tecnos, 2000.

Cerezo Mir, J., *Temas fundamentales del Derecho Penal. Tomo I*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2001.

Cerezo Mir, J., *Curso de Derecho Penal español. Parte General. Tomo III. Teoría Jurídica del Delito II*, 1ª ed., Madrid, Tecnos, 2002.

Cerezo Mir, J., *Temas fundamentales del Derecho Penal. Tomo II*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2002.

Cerezo Mir, J., *Curso de Derecho Penal español. Parte General. Tomo I. Introducción*, 6ª ed., Madrid, Tecnos, 2005.

Cerezo Mir, J., *Temas fundamentales del Derecho Penal. Tomo III*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2006.

Chace, C., *Surviving AI: The promise and peril of artificial intelligence,* 3ª ed, Three Cs, 2020.

Chelala Riva, R., “La nueva delincuencia cibernética”, en J. Andújar Urrutia y J.A. Tuero Sánchez (coords.), *Actualidad Penal 2017,* Valencia, Tirant lo Blanch, 2017, pp. 321 – 342.

Choclán Montalvo, J.A., *El delito de estafa*, 2ª ed., Barcelona*,* Bosch, 2009.

Christiansen, A., “Rationality, Expected Utility Theory and the Precautionary Principle”, *Ethics, Policy & Environment,* vol. 22, no, 1, 2019, pp. 3 – 20.

Christou, G., *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, 1ª ed., Londres, Palgrave Macmillan, 2016.

Christou, G., “The challenges of cybercrime governance in the European Union”, *European Politics and Society,* vol. 19, no. 3, 2018, pp. 355 – 375.

Christou, G., “The collective securitisation of cyberspace in the European Union”, *West European Politics,* vol. 42, no. 2, 2019, pp. 278 – 301.

Cimino, J.J. et al., “The Future of Informatics in Biomedicine”, en E.H. Shortliffe y J.J. Cimino (eds.), *Biomedical Informatics*, 5ª ed., Cham, Springer, 2021, pp. 987 – 1016.

Clark, R. et al., *The impact of quantum technologies on secure communications*, Canberra, ACT, Australian Strategic Policy Institute, 2021.

Clough, J., “The Council of Europe Convention on Cybercrime: Defining Crime in a Digital World”, *Criminal Law Forum,* vol. 23, 2012, pp. 363 – 391.

Clough, J., “A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation”, *Monash University Law Review,* vol. 40, no. 3, 2014, pp. 698 – 736.

Coles-Kemp, L., Ashenden, D., y O´Hara, K., “Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen”, *Politics and Governance,* vol. 6, no. 2, 2018, pp. 41 – 48.

Comisión Europea, *Scientific Opinion no. 2/2017: Cybersecurity in the European Digital Single Market,* Bruselas, Comisión Europea, 2017.

Conde-Pumpido Ferreiro, C., *Estafas*, 1ª ed., Valencia, Tirant lo Blanch, 1997.

Conde-Pumpido Tourón, C., "El derecho penal como última ratio: principio de intervención mínima", *Estudios de derecho judicial,* no. 48, 2003, pp. 45 – 76.

Connolly, L.Y. y Wall, D.S., "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures", *Computers & Security,* vol. 87, 2019, pp. 1 – 18.

Consejo de Europa, *Informe explicativo del Convenio sobre la Ciberdelincuencia de Budapest*, Estrasburgo, Consejo de Europa, 2001.

Consejo de Europa, *Organised crime in Europe: the threat of cybercrime,* Estrasburgo, Consejo de Europa, 2005.

Consejo de Europa, *Artificial Intelligence and Data Protection*, Estrasburgo, Consejo de Europa, 2019.

Contreras, J.L., DeNardis, L., y Teplinsky, M., "Mapping Today's Cybersecurity Landscape", *The American University Law Review,* vol. 62, no. 5, 2013, pp. 1113 – 1130.

Coravos, A. et al., "Digital Medicine: A Primer on Measurement", *Digital Biomarkers,* vol. 3, no. 2, 2019, pp. 31 – 71.

Cortés Bechiarelli, E., "Sobre la pluriofensividad de los delitos cometidos por los funcionarios públicos contra las garantías de la intimidad (artículos 534 a 536 del Código penal español)", en F. Muñoz Conde et al. (dirs.), *Un Derecho penal comprometido,* 1ª ed., Valencia, Tirant lo Blanch, 2011, pp. 221 – 238.

Cortina, A., "Fundamentos filosóficos del principio de precaución", en C.M. Romeo Casabona (edit.), *Principio de precaución, Biotecnología y Derecho*, Granada, Comares, 2004, pp. 3 – 16.

Craigen, D., Diakun – Thibault, N. y Purse, R., “Defining Cybersecurity”, *Technology Innovation Management Review,* vol. 4, no. 10, 2014, pp. 13 – 21.

Creese, S., “The threat from AI”, en D.J. Baker y P.H. Robinson (eds.), *Artificial Intelligence and the Law. Cybercrime and Criminal Liability*, 1ª ed., Oxfordshire, Routledge, 2021, pp. 201 – 221.

Cuello Contreras, J., “Acción, capacidad de acción y dolo eventual”, *Anuario de derecho penal y ciencias penales*, vol. 36, no. 1, 1983, pp. 77 – 99.

Cuello Contreras, J., *El derecho penal español. Parte general. Volumen II. Teoría del delito (2)*, 1ª ed., Madrid, Dykinson, 2009.

Daucé, F. et al., “From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia”, *Laboratorium: Russian Review of Social Research,* vol. 11, no. 3, 2019, pp. 46 – 70.

Daunis Rodríguez, A., *La graduación de la imprudencia punible*, 1ª ed., Navarra, Aranzadi, 2020.

Davara Fernández de Marcos, E. y Davara Fernández de Marcos, L., *Delitos informáticos,* 1ª ed., Cizur Menor, Navarra, Aranzadi, 2017.

De Hert, P. y Papakonstantinou, V., “The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area”, *Brussels Privacy Hub Working Paper Series,* vol. 1, no. 1, 2014, pp. 1 – 37.

De la Calle, M.J., “IA: Problema y solución de la Ciberseguridad”*, Contact Center Call Center & IP Solutions,* no. 87, 2017, pp. 32 – 35.

De la Cuesta Arzamendi, J.L. y San Juan Guillén, C., “La cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad”, en J.L. De la Cuesta Arzamendi (dir.), *Derecho Penal Informático*, Cizur Menor, Navarra, Aranzadi, 2010*,* pp. 57 – 78.

De la Cuesta Arzamendi, J.L., “El proceso de integración penal europea”, en J.L. De la Cuesta Arzamendi (dir.), *Adaptación del derecho penal español a la política criminal de la Unión Europea,* Cizur Menor, Navarra, Aranzadi, 2017, pp. 27 – 46.

De la Mata Barranco, N.J., *El principio de proporcionalidad penal*, 1ª ed., Valencia, Tirant lo Blanch, 2007.

De la Mata Barranco, N.J., “Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general”, en J.I. Echano Basaldua (dir.), *Cuadernos penales José María Lidón, no. 4. Delito e informática: algunos* aspectos, 1ª ed., Bilbao, Publicaciones de la Universidad de Deusto, 2007, pp. 41 – 84.

De la Mata Barranco, N.J., *La individualización de la Pena en los Tribunales de Justicia. La atención a la finalidad de la pena, la gravedad del hecho y las circunstancias personales del procesado en la Jurisdicción Penal, en su vinculación a la exigencia de imposición de penas proporcionadas*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2008.

De la Mata Barranco, N.J., *Derecho penal europeo y legislación española: las reformas del Código Penal*, 1ª ed., Valencia, Tirant lo Blanch, 2015.

De la Mata Barranco, N.J., “Delitos informáticos (contra sistemas y datos)”, en J.L. De la Cuesta Arzamendi (dir.), *Adaptación del derecho penal español a la política criminal de la Unión Europea,* Cizur Menor, Navarra, Aranzadi, 2017, pp. 221 – 243.

De la Mata Barranco, N.J., “La influencia del Derecho de la Unión Europea en el Derecho penal de sus estados miembros”, en J.L. De la Cuesta Arzamendi (dir.), *Adaptación del derecho penal español a la política criminal de la Unión Europea,* Cizur Menor, Navarra, Aranzadi, 2017, pp. 105 – 142.

De la Mata Barranco, N.J., “Delitos contra la propiedad intelectual e industrial y violación de secretos de empresa”, en N.J. De la Mata Barranco et al.

(autores), *Derecho penal económico y de la empresa,* Madrid, Dykinson, 2018, pp. 327 – 366.

De la Mata Barranco, N.J. y Hernández Díaz, L., "El delito de daños informáticos: una tipificación defectuosa", *Estudios penales y criminológicos,* no. 29, 2009, pp. 311 – 362.

De la Mata Barranco, N.J. y Pérez Machío, A.I., "La normativa internacional para la lucha contra la cibercriminalidad como referente de la regulación penal española", en J.L. De la Cuesta Arzamendi (dir.), *Derecho Penal Informático*, Cizur Menor, Navarra, Aranzadi, 2010*,* pp. 123 – 145.

De León Villalba, F.J., "Condicionantes, normativos y extra normativos, del ilícito militar", en F.J. De León Villalba (dir.), *Derecho penal militar. Cuestiones fundamentales*, 1ª ed., Valencia, Tirant lo Blanch, 2014, pp. 17 – 70.

De Marcos Madruga, F., "Artículo 35", en M. Gómez Tomillo (dir.), *Comentarios prácticos al Código Penal. Tomo I. Parte General. Artículos 1 – 137*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, pp. 501 – 506.

De Miguel Beriain, I., "Delitos de traición y contra la paz o la independencia del Estado, y relativos a la defensa nacional", en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho Penal, Parte Especial*, 2ª ed., Granada, Comares, 2022, pp. 865 – 878.

Dedeke, A. y Masterson, K., "Contrasting cybersecurity implementation frameworks (CIF) from three countries", *Information and Computer Security,* vol. 27, no. 3, 2019, pp. 373 – 392.

Deibert, R.J., "Toward a Human-Centric Approach to Cybersecurity", *Ethics & International Affairs,* vol. 32, no. 4, 2018, pp. 411 – 424.

Del Canto Masa, C.J., "Ciberseguridad, una cuestión prioritaria", *Cuadernos de energía,* no. 56, 2018, pp. 48 – 56.

Delgado Gil, A., “El delito de revelación de secretos de estado en los artículos 598 CP común y 53 CP militar: reflexiones sobre sus diferencias”, *Revista electrónica de ciencia penal y criminología,* no. 7, 2005, pp. 1 – 19.

