CAPÍTULO X

La tutela de la ciberseguridad a través del derecho penal

Alexandre Casadevall Portas
Fiscal de la Fiscalía Provincial de Madrid

SUMARIO. 1. Introducción. 2. El derecho penal y la ciberseguridad. 2.1. La necesidad de un derecho penal eficaz contra la ciberdelincuencia. 2.2. Ciberdelincuencia transnacional, respuesta penal internacional. *2.2.1. Convenio de Budapest. 2.2.2. Normativa de la Unión Europea. 2.2.3. Otras iniciativas*. **3. Ciberdelitos.** 3.1. Concepto y tipologías de ciberdelitos. 3.2. Análisis de los delitos contra la ciberseguridad en el Código Penal. *3.2.1. Consideraciones previas. 3.2.2. Delitos de descubrimiento y revelación de secretos. 3.2.3. Delitos de daños informáticos. 3.2.4. Estafas informáticas. 3.2.5. Ciberterrorismo*. **4. Conclusión. 5. Bibliografía.**

1. Introducción

Vivimos en un mundo digital. La realidad diaria nos demuestra que gran parte de nuestra vida se desarrolla ya en un ámbito virtual, el ciberespacio. En este espacio las personas nos relacionamos y comunicamos las unas con las otras, trabajamos, compramos, realizamos operaciones financieras, contratamos servicios, nos informamos, nos expresamos... Obviamente existen diferencias en el grado de uso de las nuevas tecnologías, pero hoy en día es difícil encontrar a alguien que no las utilice de forma diaria de un modo u otro. Esto no solo es predicable de las personas físicas. Sería impensable el funcionamiento de empresas y Administraciones públicas sin estas

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

nuevas tecnologías. Y la tendencia es que este uso siga en aumento, dadas sus ventajas y el continuo desarrollo tecnológico.

Sin embargo, imaginemos que las pérdidas sufridas por las entidades financieras por los fraudes informáticos superaran a los beneficios que les supusiera la banca digital. O que hubiera tantas intrusiones informáticas que fuera altamente probable que cualquier información almacenada en nuestros dispositivos electrónicos terminara en manos de terceras personas. O que fueran diarios los ciberataques que inutilizaran infraestructuras críticas, desde aeropuertos a centrales hidroeléctricas. No estamos hablando de un escenario remoto: el Informe Anual de Seguridad Nacional 2023 recoge como principal preocupación entre los riesgos y amenazas las campañas de desinformación y el empleo del ciberespacio para fines irregulares. Para seguir disfrutando de las ventajas que ofrecen las nuevas tecnologías es necesario tener redes y sistemas suficientemente seguros si no queremos que su uso entrañe riesgos inasumibles. Aquí entra en acción la ciberseguridad.

Podemos definir la ciberseguridad como todas las actividades necesarias para la protección de las redes y los sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas[1]. La importancia de este objetivo de redes y sistemas seguros ha motivado las distintas iniciativas que se vienen desarrollando desde hace años tanto en el ámbito europeo como en el nacional, y que han sido analizadas en capítulos anteriores. Estas iniciativas conllevan medidas en todos los ámbitos y con actores muy diversos, pero en cualquier caso destacan la necesidad de un planteamiento global en materia de seguridad de las redes y de la información. De este planteamiento global forma parte relevante el derecho penal.

2. El derecho penal y la ciberseguridad

La finalidad del derecho penal es proteger la sociedad. Para hacerlo define qué conductas se consideran delito, y determina las penas o medidas de seguridad que deben imponerse a sus responsables. Estas conductas que se definen y castigan son aquellas que lesionan de manera efectiva o potencial bienes jurídicos que el legislador valora esenciales para el funcionamiento de nuestra sociedad. Para protegerlos utiliza el poder punitivo del Estado, por considerar que los restantes medios de tutela y sanción son ineficaces o insuficientes.

1. Artículo 2.1) 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) n.º 526/2013 ("Reglamento sobre la Ciberseguridad").

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Por lo tanto, el derecho penal se configura como un instrumento de lucha contra la criminalidad informática que castiga aquellas conductas que el legislador considera que lesionan o ponen en peligro bienes jurídicos relacionados con la seguridad en el ciberespacio.

Este castigo penal tiene, por una parte, una finalidad retributiva, sancionando a quien ha cometido una conducta prohibida, para compensar el mal que ha causado con su conducta. Sin embargo, cumple además una importante función preventiva: la amenaza del castigo penal evita en muchos casos que se cometan delitos por parte de quienes, teniendo ocasión de delinquir, deciden finalmente no hacerlo por temor a las penas que se les puedan imponer si son descubiertos y condenados. El derecho penal contribuye así de forma esencial a la ciberseguridad.