Delgado Gil, A., *Delitos cometidos por funcionarios públicos. Negociaciones prohibidas, actividades incompatibles y uso indebido de secreto o información privilegiada*, Valencia, Tirant lo Blanch, 2008.

Delgado Gil, A., “La responsabilidad del militar por el delito de revelación de secretos e informaciones relativas a la seguridad y defensa nacionales (comentario a la STS, Sala de lo Militar, de 16 de marzo de 2017), *CEFLegal: revista práctica de derecho. Comentarios y casos prácticos,* no. 203, 2017.

Delgado Gil, A., “El delito de descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional (por el depositario o conocedor), *Cuadernos de política criminal*, no. 125, 2018, pp. 45 – 70.

Dennis, C.M. y Goldman, D.A., “Data Security Laws and the Cybersecurity Debate”, *Journal of Internet Law,* vol. 17, no. 2, 2013, pp. 1 – 11.

Department of the Prime Minister and Cabinet, *New Zealand's cyber security strategy 2019,* Wellington, Department of the Prime Minister and Cabinet, 2019.

Díaz Alabart, S., *Robots y responsabilidad civil,* 1ª ed., Madrid, Reus, 2018.

Díaz Gómez, A., “El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest”, *Revista electrónica del Departamento de Derecho de la Universidad de la Rioja* (*REDUR)*, no. 8*,* 2010, pp. 169 – 203.

Díez Ripollés, J.L., *Política criminal y derecho penal -Estudios-*, 2ª ed., Valencia, Tirant lo Blanch, 2013.

Díez Ripollés, J.L., *Delitos y penas en España*, 1º ed., Madrid, Catarata, 2015.

Dimmroth, K. y Schünemann, W.J., “The Ambiguous Relation Between Privacy and Security in German Cyber Politics: A Discourse Analysis of Governmental and Parliamentary Debates”, en W.J. Schünemann y M. Baumann (eds.), *Privacy, Data Protection and Cybersecurity in Europe,* Cham, Springer, 2017, pp. 97 – 112.

Dobrinoiu, M., “Opinions on the Unconstitutionality Aspects Related to the Cybersecurity Law”, *Challenges of the Knowledge Society,* vol. 5, no. 1, 2015, pp. 28 – 32.

Domínguez Peco, E.M., “Los robots en el Derecho penal”, en M. Barrio Andrés (dir.), *Derecho de los Robots*, 2ª ed., Madrid, Wolters Kluwer, 2019, pp. 169 – 188.

Donaire Villa, F.J., “La nueva regulación sobre ciberseguridad de redes y sistemas de información en España: preguntas y respuestas sobre el Real Decreto-ley 12/2018, de transposición de la Directiva NIS”, *Revista de privacidad y derecho digital,* vol. 4, no. 14, 2019, pp. 123 – 165.

Doval País, A., “La intimidad y los secretos de empresa como objetos de ataque por medios informáticos”, *Eguzkilore*, no. 22, 2008, pp. 89 – 115.

Drăgan, A.T., “Illegal Access to a Computer System from the Standpoint of the Current Criminal Code”, *Journal of Legal Studies,* vol. 23, no. 37, 2019, pp. 33 – 43.

Edgar, T.W. y Manz, D.O., *Research Methods for Cyber Security,* Cambridge, Elsevier, 2017.

Emergency Care Research Institute, “Cybersecurity attacks top ECRI list of health technology hazards for 2022”, *Reactions Weekly*, vol. 1892, no. 1, 2022, p. 1.

Erbschloe, M., *Threat Level Red. Cybersecurity Research Programs of the U.S. Government,* 1ª ed., Boca Raton, FL, CRC Press, 2017.

Esakov, G., “International Criminal Law in Russia: Missed Crimes Waiting for a Revival”, *Journal of International Criminal Justice,* vol. 15, no. 2, 2017, pp. 371 – 392.

Escobar Vélez, S., “El traslado del principio de precaución al Derecho penal en España”, *Nuevo Foro Penal,* no. 75, 2010, pp. 15 – 40.

Escribano Úbeda-Portugués, J., “La comunidad internacional frente al terrorismo: desarrollos y nuevos retos en el siglo XXI”, en L. Zúñiga Rodríguez (dir.), *Nuevos desafíos frente a la criminalidad organizada transnacional y el terrorismo*, 1ª ed., Madrid, Dykinson, 2021, pp. 361 – 388.

Escrivá Gascó, G. et al., *Seguridad Informática,* 1ª ed., Madrid, Macmillan Profesional, 2013.

Esteban Ruiz, A. M.ª, “El secuestro 2.0 en la era del Internet de las cosas: el *ransomware*”, en F. Bueno De Mata (dir.), *Fodertics 6.0: los nuevos retos del derecho ante la era digital*, Granada, Comares, 2017, pp. 127 – 136.

Estévez Mendoza, L., “Prevención e investigación de delitos en España: ¿un nuevo terreno para la IA?”, en F. Bueno de Mata (dir.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia,* Granada, Comares, 2020, pp. 259 – 272.

Estrada i Cuadras, A., *Violaciones de secreto empresarial. Un estudio de los ilícitos mercantiles y penales*, 1ª ed., Barcelona, Atelier, 2016.

Faraldo Cabana, P., *Las nuevas tecnologías en los delitos contra el patrimonio y el orden* socioeconómico, 1ª ed., Valencia, Tirant lo Blanch, 2009.

Faraldo-Cabana, P., “Defraudación de telecomunicaciones y uso no consentido de terminales de telecomunicación: dificultades de delimitación entre los arts. 255 y 256 CP”, en F. Muñoz Conde et al. (dirs.), *Un derecho penal comprometido: libro homenaje al prof. Dr. Gerardo Landrove Díaz,* Valencia, Tirant lo Blanch, 2011, pp. 363 – 383.

Federal Bureau of Investigation, *Internet Crime Report 2019,* Washington, D.C., Federal Bureau of Investigation, 2020.

Feijoo Sánchez, B.J., *Homicidio y lesiones imprudentes: requisitos y límites* materiales, 1ª ed., Argentina, Olejnik, 2021.

Fernández Bermejo, D. y Martínez Atienza, G., *Ciberseguridad, Ciberespacio y Ciberdelincuencia,* Cizur Menor, Navarra, Aranzadi, 2018.

Fernández Bermejo, D., "Algunas cuestiones jurídico penales sobre la ciberdelincuencia", en E. Monterroso Casado (dir.), *Inteligencia Artificial y Riesgos Cibernéticos. Responsabilidades y Aseguramiento,* Valencia, Tirant lo Blanch, 2019, pp. 325 – 374.

Fernández Delgado, L.G. (edit.), "Reino Unido lidera el nuevo ránking de ciberseguridad mundial, seguido de EE.UU. quedando España en un meritorio séptimo lugar", *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, vol. 28, no. 135, 2019, pp. 140 – 142.

Fernández López, M., "Algunas propuestas para regular la investigación del cibercrimen", en J.M. Asencio Mellado y O. Fuentes Soriano (dirs.), *La reforma del proceso penal,* Madrid, Wolters Kluwer, 2011, pp. 269 – 292.

Fernández Rodera, J.A., "Artículo 598", en M. Gómez Tomillo y A. M.ª Javato Martín (dirs.), *Comentarios prácticos al Código Penal. Tomo VI. Delitos contra la Constitución, el orden público. Delitos de traición y contra la paz o la independencia del Estado y relativos a la defensa nacional. Delitos contra la Comunidad internacional. Artículos 472 – 616 quáter*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, pp. 723 – 724.

Fernández Rodríguez, J.J., "Ciberseguridad: ¿Desafío insuperable? En búsqueda de escenarios de respuestas adecuados", en C. García Novoa y D. Santiago Iglesias (dirs.), *4ª Revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital*, Cizur Menor, Aranzadi, 2018, pp. 51 – 80.

Fernández Teruelo, J.G., *Cibercrimen: los Delitos Cometidos a Través de Internet*, 1ª ed., Madrid, Constitutio Criminalis Carolina, 2007.

Fernández Teruelo, J.G., *Derecho penal e Internet: especial consideración de los delitos que afectan a jóvenes y adolescentes,* , 1ª ed., Valladolid, Lex Nova, 2011.

Ferrer Gelabert, S., "E-salud: la tecnología al servicio de la salud", en C. Gil Membrado (dir.), *E-salud, autonomía y datos clínicos. Un nuevo paradigma*, 1ª ed., Madrid, Dykinson, 2021, pp. 13 – 31.

Finnemore, M. y Hollis, D.B., "Constructing Norms for Global Cybersecurity", *The American Journal of International Law,* vol. 110, no. 3, 2016, pp. 425 – 479.

Fiscalía General del Estado, *Instrucción no. 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías",* Madrid, Fiscalía General del Estado, 2011.

Fiscalía General del Estado, *Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos*, Madrid, Fiscalía General del Estado, 2017.

Fosch-Villaronga, E., *Robots, Healthcare, and the Law. Regulating Automation in Personal Healthcare*, 1ª ed., Oxfordshire, Routledge, 2020.

Frana, P.L., "Biometric Privacy and Security", en P.L. Frana y M.J. Klein (eds.), *Encyclopedia of Artificial Intelligence: The Past, Present and Future of AI,* 1ª ed., Santa Bárbara, CA, ABC-CLIO, 2021, pp. 44 – 47.

Fundación Instituto Roche, *Informe Anticipando Inteligencia artificial en salud: retos éticos y legales*, Madrid, Fundación Instituto Roche, 2020.

Galán Muñoz, A., *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 C.P.,* 1ª ed., Valencia, Tirant lo Blanch, 2005.

Galán Muñoz, A., "¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación", en A. Galán Muñoz (coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación,* 1ª ed., Valencia, Tirant lo Blanch, 2014, pp. 203 – 280.

Galán Muñoz, A., "La problemática utilización del principio de precaución como referente de la política criminal del moderno derecho penal. ¿Hacia un derecho penal del miedo a lo desconocido o hacia uno realmente preventivo?", *Revista de estudios de la justicia,* no. 22, 2015, pp. 69 – 117.

Galán Muñoz, A., *Los ciberdelitos en el ordenamiento español*, 1ª ed., Barcelona, Editorial UOC, 2019.

Ganuza Artiles, N., "Situación de la ciberseguridad en el ámbito internacional y en la OTAN", *Cuadernos de estrategia,* no. 149, 2011, pp. 166 – 214.

García-Prieto Cuesta, J., "¿Qué es un robot?", en M. Barrio Andrés (dir.), *Derecho de los Robots*, 2ª ed., Madrid, Wolters Kluwer, 2019, pp. 29 – 64.

García García, S., "Una aproximación a la futura regulación de la inteligencia artificial en la Unión Europea", *Revista de Estudios Europeos,* vol. 79, 2022, pp. 304 – 323.

García Portero, R., "Los robots en la sanidad", en M. Barrio Andrés (dir.), *Derecho de los Robots*, 2ª ed., Madrid, Wolters Kluwer, 2019, pp. 243 – 268.

García Sánchez, M.D., "Retos del uso de la inteligencia artificial en el proceso: impugnaciones con fundamentación algorítmica y derecho a la tutela judicial efectiva", en F. Bueno de Mata (dir.), *Fodertics 9.0: estudios sobre tecnologías disruptivas y justicia,* Granada, Comares, 2021, pp. 233 – 244.

García Teruel, R.M., "El Derecho de daños ante la inteligencia artificial y el *machine learning*: una aproximación desde las recomendaciones del Parlamento Europeo y del Grupo de Expertos de la Comisión Europea", en J.

Ataz López y J.A. Cobacho Gómez (coords.), *Cuestiones clásicas y actuales del Derecho de daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón. Tomo II,* Cizur Menor, Navarra, Aranzadi, 2021, pp. 1009 – 1056.

Garro Carrera, E. y Asúa Batarrita, A., *Atenuantes de reparación y de confesión. Equívocos de la orientación utilitaria. A propósito de una controvertida Sentencia del Juzgado de lo Penal no. 8 de Sevilla*, 1ª ed., Valencia, Tirant lo Blanch, 2008.

Gau, J.M., *Statistics for Criminology and Criminal Justice,* 3ª ed., Thousand Oaks, CA, SAGE Publications, 2019.

Geraci, R.M., *Apocalyptic AI*, 1ª ed., New York, NY, Oxford University Press, 2010.

Gercke, M., "10 years Convention on Cybercrime: Achievements and Failures of the Council of Europe´s Instrument in the Fight against Internet-related Crimes", *Computer Law Review International,* vol. 12, no. 5, 2011, pp. 142 – 149.

Gil Gil, A., "Daños informáticos", en E. Sanz Delgado y D. Fernández Bermejo (coords.), *Tratado de Delincuencia Cibernética*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021, pp. 467 – 510.

Gillespie, A.A., *Cybercrime: Key Issues and Debates,* 1ª ed., Abingdon, Routledge, 2016.

Glennon, M.J., "The Dark Future of International Cybersecurity Regulation", *Journal of National Security Law & Policy,* vol. 6, no. 2, 2013, pp. 563 – 570.

Goldstein, J.C. y Goldstein, H.V., "Intraoperative cyberattacks: cyberthreat awareness and cyber-resilience strategies in anesthesia", *Canadian Journal of Anesthesia,* vol. 68, no. 12, 2021, pp. 1838 – 1839.

Gómez Navajas, J., *La protección de los datos personales: un análisis desde la perspectiva del Derecho Penal*, 1ª ed., Navarra, Civitas, 2005.

Gómez Pavón, G., “Capítulo 5. Los delitos de descubrimiento y revelación de secretos de empresa”, en P. Gómez Pavón, M. Bustos Rubio, y D. Pavón Herradón (autores), *Delitos Económicos. Análisis doctrinal y jurisprudencial. Adaptado a la LO 1/2019, de 20 de febrero, por la que se modifica la LO del CP, para transponer Directivas de la UE en los ámbitos financieros y de terrorismo,* 1ª ed., Madrid, Wolters Kluwer, 2019, pp. 129 – 154.

Gómez Rivero, M.ª D. C., *Los delitos contra la propiedad intelectual e industrial. La tutela penal de los derechos sobre bienes inmateriales*, 1ª ed., Valencia, Tirant lo Blanch, 2012.

González, A. et al., *Memento Práctico de Derecho de las Nuevas Tecnologías 2020 - 2021*, Madrid, Francis Lefebvre, 2019.

González Cussac, J.L., “Computación en nube: la verificación de los ordenamientos internos en los países de localización como garantía de la seguridad y la confidencialidad de la información”, en R. Martínez Martínez (edit.), *Derecho y Cloud Computing*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2012, pp. 289 – 307.

González Rus, J.J., “Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (artículo 264.2 del Código penal)”, en J.L. Díez Ripollés, C.M. Romeo Casabona, L. Gracia Martín y J.F. Higuera Guimerá (eds.), *La ciencia del derecho penal ante el nuevo siglo: libro homenaje al profesor doctor don José Cerezo Mir*, Madrid, Tecnos, 2002, pp. 1281 – 1298.

Górka, M., “The Cybersecurity Strategy of the Visegrad Group Countries”, *Politics in Central Europe,* vol. 14, no. 2, 2018, pp. 75 – 98.

Gorriz Royo, E. M.ª, *El concepto de autor en Derecho penal*, 1ª ed., Valencia, Tirant lo Blanch, 2008.

Gracia Martín, L., Boldova Pasamar, M.A., y Alastuey Dobón, C., *Lecciones de consecuencias jurídicas del delito*, 5ª ed., Valencia, Tirant lo Blanch, 2016.

Greengard, S., “Cybersecurity Gets Smart”, *Communications of the ACM*, vol. 59, no. 5, 2016, pp. 29 – 31.

Guérez Tricarico, P., “Delitos patrimoniales y contra el orden socioeconómico. Sección 14. Daños”, en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1413 – 1421.

Guía práctica de Ciberseguridad, Cizur Menor, Navarra, Aranzadi, 2019.

Guillén, R., “Retos a la Hora de Proteger la Ciberseguridad de los Hospitales Conectados”, *Revista de la Sociedad Española de Informática y Salud*, no. 134, 2019, pp. 37 – 40.

Guisasola Lerma, C., “Tutela penal del secreto de comunicaciones. Estudio particular del supuesto de interceptación ilegal de telecomunicaciones por autoridad o funcionario público”, en J.C. Carbonell Mateu, J.L. González Cussac, y E. Orts Berenguer (dirs.), *Constitución, derechos fundamentales y sistema penal. Semblanzas y estudios con motivo del setenta aniversario del profesor Tomás Salvador Vives Antón. Tomo I*, 1ª ed., Valencia, Tirant lo Blanch, 2009, pp. 945 – 974.

Gutiérrez Mayo, E., Castro Romero, M.ª V., y Pérez Golpe, I., *Delitos informáticos. Paso a paso. Análisis detallado de las conductas delictivas más comunes en el entorno informático*, 1ª ed., A Coruña, Colex, 2021.

Haataja, S., “The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach”, *Law, Innovation and Technology,* vol. 9, no. 2, 2017, pp. 159 – 189.

Hansen, L. y Nissenbaum, H., “Digital Disaster, Cyber Security, and the Copenhagen School”, *International Studies Quarterly,* vol. 53, no. 4, 2009, pp. 1155 – 1175.

Henderson, C., “The United Nations and the regulation of cyber-security”, en N. Tsagourias y R. Buchan (eds.), *Research Handbook on International Law and Cyberspace,* Cheltenham, Edward Elgar Publishing, 2015, pp. 465 – 490.

Hernández Díaz, L., *Los accesos ilícitos a sistemas informáticos: normativa internacional y regulación en el ordenamiento penal español*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2019.

Herrero González, A., "The value of data and its applicability in the Health Sector", *Revista Española de Medicina Nuclear e Imagen Molecular*, vol. 41, no. 1, 2022, pp. 39 – 42.

Hidary, J.D., *Quantum Computing: An Applied Approach*, 1ª ed., Cham, Springer, 2019.

Hirsch Ballin, E., Dijstelbloem, H., y De Goede, P., "The Extension of the Concept of Security", en E. Hirsch Ballin, H. Dijstelbloem y P. De Goede (eds.), *Security in an Interconnected World: A Strategic Vision for Defence Policy,* 1ª ed., Cham, Springer, 2020, pp. 13 – 39.

Holzinger, A., Röcker, C., y Ziefle, M., "From Smart Health to Smart Hospitals", en A. Holzinger, C. Röcker, y M. Ziefle (eds.), *Smart Health. Open Problems and Future Challenges*, 1ª ed., Cham, Springer, 2015, pp. 1 – 20.

Holzleitner, M. y Reichl, J., "European provisions for cyber security in the smart grid: An overview of the NIS-directive", *e & i Elektrotechnik und Informationstechnik,* no. 134, 2017, pp. 14 – 18.

Iglesias Cabero, M., *Robótica y Responsabilidad. Aspectos legales en las diferentes áreas del Derecho*, 1ª ed., A Coruña, Colex, 2017.

Instituto Nacional de Ciberseguridad de España, *Balance de ciberseguridad 2018,* León, Instituto Nacional de Ciberseguridad de España, 2019.

Instituto Nacional de Ciberseguridad de España, *Balance de ciberseguridad 2019,* León, Instituto Nacional de Ciberseguridad de España, 2020.

Instituto Nacional de Ciberseguridad de España, *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario,* León, Instituto Nacional de Ciberseguridad de España, 2020.

Instituto Nacional de Ciberseguridad de España, *Balance de ciberseguridad 2020,* León, Instituto Nacional de Ciberseguridad de España, 2021.

Instituto Nacional de Ciberseguridad de España, *Balance de ciberseguridad 2021,* León, Instituto Nacional de Ciberseguridad de España, 2022.

Instituto Nacional de Ciberseguridad de España / Agencia Estatal Boletín Oficial del Estado, *Código de Derecho de la Ciberseguridad: edición actualizada a 4 de mayo de 2022,* Madrid, Instituto Nacional de Ciberseguridad de España / Agencia Estatal Boletín Oficial del Estado, 2022.

Iñigo Corroza, E., Sánchez-Ostiz, P., y Pereira Garmendia, M.M., "Cibercriminalidad", en E. Valpuesta Gastaminza y J.C. Hernández Peña (coords.), *Tratado de Derecho* digital, 1ª ed., Madrid, Wolters Kluwer, 2021, pp. 665 – 690.

Jacomet, C. et al., "E-health. Patterns of use and perceived benefits and barriers among people living with HIV and their physicians. Part 1: Information retrieval on the Internet and social networks", *Médecine et Maladies Infectieuses*, vol. 50, no. 7, 2020, pp. 575 – 581.

Jacomet, C. et al., "E-health. Patterns of use and perceived benefits and barriers among people living with HIV and their physicians. Part 2: Health apps and smart devices", *Médecine et Maladies Infectieuses*, vol. 50, no. 7, 2020, pp. 582 – 589.

Jacomet, C. et al., "E-health. Patterns of use and perceived benefits and barriers among people living with HIV (PLHIV) and their physicians. Part 3: Telemedicine and collection of computerized personal information", *Médecine et Maladies Infectieuses*, vol. 50, no. 7, 2020, pp. 590 – 596.

Jiménez Fortea, F.J., "¿Existe un *Derecho procesal del enemigo* en la lucha contra el terrorismo en España?", en F.J. Garrido Carrillo (dir.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumentos,*

límites y perspectivas en la era digital, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2022, pp. 193 – 226.

Jiménez García, F., "La ciberseguridad en el marco internacional. El sistema del Convenio de Budapest de 2001 sobre la ciberdelincuencia adoptado en el Consejo de Europa", en E.R. Jordá Capitán y V. De Priego Fernández (dirs.), *La protección y seguridad de la persona en Internet. Aspectos sociales y jurídicos",* Madrid, Reus, 2014, pp. 49 – 79.

Jimeno Muñoz, J., *Derecho de daños tecnológicos, ciberseguridad e Insurtech*, 1ª ed., Madrid, Dykinson, 2019.

Joyanes Aguilar, L., *Internet de las Cosas. Un futuro hiperconectado: 5G, Inteligencia Artificial, Big Data, Cloud, Blockchain y Ciberseguridad*, 1ª ed., Barcelona, Marcombo, 2021.

Juanes Peces, A., "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Capítulo I. Del descubrimiento y revelación de secretos", en C. Conde-Pumpido Tourón (dir.), *Comentarios al Código Penal, Tomo 2*, Barcelona, Bosch, 2007, pp. 1537 – 1593.

Kaiser, J., "Blueprint for cyber health care", *Science*, vol. 287, no. 5458, 2000, p. 1551.

Kańciak, A., "An Analysis of the Legal Systems and Mechanisms Introduced in the European Union in the Fight Against Cyberspace Threats", *Internal Security,* vol. 8, no. 2, 2016, pp. 195 – 224.

Kaplan, M., "Sex Offenses and the Problem of Prevention", en L. Alexander y K. Kessler Ferzan (eds.), *The Palgrave Handbook of Applied Ethics and the Criminal Law,* 1ª ed., Londres, Palgrave Macmillan, 2019, pp. 709 – 727.

Karapilafis, G., "Artificial Intelligence in Cyber Defense", en N. J. Daras (edit.), *Cyber-Security and Information Warfare,* 1ª ed., Nueva York, NY, Nova Science Publishers, 2019, pp. 193 – 200.

Kaye, J. et al., *Governing biobanks: understanding the interplay between law and practice,* 1ª ed., Oxford, Hart Publishing Ltd., 2012.

Keenlyside, A.T. et al., "El *hacking* desde una perspectiva legal, criminológica y técnica", *Revista Aranzadi Doctrinal,* no. 6, 2021, pp. 1 – 24.

Kettemann, M.C., "Ensuring Cybersecurity through International Law", *Revista española de derecho internacional,* vol. 69, no. 2, 2017, pp. 281 – 289.

Kettunen, M., *Legitimizing European Criminal Law: Justification and Restrictions,* 1ª ed., Cham, Springer, 2020.

Kierkegaard, S., "Cybercrime convention: narrowing the cultural and privacy gap?", *International Journal of Intercultural Information Management,* vol. 1, no. 1, 2007, pp. 17 – 32.

Kohnke, A., Sigler, K., y Shoemaker, D., *Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework*, 1ª ed., Boca Raton, FL, CRC Press, 2017.

Korobeev, A.I., Dremlyuga, R.I., y Kuchina, Y.O., "Cybercrimes in the Russian Federation: Criminological and Criminal Law Analysis of the Situation", *Russian Journal of Criminology,* vol. 13, no. 3, 2019, pp. 416 – 425.

Kosseff, J., *Cybersecurity Law,* 1ª ed., Hoboken, NJ, Wiley, 2017.

Kosseff, J., "Defining Cybersecurity Law", *Iowa Law Review,* vol. 103, no. 3, 2018, pp. 985 – 1031.

Kostoff R.N. et al., "Adverse health effects of 5G mobile networking technology under real-life conditions", *Toxicology Letters,* vol. 323, 2020, pp. 35 – 40.

Kotronis C. et al., "Evaluating Internet of Medical Things (IoMT)-Based Systems from a Human – Centric Perspective", *Internet of Things,* vol. 8, 2019, pp. 1 – 17.

Kovács, L., “Cyber Security Policy and Strategy in the European Union and NATO”, *Land Forces Academy Review,* vol. 23, no. 1, 2018, pp. 16 – 24.

Kurgalin, S. y Borzunov, S., *Concise Guide to Quantum Computing: Algorithms, Exercises and* Implementations, 1ª ed., Cham, Springer, 2021.

Landau, S., *Listening in Cybersecurity in an Insecure Age,* 1ª ed., New Haven, Yale University Press, 2017.

Laptev, V. y Fedin, V., “Legal Awareness in a Digital Society”, *Russian Law Journal*, vol. 8, no.1, 2020, pp. 138 – 157.

Lazari, A., “De ciberataques y ciberleviatanes: cartografía de la governance en el prisma del derecho europeo y comparado”, en G. Fernández Arribas (edit.), *Ciberataques y ciberseguridad en la escena internacional,* 1ª ed., Cizur Menor, Navarra, Aranzadi, 2019, pp. 175 – 206.

Leclair, J. y Keeley, G., *Cybersecurity in Our Digital Lives,* 1ª ed., Albany, NY, Hudson Whitman / Excelsior College Press, 2015.

Liu, E., Effiok, E., y Hitchcock, J., “Survey on health care applications in 5G networks”, *IET Communications,* vol. 14, no. 7, 2020, pp. 1073 – 1080.

Llaneza González, P., *Seguridad y responsabilidad en la Internet de las cosas (IoT)*, 1ª ed., Madrid, Wolters Kluwer, 2018.

Lledó Benito, I., “Visión del Derecho penal en relación con la robótica, IA y la ciberdelincuencia”, en F. Lledó Yagüe, I. Benítez Ortúzar y O. Monje Balmaseda (dirs.), *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0. Los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes,* 1ª edición, Madrid, Dykinson, 2021, pp. 149 – 196.

Lledó Benito, I., *El Derecho penal, robots, IA y cibercriminalidad: desafíos éticos y jurídicos. ¿Hacia una distopía?*, 1ª ed., Madrid, Dykinson, 2022.

Llobet Anglí, M., “Delitos contra el orden público. Sección 3. Desórdenes públicos”, en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 2075 – 2085.

Llobet Anglí, M., “Delitos patrimoniales y contra el orden socioeconómico. Sección 3. Robo con fuerza en las cosas”, en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1299 – 1316.

Loncaric, F. et al., “La integración de la inteligencia artificial en el abordaje clínico del paciente: enfoque en la imagen cardíaca”, *Revista Española de Cardiología,* vol. 74, no. 1, 2021, pp. 72 – 80.

López-Muñoz, J., *Cibercriminalidad e investigación tecnológica*, 1ª ed., Madrid, Dykinson, 2020.

López Picó, R., “Investigación tecnológica en el proceso penal: *hacking* legal”, en F. Bueno de Mata (dir.), *Fodertics 7.0: estudios sobre derecho digital,* Granada, Comares, 2019, pp. 349 – 356.

López Rodríguez, O., “Gestión de riesgos en protección de datos y seguridad de la información”, en P. Simón Castellano y A. Abadías Selma (coords.), *Mapa de riesgos penales y prevención del delito en la empresa*, 1ª ed., Madrid, Wolters Kluwer, 2020, pp. 235 – 257.

Lozano Merino, M.A., “Ciberseguridad y COVID-19 nos empujan para la transformación digital”, *Aranzadi digital,* no. 1/2020, 2020, pp. 1 – 10.

Lüttger, H., *Medicina y Derecho penal*, 1ª ed., Argentina, Olejnik, 2021.

Luzón Cuesta, J.M., Luzón Cánovas, A., y Luzón Cánovas, M., *Compendio de Derecho Penal, Parte Especial*, 23ª ed., Madrid, Dykinson, 2021.

Machín, N. y Gazapo, M., “La Ciberseguridad como factor crítico en la Seguridad de la Unión Europea”, *Revista UNISCI,* no. 42, 2016, pp. 47 – 68.

Mackey, T.K. y Nayyar, G., “Digital danger: a review of the global public health, patient safety and cybersecurity threats posed by illicit online pharmacies”, *British Medical Bulletin,* vol. 118, no. 1, 2016, pp. 115 – 131.

Madsen, W., “Cybercrime Convention Steams Ahead”, *Network Security*, no. 5, 2001, p. 6.

Maldonado Guzmán, D.J., “El mal denominado delito de *grooming online* como forma de violencia sexual contra menores. Problemas jurídicos y aspectos criminológicos”, *Revista Electrónica de Estudios Penales y de la Seguridad: REEPS,* no. Extra 5, 2019, pp. 1 – 18. Martin, G. et al., “WannaCry - A year on”, *The BMJ,* vol. 361, 2018, pp. 1 – 2.

Manjikian, M., *Cybersecurity Ethics: An Introduction,* 1ª ed., Abingdon, Routledge, 2018.

Maraver Gómez, M., “Delitos contra la seguridad colectiva. Sección 1. Delitos de riesgo catastrófico. B. Estragos”, en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1691 – 1694.

Maraver Gómez, M., “Delitos patrimoniales y contra el orden socioeconómico. Sección 8. Estafa”, en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1348 – 1369.

Marcus, G. y Davis, E., *Rebooting AI: Building Artificial Intelligence We Can Trust,* 1ª ed., New York, NY, Pantheon Books, 2019.

Marín Cano, A., “Investigación penal de delitos tecnológicos”, en F. Bueno de Mata (dir.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia,* Granada, Comares, 2020, pp. 285 – 298.

Markopoulou, D., Papakonstantinou, V., y De Hert, P., “The new EU cybersecurity framework: The NIS Directive, ENISA´s role and the General Data Protection Regulation”, *Computer Law & Security Review,* vol. 35, no. 6, 2019, pp. 1 – 11.

Maroz, N., “Regionalization of international cooperation in the fight against cybercrime”, *Law Review: Judicial Doctrine & Case Law*, vol. 10, no. 2, 2019, pp. 218 – 227.

Marsili, M., “The War on Cyberterrorism”, *Democracy and Security,* vol. 15, no. 2, 2019, pp. 172 – 199.

Martin, G., Kinross, J., y Hankin, C., “Effective cybersecurity is fundamental to patient safety”, *The BMJ,* vol. 357, 2017, pp. 1 – 2.

Martínez-Buján Pérez, C., *Delitos relativos al secreto de empresa*, 1ª ed., Valencia, Tirant lo Blanch, 2010.

Martínez-Buján Pérez, C., *Derecho penal económico y de la empresa*, 1ª ed., Valencia, Tirant lo Blanch, 2013.

Martínez Galindo, G., “Motivación criminal de los adolescentes en el ciberespacio”, en A. Abadías Selma, S. Cámara Arroyo, y P. Simón Castellano (coords.), *Tratado sobre delincuencia juvenil y responsabilidad penal del menor. A los 20 años de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores,* 1ª ed., Madrid, Wolters Kluwer, 2021, pp. 501 – 516.

Mata y Martín, R. M., *Estafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago. El Uso Fraudulento de Tarjetas y otros Instrumentos de Pago,* 1ª ed., Cizur Menor, Navarra, Aranzadi, 2007.

Mata y Martín, R. M., “Medios electrónicos de pago y delitos de estafa”, en R.M. Mata y Martín (dir.), *Los medios electrónicos de pago. Problemas* jurídicos, 1ª ed., Granada, Comares, 2007, pp. 320 – 365.

Mata y Martín, R. M., “Artículo 248”, en M. Gómez Tomillo (dir.), *Comentarios prácticos al Código Penal. Tomo III. Delitos contra el patrimonio y socioeconómicos. Artículos 234 – 318 bis*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, pp. 165 – 176.

Matusitz, J., “Postmodernism and Networks of Cyberterrorists”, *Journal of Digital Forensic Practice,* vol. 2, no. 1, 2008, pp. 17 – 26.

Mazur, J., “Automated Decision – Making and the Precautionary Principle in EU Law”, *Baltic Journal of European Studies,* vol. 9, no. 4, 2019, pp. 3 – 18.

McGuire, M., *Nation States, Cyberconflict and the Web of Profit*, Palo Alto, CA, HP Inc., 2021.

Medina, M. y Molist, M., *Cibercrimen,* 1ª ed., Barcelona, Tibidabo, 2015.

Melón Muñoz, A. et al., *Memento Práctico Procesal Penal 2022*, Madrid, Francis Lefebvre, 2021.

Mestre Delgado, E., “Tema 22. Delitos contra la Administración Pública”, en C. Lamarca Pérez (coord.), *Delitos. La parte especial del Derecho penal*, 6ª ed., Madrid, Dykinson, 2021, pp. 871 – 930.

Middleton, B., *A History of Cyber Security Attacks: 1980 to Present,* 1ª ed., Boca Raton, FL, CRC Press, 2017.

Milione, C., “La noción de seguridad en la doctrina del Tribunal Europeo de Derechos Humanos: referencias al derecho a la tutela judicial efectiva”, *Revista de Derecho Político,* no. 107, 2020, pp. 241 – 267.

Milivojevic, S., *Crime and Punishment in the Future Internet. Digital Frontier Technologies and Criminology in the Twenty-First Century*, 1ª ed., Oxfordshire, Routledge, 2021.

Mínguez Rosique, M., “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Sección 1. Descubrimiento y revelación de secretos”, en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1178 – 1190.

Ministerio de Defensa de España, *El ciberespacio. Nuevo escenario de confrontación,* Madrid, Ministerio de Defensa de España, 2012.

Ministerio del Interior de España, *Estudio sobre la cibercriminalidad en España 2018,* Madrid, Ministerio del Interior de España, 2019.

Miró Llinares, F., *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio,* 1ª ed., Madrid, Marcial Pons, 2012.

Miró Llinares, F., "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología. Tercera época,* no. 20, 2018, pp. 87 – 130.

Molina Fernández, F., "Delitos de traición y contra la paz o la independencia del Estado y relativos a la Defensa Nacional. Sección 3. Descubrimiento y revelación de secretos e informaciones relativas a la Defensa Nacional", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 2194 – 2196.

Montserrat Sánchez-Escribano, M.I., "La protección penal del servidor de Cloud Computing y de los datos almacenados en él o en proceso de transferencia hacia él", en Apolònia Martínez Nadal (dir.), *Big Data, Cloud Computing y otros retos jurídicos planteados por las tecnologías emergentes*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2019, pp. 105 – 122.

Morales Prats, F., "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en G. Quintero Olivares (dir.), *Comentarios a la Parte Especial del Derecho* Penal, 10ª ed., Cizur Menor, Navarra, Aranzadi, 2016, pp. 429 – 508.

Morán Blanco, S., "La ciberseguridad y el uso de las Tecnologías de la Información y la Comunicación (TIC) por el terrorismo", *Revista española de derecho internacional,* vol. 69, no. 2, 2017, pp. 195 – 221.

Moret Millás, V., "El marco jurídico de la ciberseguridad en España", en F. Pérez Bes (coord.), *El derecho de Internet*, Barcelona, Atelier, 2016, pp. 253 – 300.

Moret Millás, V., “Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español”, *Bie3: Boletín IEEE*, no. 5, 2017, pp. 733 – 751.

Moret Millás, V., “Un nuevo escenario jurídico para la ciberseguridad en España: el Real Decreto-Ley 12/2018, de Seguridad de las redes y sistemas de información”, *Diario La Ley,* no. 9270, 2018, pp. 1 – 16.

Morón Lerma, E., *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red,* 2ª ed., Cizur Menor, Navarra, Aranzadi, 2002.

Mozo Seoane, A., “La revolución tecnológica y sus retos: medios de control, fallos de los sistemas y ciberdelincuencia”, en C. Rogel Vide (coord.), *Los robots y el Derecho*, 1ª ed., Madrid, Reus, 2018, pp. 79 – 98.

Muñoz-González, L. y Lupu, E.C., “The security of Machine Learning Systems”, en L. F. Sikos (edit.), *AI in Cybersecurity*, Cham, Springer, 2019, pp. 47 – 80.

Muñoz Conde, F., *Derecho Penal, Parte Especial*, 23ª ed., Valencia, Tirant lo Blanch, 2021.

Murch R.S. et al., “Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy”, *Frontiers in Bioengineering and Biotechnology,* vol. 6, no. 39, 2018, pp. 1 - 6.

Murphy, S.D., “Adoption of Convention on Cybercrime”, *The American Journal of International Law,* vol. 95, no. 4, 2001, pp. 889 – 891.

Nadarzynski, T. et al., “Acceptability of artificial intelligence (AI)-led chatbot services in healthcare: A mixed-methods study”, *Digital Health,* vol. 5, 2019, pp. 1 – 12.

Nava Garcés, A.E., “El caso WannaCry. Ataque en la red”, *Revista Penal*, no. 42, 2018, pp. 148 – 164.

Navas Navarro, S., “Derecho e inteligencia artificial desde el diseño. Aproximaciones”, en S. Navas Navarro (coord.), *Inteligencia artificial. Tecnología. Derecho,* Valencia, Tirant lo Blanch, 2017, pp. 23 – 72.

Nicolás Jiménez, P., *La protección jurídica de los datos genéticos de carácter personal,* 1ª ed., Granada, Comares, 2006.

Nicolás Jiménez, P., “La protección de los datos genéticos de carácter personal en Derecho penal español: un caso práctico”, en E.J. Armaza Armaza, J. Mendoza Valdez, I. De Miguel Beriain y A. Urruela Mora (coords.), *Temas de Derecho penal: libro homenaje a Luis Guillermo Cornejo Cuadros,* Arequipa, Adrus, 2008, pp. 189 – 202.

Nicolás Jiménez, P., “Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos”, *Revista de Derecho y Genoma Humano: Genética, Biotecnología y Medicina Avanzada*, no. extra, 2019, pp. 129 – 167.

Nieto Rodríguez, M., “El nuevo concepto de seguridad: amenazas y riesgos emergentes”, en Ministerio de Defensa – Instituto Español de Estudios Estratégicos (eds.), *La cooperación Fuerzas de Seguridad – Fuerzas Armadas frente a los riesgos emergentes,* 1ª ed., Madrid, Ministerio de Defensa – Instituto Español de Estudios Estratégicos, 2001, pp. 15 – 58.

O'Connell, M.E., “Cyber Security without Cyber War”, *Journal of Conflict & Security Law,* vol. 17, no. 2, 2012, pp. 187 – 209.

Obispo Triana, C., “Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos”, *Revista Aranzadi Doctrinal*, no. 10, 2017, pp. 183 – 192.

Obrador Serra, F., “Análisis del concepto de seguridad”, *Cuadernos de estrategia,* no. 49, 1992, pp. 25 – 49.

Olănescu, S.S. y Olănescu, A.V., “Cyberterrorism: The Latest Crime Against International Public Order”, *Lex ET Scientia International Journal,* vol. 1, no. XXVI, 2019, pp. 92 – 100.

Oliver, N., “Hacia una inteligencia artificial por y para la sociedad”, *Temas para el debate,* no. 299, 2019, pp. 37 – 39.

Orts Berenguer, E., y Roig Torres, M., *Delitos informáticos y delitos comunes cometidos a través de la informática,* Valencia, Tirant lo Blanch, 2001.

Otero, P., “El derecho penal frente a los riesgos de internet: el ciberdelito”, *Actuarios*, no. 48, 2021, pp. 30 – 32.

Owen, T., Noble, W., y Speed, F.C., *New Perspectives on Cybercrime,* 1ª ed., Cham, Springer, 2017.

Oxford Commission on AI & Good Governance, *Harmonising Artificial Intelligence: The role of standards in the EU AI Regulation,* Oxford, Oxford Commission on AI & Good Governance, 2021.

Palazzo, F., “Principio de última ratio e hipertrofia del derecho penal”, en L.A. Arroyo Zapatero e I. Berdugo Gómez de la Torre (dirs.), *Homenaje al Dr. Marino Barbero Santos: In Memoriam (Vol. 1)*, Cuenca, Ediciones de la Universidad de Castilla – La Mancha / Ediciones Universidad de Salamanca, 2001, pp. 433 – 442.

Palma Herrera, J.M., “Inteligencia artificial y lucha contra la delincuencia. Potencialidad y peligros en el mundo global”, en F.H Llano Alonso y J. Garrido Martín (eds.), *Inteligencia artificial y Derecho. El jurista ante los retos de la era digital,* Cizur Menor, Navarra, Aranzadi, 2021, pp. 279 – 294.

Palomino Martín, J.M., *Derecho penal y nuevas tecnologías. Hacia un sistema informático para la aplicación del Derecho penal*, 1ª ed., Valencia, Tirant lo Blanch, 2006.

Parisi, A., *Hands-On Artificial Intelligence for Cybersecurity. Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies,* 1ª ed., Birmingham, Packt, 2019.

Parker, M.J. et al., "Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic", *Journal of Medical Ethics,* 2020, pp. 1 – 5.

Pastor Muñoz, N., *Riesgo permitido y principio de legalidad: la remisión a los estándares sociales de conducta en la construcción de la norma jurídico-penal*, 1ª ed., Barcelona, Atelier, 2019.

Pattison, J., "From defence to offence: The ethics of private cybersecurity", *European Journal of International Security,* vol. 5, no. 2, 2020, pp. 233 – 254.

Payne, B.K. y Hadzhidimova, L., "Cyber Security and Criminal Justice Programs in the United States: Exploring the Intersections", *International Journal of Criminal Justice Sciences,* vol. 13, no. 2, 2018, pp. 385 – 404.

Pérez Bes, F. et al., *Memento Experto en Ciberseguridad*, 1ª ed., Madrid, Francis Lefebvre, 2021.

Pérez Bes, F., "Soft-law, Self-regulation and Compliance in AI", en P. García Mexía y F. Pérez Bes (eds.), *Artificial Intelligence and the Law,* 1ª ed., Madrid, Wolters Kluwer, 2021, pp. 77 – 108.

Pérez del Valle, C., *La imprudencia en el Derecho penal. El tipo subjetivo del delito imprudente*, 1ª ed., Barcelona, Atelier, 2012.

Pérez Machío, A.I., "Consideraciones de derecho comparado: la proyección de la normativa internacional en el tratamiento penal de la delincuencia informática", en J.L. De la Cuesta Arzamendi (dir.), *Derecho Penal Informático*, Cizur Menor, Navarra, Aranzadi, 2010, pp. 147 – 158.

Pérez-Prat Durbán, L., "Los ciberataques y el uso de la fuerza en las relaciones internacionales", en G. Fernández Arribas (edit.), *Ciberataques y*

ciberseguridad en la escena internacional, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2019, pp. 17 – 50.

Piernas López, J.J., *Ciberdiplomacia y ciberdefensa en la Unión Europea*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2020.

Pierotti, W., "Cyber Babel: Finding the Lingua Franca in Cybersecurity Regulation", *Fordham Law Review,* vol. 87, no. 1, 2018, pp. 405 – 435.

Piggin, R., "NIS Directive and the Security of Critical Services", *ITNOW,* vol. 60, no. 1, 2018, p. 44.

Popham, J. et al., "Exploring police-reported cybercrime in Canada: variation and correlates", *Policing: An International Journal,* vol. 43, no. 1, 2020, pp. 35 – 48.

Portilla Contreras, G., *El Derecho penal a la libertad y seguridad (de los derechos)*, 1ª ed., Madrid, Iustel, 2012.

Postigo Palacios, A., *Seguridad informática,* 1ª ed., Madrid, Paraninfo, 2020.

Pozuelo Pérez, L., "Delitos contra la Administración pública. Sección 5. Infidelidad en la custodia de documentos y violación de secretos", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1886 – 1891.

Pozuelo Pérez, L., "Delitos contra la Constitución. Sección 6. Delitos cometidos por funcionarios públicos contra las garantías constitucionales", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 2020 – 2030.

Proshchyn, I. y Shypovskyi, V., "Cyber security in the national security & defence sector of Ukraine: today´s challenges and ways to avoid possible threats", *Social Development & Security,* vol. 10, no. 1, 2020, pp. 3 – 8.

Quintero Olivares, G., “La robótica ante el derecho penal: el vacío de respuesta jurídica a las desviaciones incontroladas”, *Revista Electrónica de Estudios Penales y de la Seguridad: REEPS*, no. 1, 2017, pp. 1 – 23.

Raff, E., Lantzy, S., y Maier, E.J., “Dr. AI, Where Did You Get Your Degree?”, en F. Koch et al. (eds.), *Artificial Intelligence in Health*, 1ª ed., Cham, Springer, 2019, pp. 76 – 83.

Rallo Lombarte, A. et al*., Robo de identidad y protección de datos,* Cizur Menor, Navarra, Aranzadi, 2010.

Reed, J.C. y Dunaway, N., “Cyberbiosecurity Implications for the Laboratory of the Future”, *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 182, 2019, pp. 1 – 14.

Rey Huidobro, L.F., “La estafa informática: relevancia penal del *phishing* y el *pharming*”, *La ley penal: revista de derecho penal, procesal y penitenciario,* vol. 10, no. 101, 2013, pp. 22 – 35.

Rhodes, J.D. y Litt, R.S., *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals,* 2ª ed., Chicago, IL, ABA Publishing, 2018.

Richardson, L.C. et al., “Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape”, *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 99, 2019, pp. 1 – 5.

Richardson, S.V.A. y Gilmour, N., “Cyber Crime and National Security: A New Zealand Perspective”, *The European Review of Organised Crime,* vol. 2, no. 2, 2015, pp. 51 – 70.

Richet, J., *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*, 1ª ed., Hershey, PA, IGI Global, 2015.

Robles Carrillo, M., “Las fuerzas armadas ante el reto de la ciberseguridad”, en S. Olarte Encabo (dir.), *Estudios sobre derecho militar y defensa,* Cizur Menor, Navarra, Aranzadi, 2015, pp. 415 – 441.

Rodríguez Fernández, R., “Las penas en el Código Penal de 1995”, en R. Rodríguez Fernández y P. Simón Castellano (autores), *La pena de ingreso en prisión. Regulación actual y antecedentes históricos*, 1ª ed., Madrid, Wolters Kluwer, 2021, pp. 243 – 360.

Rodríguez Mesa, M.J., *Los delitos de daños: Capítulo IX del Título XIII del CP tras la reforma de la LO 1/2015,* 1ª ed., Valencia, Tirant lo Blanch, 2017.

Rodríguez-Miguel Ramos, J., *La autoprotección en la estafa en la jurisprudencia del Tribunal Supremo*, 1ª ed., Valencia, Tirant lo Blanch, 2013.

Rogachev, I., “The European Convention on Cybercrime is Inadequate to the Task”, *Security Index: A Russian Journal on International Security,* vol. 17, no. 4, 2011, pp. 5 – 8.

Romeo Casabona, C.M., *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las nuevas tecnologías de la información,* 1ª ed., Madrid, Fundesco, 1988.

Romeo Casabona, C.M., “Los delitos de daños en el ámbito informático”, *Cuadernos de política criminal*, no. 43, 1991, pp. 91 – 118.

Romeo Casabona, C.M., “La protección penal de la intimidad y de los datos personales en sistemas informáticos y en redes telemáticas (Internet)”, *Estudios jurídicos. Ministerio Fiscal,* 2001, pp. 273 – 312.

Romeo Casabona, C.M., “La peligrosidad y el peligro en la estructura del tipo del delito imprudente”, en J.L. Díez Ripollés, C.M. Romeo Casabona, L. Gracia Martín y J.F. Higuera Guimerá (eds.), *La ciencia del derecho penal ante el nuevo siglo: libro homenaje al profesor doctor don José Cerezo Mir*, Madrid, Tecnos, 2002, pp. 941 – 962.

Romeo Casabona, C.M., “La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet”, *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento,* no. 2, 2002, pp. 123 – 149.

Romeo Casabona, C.M., “La protección penal de la intimidad y de los datos personales: los mensajes de correo electrónico y otras comunicaciones de carácter personal a través de Internet y problemas sobre la ley penal aplicable”, *Estudios Jurídicos. Ministerio Fiscal,* no. 2, 2003, pp. 73 – 104.

Romeo Casabona, C.M., “Aportaciones del principio de precaución al Derecho Penal”, en C.M. Romeo Casabona (edit.), *Principio de precaución, Biotecnología y Derecho*, Granada, Comares, 2004, pp. 385 – 422.

Romeo Casabona, C.M., *Las Transformaciones del Derecho penal en un mundo en cambio (Volumen I)*, 1ª ed., Arequipa, Adrus, 2004.

Romeo Casabona, C.M., *Las Transformaciones del Derecho penal en un mundo en cambio (Volumen II)*, 1ª ed., Arequipa, Adrus, 2004.

Romeo Casabona, C.M., *Los delitos de descubrimiento y revelación de secretos,* 1ª ed., Valencia, Tirant lo Blanch, 2004.

Romeo Casabona, C.M., “Sobre la estructura monista del dolo. Una visión crítica”, en H. Joachim Hirsch, J. Cerezo Mir y E. Alberto Donna (dirs.), *Hans Welzel en el pensamiento penal de la modernidad*, 1ª ed., Santa Fe, Rubinzal – Culzoni, 2005, pp. 451 – 484.

Romeo Casabona, C.M., “De los delitos informáticos al cibercrimen. Una aproximación conceptual y político criminal”, en C.M. Romeo Casabona (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Granada, Comares, 2006, pp. 1 – 42.

Romeo Casabona, C.M., “La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de la

red", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* no. 10, 2006, pp. 15 – 33.

Romeo Casabona, C.M., "Los datos de carácter personal como bienes jurídicos penalmente protegidos", en C.M. Romeo Casabona (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Granada, Comares, 2006, pp. 167 – 190.

Romeo Casabona, C.M., "De los delitos informáticos al cibercrimen", en F. Pérez Álvarez (edit.), *Universitas vitae. Homenaje a Ruperto Núñez Barbero*, 1ª ed., Salamanca, Ediciones Universidad de Salamanca, 2007, pp. 649 – 670.

Romeo Casabona, C.M., "Conocimiento científico y causalidad en el Derecho Penal", en C.M. Romeo Casabona y F. Guanarteme Sánchez Lázaro (eds.), *La adaptación del derecho penal al desarrollo social y tecnológico,* Granada, Comares, 2010, pp. 117 – 145.

Romeo Casabona, C.M., "Derecho penal y libertades de expresión y comunicación en Internet", en C.M. Romeo Casabona y F. Guanarteme Sánchez Lázaro (eds.), *La adaptación del derecho penal al desarrollo social y tecnológico,* Granada, Comares, 2010, pp. 299 – 330.

Romeo Casabona, C.M. et al., "Informe sobre los intentos de adaptación del Derecho Penal al desarrollo social y tecnológico: líneas de investigación y conclusiones", ", en C.M. Romeo Casabona y F. Guanarteme Sánchez Lázaro (eds.), *La adaptación del derecho penal al desarrollo social y tecnológico,* Granada, Comares, 2010, pp. 489 - 586.

Romeo Casabona, C.M., *El médico y el Derecho Penal. Tomo I. La actividad curativa. Licitud y responsabilidad penal,* 1ª ed., Santa Fe, Rubinzal – Culzoni, 2011.

Romeo Casabona, C.M., *El médico y el Derecho Penal. Tomo II – Volumen I. Los problemas penales actuales de la Biomedicina,* 1ª ed., Santa Fe, Rubinzal – Culzoni, 2011.

Romeo Casabona, C.M., "La penetración del Derecho penal económico en el marco jurídico europeo: los delitos contra los sistemas de información", en C.M. Romeo Casabona y F. Flores Mendoza (eds.), *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica,* Granada, Comares, 2012, pp. 331 – 373.

Romeo Casabona, C.M. et al., "Informe sobre los nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica. Líneas de investigación y conclusiones", en C.M. Romeo Casabona y F. Flores Mendoza (eds.), *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica,* Granada, Comares, 2012, pp. 657 – 847.

Romeo Casabona, C.M., "Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad", *Revista Penal,* no. 42, 2018, pp. 165 – 179.

Romeo Casabona, C.M., "Criminal responsability of robots and autonomous artificial intelligent systems?", *Comunicaciones en propiedad industrial y derecho de la competencia*, no. 91, 2020, pp. 167 – 188.

Romeo Casabona, C.M., "Delitos contra el patrimonio y el orden socioeconómico II. Defraudaciones, insolvencias punibles, alteración de precios en concursos y subastas públicas y daños", en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho Penal, Parte Especial*, 2ª ed., Granada, Comares, 2022, pp. 373 – 392.

Romeo Casabona, C.M., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho Penal, Parte Especial*, 2ª ed., Granada, Comares, 2022, pp. 265 – 299.

Roth, K., “Implications for Virtual Worlds: A Comparative Study of United Kingdom, United States and Australia on Networks Readiness, Government Investment and Cyber-security”, *Journal of Virtual Worlds Research*, vol. 2, no. 5, 2010, pp. 1 – 13.

Rubio Viñuela, Y., “Los claroscuros de la ciberseguridad”, *Revista Tribuna norteamericana,* no. 30, 2019, pp. 16 – 21.

Rueda Martín, M.ª A., *Protección penal de la intimidad personal e informática: los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código penal,* 1ª ed., Barcelona, Atelier, 2004.

Rueda Martín, M.ª A., “Los ataques contra los sistemas informáticos: conductas de hacking. Cuestiones político-criminales”, en C.M. Romeo Casabona y F. Guanarteme Sánchez Lázaro (eds.), *La adaptación del derecho penal al desarrollo social y tecnológico,* 1ª ed., Granada, Comares, 2010, pp. 348 – 379.

Rueda Martín, M.ª A., *La nueva protección de la vida privada y de los sistemas de información en el Código penal,* 1ª ed., Barcelona, Atelier, 2018.

Rueda Martín, M.ª A., “La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español”, *Diritto Penale Contemporaneo: Rivista Trimestrale*, no. 3, 2020, pp. 199 – 216.

Rueda Martín, M.ª A., “Los ataques de denegación de servicios como ciberdelito en el Código Penal español”, *Revista Penal*, no. 49, 2022, pp. 183 – 216.

Ruiz Domínguez, F., “Ciberbioseguridad: implicaciones técnico-jurídicas para la perfecta desconocida en seguridad y defensa”, *Bie3: Boletín IEEE*, no. 22, 2021, pp. 660 – 674.

Ruiz Marco, F., *Los delitos contra la intimidad: especial referencia a los ataques cometidos a través de la informática,* 1ª ed., Madrid, Colex, 2001.

Rusell, S.J. y Norvig, P., *Inteligencia Artificial. Un Enfoque Moderno*, 2ª edición, Madrid, Pearson Educación, 2004.

Rutkowski, A., "Public international law of the international telecommunication instruments: cyber security treaty provisions since 1850", *Info,* vol. 13, no. 1, 2011, pp. 13 – 31.

Sáinz-Cantero Caparrós, J.E., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I)", en L. Morillas Cueva (dir.), *Sistema de Derecho Penal. Parte Especial*, 4ª ed., Madrid, Dykinson, 2021, pp. 343 – 366.

Saiz Blanco, M., "Seguridad de la información", en O. Tejerina (coord.), *Aspectos jurídicos de la ciberseguridad*, Madrid, Ra-Ma, 2020, pp. 23 – 101.

Salat Paisal, M., *La relación entre Derecho penal y Derecho administrativo sancionador. Una propuesta basada en la idea de la prisión como ultima ratio*, 1ª ed., Valencia, Tirant lo Blanch, 2021.

Sales, N.A., "Privatizing Cybersecurity", *U.C.L.A. Law Review,* vol. 65, no. 3, 2018, pp. 620 – 689.

Salvador Cerqueda, A., "Gestión de incidentes de seguridad desde la perspectiva de la protección de datos y los secretos empresariales", en S. Pereira Puigvert y F. Ordoñez Ponz (dirs.), *Investigación y proceso penal en el siglo XXI. Nuevas tecnologías y protección de datos*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021, pp. 361 – 376.

Salvadori, I., "Agentes artificiales, opacidad tecnológica y distribución de la responsabilidad penal", *Cuadernos de Política Criminal. Segunda época,* no. 133, 2021, pp. 137 – 174.

Sánchez-Ostiz, P., *A vueltas con la Parte Especial. Estudios de Derecho penal*, 1ª ed., Barcelona, Atelier, 2020.

Sánchez Bernal, J., “El bien jurídico protegido en el delito de estafa informática”, *Cuadernos del Tomás: revista de estudios del Colegio Mayor Tomás Luis de Victoria,* no. 1, 2009, pp. 105 – 121.

Sanchini, V. y Marelli, L., “Data Protection and Ethical Issues in European P5 eHealth”, en G. Pravettoni y S. Triberti (eds.), *P5 eHealth: An Agenda for the Health Technologies of the Future*, 1ª ed., Cham, Springer, 2020, pp. 173 – 189.

Sanz Morán, A. J., “Reflexiones sobre el bien jurídico”, en J.C. Carbonell Mateu, J.L. González Cussac, y E. Orts Berenguer (dirs.), *Constitución, derechos fundamentales y sistema penal. Semblanzas y estudios con motivo del setenta aniversario del profesor Tomás Salvador Vives Antón. Tomo II*, 1ª ed., Valencia, Tirant lo Blanch, 2009, pp. 1753 – 1770.

Schallbruch, M. y Skierka, I., *Cybersecurity in Germany,* 1ª ed., Cham, Springer, 2018.

Schatz, D., Bashroush, R. y Wall, J., “Towards a more representative definition of cyber security”, *The Journal of Digital Forensics, Security and Law,* vol. 12, no. 2, 2017, pp. 53 – 74.

Segura Serrano, A., “Ciberseguridad y Derecho Internacional”, *Revista española de derecho internacional,* vol. 69, no. 2, 2017, pp. 291 – 299.

Serrano Durbá, C., “Garantías de seguridad en los servicios de computación en nube”, en D. Canals Ametller (dir.), *Ciberseguridad: un nuevo reto para el Estado y los Gobiernos Locales*, 1ª ed., Madrid, Wolters Kluwer, 2021, pp. 321 – 346.

Serrano Ferrer, M.ª P., *El reflejo de las nuevas tecnologías en el Derecho penal y otros destellos*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2016.

Serrano Ferrer, M.ª P., *Derecho penal y nuevas tecnologías*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021.

Serrano Gómez, A. et al., *Curso de Derecho Penal. Parte Especial*, 6ª ed., Madrid, Dykinson, 2021.

Shires, J., "Cybersecurity Governance in the GCC", en R. Ellis y V. Mohan (eds.), *Rewired: Cybersecurity Governance,* Hoboken, NJ, Wiley, 2019, pp. 19 – 36.

Shryock, T., "The growing cyber threat to physician practices", *Medical Economics,* vol. 96, no. 10, 2019, pp. 22 – 27.

Sikos, L.F., "The Formal Representation of Cyberthreats for Automated Reasoning", en L.F. Sikos y K. R. Choo (eds.), *Data Science in Cybersecurity and Cyberthreat Intelligence,* 1ª ed*.,* Cham, Springer, 2020, pp. 1 – 12.

Siracusano, F., "The European Investigation Order for Evidence Gathering Abroad", en T. Rafaraci y R. Belfiore (eds.), *EU Criminal Justice: Fundamental Rights, Transnational Proceedings and the European Public Prosecutor´s Office,* Cham, Springer, 2019, pp. 85 – 101.

Sola Reche, E., "Principio de precaución y tipicidad penal", en C.M. Romeo Casabona (edit.), *Principio de precaución, Biotecnología y Derecho*, Granada, Comares, 2004, pp. 475 – 491.

Solé Pascual, C. y Hernández, A., "Estrategias nacionales de ciberseguridad en el mundo", *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones,* no. 66, 2014, pp. 34 – 37.

Sospedra Navas, F.J. y Beltrán Miralles, S., "Cuestiones generales", en F.J. Sospedra Navas (dir.), *Prácticum Proceso Penal 2022*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2021, pp. 27 – 154.

Souto García, E.M., *Los Delitos de Hurto y Robo,* 1ª ed., Valencia, Tirant lo Blanch, 2017.

Stahn, C., *A Critical Introduction to International Criminal Law,* 1ª ed., Cambridge, Cambridge University Press, 2019.

Stallings, W., *Fundamentos de Seguridad en Redes. Aplicaciones y Estándares,* 2ª ed., Madrid, Pearson Educación, 2004.

Stefánsson, H.O., "On the Limits of the Precautionary Principle", *Risk Analysis,* vol. 39, no. 6, 2019, pp. 1204 – 1222.

Stitilis, D., Pakutinskas, P., y Malinauskaite, I., "EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis", *Security Journal*, vol. 30, no. 4, 2016, pp. 1151 – 1168.

Stoddart, K., "UK cyber security and critical national infrastructure protection", *International Affairs,* vol. 92, no. 5, 2016, pp. 1079 – 1105.

Suárez-Mira Rodríguez, C., Judel Prieto, A., y Piñol Rodríguez, J.R., *Manual de Derecho Penal. Parte Especial. Tomo II,* 8ª ed., Cizur Menor, Navarra, Aranzadi, 2020.

Supervisor Europeo de Protección de Datos, *Shaping a Safer Digital Future. The EDPS Strategy 2020 - 2024*, Bruselas, Supervisor Europeo de Protección de Datos, 2021.

Taylor, M.J. y Whitton, T., "Public Interest, Health Research and Data Protection Law: Establishing a Legitimate Trade-Off between Individual Control and Research Access to Health Data", *Laws,* vol. 9, no. 1, 2020, pp. 1 – 24.

Taylor, M.J. y Wilson, J., "Reasonable Expectations of Privacy and Disclosure of Health Data", *Medical Law Review,* vol. 27, no. 3, 2019, pp. 432 – 460.

Tejada de la Fuente, E. y Martín Martín de la Escalera, A.M., "Cibercrimen", en A.M. Díaz Fernández (dir.), *Conceptos fundamentales de inteligencia,* Valencia, Tirant lo Blanch, 2016, pp. 37 – 44.

Tejada de la Fuente, E., "Introducción: ciberseguridad y ciberdelincuencia: respuestas desde el estado de derecho. La armonización legislativa transnacional, en particular: las medidas de investigación criminal en la

Convención de Budapest", en J.I. Zaragoza Tejada (coord.), *Investigación tecnológica y derechos fundamentales: comentarios a las modificaciones introducidas por la Ley 13/2015,* Cizur Menor, Navarra, Aranzadi, 2017, pp. 25 – 72.

Tejerina Rodríguez, O., "Criptoactivos y ciberseguridad", en M. Barrio Andrés (dir.), *Criptoactivos. Retos y desafíos* normativos, 1ª ed., Madrid, Wolters Kluwer, 2021, pp. 293 – 309.

Tomás-Valiente Lanuza, C., "Artículo 197 bis", en M. Gómez Tomillo (dir.), *Comentarios prácticos al Código Penal. Tomo II. Los delitos contra las personas. Artículos 138 – 233*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, pp. 673 – 678.

Tomás-Valiente Lanuza, C., "Artículo 413", en M. Gómez Tomillo (dir.), *Comentarios prácticos al Código Penal. Tomo V. Delitos de falsedades, contra la Administración Pública y contra la Administración de Justicia. Artículos 386 – 471 bis*, 1ª ed., Cizur Menor, Navarra, Aranzadi, 2015, pp. 253 – 256.

Tomás-Valiente Lanuza, C., "Delitos patrimoniales y contra el orden socioeconómico. Sección 15. Delitos relativos a la propiedad intelectual", en F. Molina Fernández (coord.), *Memento Práctico de Derecho Penal 2021*, Madrid, Francis Lefebvre, 2020, pp. 1421 – 1436.

Topol, E.J., *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again,* 1ª ed., New York, NY, Hachette Book Group, 2019.

Topol, E.J., "High-performance medicine: the convergence of human and artificial intelligence", *Nature Medicine*, vol. 25, no. 1, 2019, pp. 44 – 56.

Torres-Soriano, M.R., "Cómo contener a un califato virtual", *Cuadernos de estrategia,* no. 180, 2016, pp. 167 – 194.

Tosoni, L., “Rethinking Privacy in the Council of Europe´s Convention on Cybercrime”, *Computer Law & Security Review,* vol. 34, no. 6, 2018, pp. 1197 – 1214.

Tschider, C.A., *International Cybersecurity and Privacy Law in Practice,* 1ª ed., Alphen aan den Rijn, Kluwer Law International B.V., 2018.

Unión Internacional de Telecomunicaciones, *Global Cybersecurity Index (GCI) 2018*, Ginebra, Unión Internacional de Telecomunicaciones, 2018.

Urbas, G., *Cybercrime Legislation, Cases and Commentary,* 1ª ed., Chatswood, NSW, LexisNexis Butterworths, 2015.

Urruela Mora, A., “Derecho penal militar”, en C.M. Romeo Casabona, E. Sola Reche y M.A. Boldova Pasamar (coords.), *Derecho Penal, Parte Especial*, 2ª ed., Granada, Comares, 2022, pp. 911 – 920.

Valentín Carrera, L. y Rego, M., “La innovación en ciberseguridad desde la perspectiva de los centros tecnológicos”, *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, vol. 30, no. 145, 2021, p. 137.

Vallejo Casas, J.A. y Rodríguez Cáceres, E., “Inteligencia Artificial y Medicina Nuclear. Hoy ya es futuro”, *Revista Española de Medicina Nuclear e Imagen Molecular*, vol. 41, no. 1, 2022, pp. 1 – 2.

Valls Prieto, J., *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial,* 1ª ed., Madrid, Dykinson, 2017.

Valls Prieto, J., *Inteligencia artificial, Derechos Humanos y bienes jurídicos*, 1ª ed., Cizur Menor, Aranzadi, 2021.

Van de Poel, I., “Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security”, en M. Christen, B. Gordijn, M. Loi (eds.), *“The Ethics of Cybersecurity”,* Cham, Springer, 2020, pp. 45 – 71.

Van Dine, A., “When is Cyber Defense a Crime? Evaluating Active Cyber Defense Measures Under the Budapest Convention”, *Chicago Journal of International Law,* vol. 20, no.2, 2020, pp. 530 – 564.

Van Oorschot, P.C., *Computer Security and the Internet: Tools and Jewels,* 1ª ed., Cham, Springer, 2020.

Van Wynsberghe, A., *Healthcare Robots: Ethics, Design and Implementation*, 1ª ed., Burlington, VT, Ashgate, 2015.

Vasiliev, S., “The Crises and Critiques of International Criminal Justice”, en K.J. Heller et al. (eds.), *The Oxford Handbook of International Criminal Law,* Oxford, Inglaterra, Oxford University Press, 2020, pp. 626 – 651.

Velasco Núñez, E., *Delitos cometidos a través de Internet. Cuestiones* procesales, 1ª ed., Madrid, Wolters Kluwer, 2010.

Velasco Núñez, E., *Delitos tecnológicos. Cuestiones penales y procesales*, 1ª ed., Madrid, Wolters Kluwer, 2021.

Velasco Núñez, E. y Sanchís Crespo, C., *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*, 1ª ed., Valencia, Tirant lo Blanch, 2019.

Velasco San Martín, C., *Jurisdicción y Competencia Penal en Relación al Acceso Transfronterizo en Materia de Ciberdelitos,* 1ª ed., Valencia, Tirant lo Blanch, 2016.

Ventre, D., *Artificial Intelligence, Cybersecurity and Cyber Defense,* 1ª ed, Londres, Wiley, 2020.

Veresha, R.V., “Preventive measures against computer related crimes: Approaching an individual”, *Informatologia,* vol. 51, no. 3-4, 2018, pp. 189 – 199.

Von der Leyen, U. et al., “Cómo evolucionarán los ciberataques en 2022”, *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, vol. 31, no. 148, 2022, pp. 91 – 147.

Von Solms, R. y Van Niekerk, J., “From information security to cyber security”, *Computers & Security,* no. 38, 2013, pp. 97 – 102.

Vos, J., *Quantum Computing in Action*, Shelter Island, NY, Manning Publications, 2020.

Wales, E., “Draft Council of Europe Cybercrime Convention Upsets Civil Rights Bodies”*, Computer Fraud & Security,* no. 12, 2000, p. 7.

Walsh, P.F., *Intelligence, Biosecurity and Bioterrorism,* 1ª ed., Londres, Palgrave Macmillan, 2018.

Warner, M., “Cybersecurity: A Pre-History”, *Intelligence and National Security,* vol. 27, no. 5, 2012, pp. 781 – 799.

Weber, A.M., “The Council of Europe´s Convention on Cybercrime”, *Berkeley Technology Law Journal,* vol. 18, no. 1, 2003, pp. 425 – 446.

Weber, R.H. y Studer, E., “Cybersecurity in the Internet of Things: Legal aspects”, *Computer Law & Security Review*, no. 32, 2016, pp. 715 – 728.

Wells, F., “Hacked off: How Germany and the United States are Dealing with the Continuous Threat of Cyber Attacks”, *National Security Law Brief,* vol. 10, no. 1, 2020, pp. 343 – 473.

Welzel, H., *Derecho Penal. Parte General*, Buenos Aires, Roque Depalma Editor, 1956.

Wertheim, S., “Tips for Fighting off Cybercrime in 2020”, *The CPA Journal,* vol. 90, no. 3, 2020, pp. 64 – 66.

Whitfill, J., “Data Security and Patient Privacy”, en B.F. Branstetter IV (edit.), *Practical Imaging Informatics: Foundations and Applications for Medical Imaging*, 2ª ed., Cham, Springer, 2021, pp. 119 – 130.

Willems, E., *Cyberdanger: Understanding and Guarding Against Cybercrime*, 1ª ed., Cham, Springer, 2019.

Williams, P.A.H. et al., “Working as a Health Cybersecurity Specialist”, en K. Butler – Henderson, K. Day, y K. Gray (eds.), *The Health Information Workforce: Current and Future Developments*, Cham, Springer, 2021, pp. 225 – 236.

Williams, P.A.H. y Woodward, A.J., “Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem”, *Medical Devices: Evidence and Research*, vol. 8, 2015, pp. 305 – 316.

Witkowski, E. y Ward, T., “Artificial Intelligence Assisted Surgery”, en A. Bohr y K. Memarzadeh (eds.), *Artificial Intelligence in Healthcare,* 1ª ed., Londres, Elsevier, 2020, pp. 179 – 202.

Yaacoub, J.A. et al., “Securing internet of medical things systems: Limitations, issues and recommendations”, *Future Generation Computer Systems*, vol. 105, 2020, pp. 581 – 606.

Zafra Espinosa de los Monteros, R., “La bunkerización del Espacio de Libertad, Seguridad y Justicia”, en M.I. González Cano (coord.), *Integración europea y justicia penal*, Valencia, Tirant lo Blanch, 2018, pp. 165 – 206.

Zaldívar Robles, J., “La protección penal del derecho a la intimidad”, *Teoría y derecho: revista de pensamiento jurídico,* no. 19, 2016, pp. 162 – 188.

Zárate, C., “Hacia un marco normativo supranacional en materia de ciberseguridad”, *Actualidad jurídica Aranzadi,* no. 916, 2016, p. 12.

Zarzalejos Nieto, J., “La competencia de los tribunales penales”, en J. Banacloche Palao y J. Zarzalejos Nieto (eds.), *Aspectos fundamentales de Derecho procesal penal*, 5ª ed., Madrid, Wolters Kluwer, 2021, pp. 45 – 80.