2.1. La necesidad de un derecho penal eficaz contra la ciberdelincuencia

Los datos estadísticos y la propia experiencia práctica diaria ponen de manifiesto que la ciberdelincuencia se encuentra en clara expansión. El Informe sobre la cibercriminalidad en España 2023 del Ministerio del Interior constata el aumento de los delitos informáticos en el periodo comprendido entre 2019 y 2023. Destaca, por una parte, que en 2023 ha habido un 26 % más de hechos delictivos conocidos con respecto al año 2022 (pasando de 374 737 a 472 125), y, por otra, que el porcentaje de delitos informáticos respecto de la delincuencia en general ha pasado del 9,9 % en 2019 al 19,2 % en 2023.

Este crecimiento se explica en gran parte porque las nuevas tecnologías han abierto un gran abanico de posibilidades para cometer delitos de la más diversa índole. En algunos casos se trata de nuevas conductas que han aparecido a raíz del desarrollo digital. En otros se trata de delitos que ya existían, pero que han pasado a cometerse usando herramientas informáticas, aprovechando las ventajas que estas ofrecen.

Resulta especialmente preocupante que el porcentaje de esclarecimiento de estos delitos esté disminuyendo, según observa el mismo informe (15,9 % en 2021, 14,6 % en 2022 y 13,5 % en 2023). La estadística muestra que, a pesar de los esfuerzos de las autoridades policiales y judiciales, la mayor parte de los ciberdelitos quedan impunes. Esto compromete la eficacia del derecho penal como instrumento de prevención, que depende en gran medida de la posibilidad de identificar, enjuiciar y condenar a los autores de los delitos.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

2.2. Ciberdelincuencia transnacional, respuesta penal internacional

La ciberdelincuencia tiene particularidades que dificultan una respuesta penal efectiva[2]. Junto a la constante aparición de nuevas modalidades delictivas a medida que se producen avances técnicos y a la capacidad de los autores de ocultar su identidad por diversos mecanismos, destaca el carácter transfronterizo de muchos de los delitos cometidos a través del ciberespacio. Ello hace que la persecución penal sea muy compleja.

De entrada, se exige la especialización de las autoridades policiales y judiciales que deberán investigar y enjuiciar estos delitos. Esta especialización se viene desarrollando desde hace años, y en ella cabe destacar la del Ministerio Fiscal, con la decisiva labor llevada a cabo por la Unidad de Criminalidad Informática de la Fiscalía General del Estado y por las secciones de Criminalidad Informática de las distintas Fiscalías. Pero, además, las autoridades nacionales se enfrentan al obstáculo de que frecuentemente autores, víctimas o pruebas se encuentran en otros países, con un ordenamiento jurídico distinto.

Es por ello que la respuesta penal contra la ciberdelincuencia exige trabajar siguiendo dos grandes líneas de actuación íntimamente vinculadas: la primera, la evolución ágil y efectiva de la legislación sobre la materia, procurando aproximar los ordenamientos jurídicos de los distintos Estados; la segunda, reforzar y agilizar los mecanismos de cooperación internacional. A continuación, analizaremos algunas de las iniciativas más relevantes en esta respuesta internacional, donde destaca la reciente aprobación de varios instrumentos llamados a mejorar de forma significativa la lucha contra la ciberdelincuencia.

2.2.1. Convenio de Budapest

El Convenio sobre la ciberdelincuencia del Consejo de Europa de 2001, conocido como Convenio de Budapest, desempeña un papel central en la lucha contra la criminalidad informática. Fue el primer tratado internacional en centrarse específicamente en la cibercriminalidad y en la prueba

2. Un ejemplo de estas particularidades es la tendencia conocida como *Crime as a Service* o *CaaS*, que consiste en subcontratar servicios ilegales: los ciberdelincuentes alquilan o venden *malware* u otros servicios a terceros para que estos puedan cometer delitos informáticos. Esto permite que personas sin conocimientos técnicos puedan lanzar ataques informáticos que excedan de sus capacidades, y al mismo tiempo contribuye a que dentro de la ciberdelincuencia se produzca una especialización en función de los servicios específicos que se comercialicen.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

electrónica. A pesar de tratarse de un convenio del Consejo de Europa está abierto a terceros países, y en noviembre de 2024 los Estados parte ascendían a un total de 76 (entre los que destacan veintiséis de la Unión Europea y los Estados Unidos). Además, su influencia es patente en las legislaciones nacionales sobre la materia de otros muchos Estados. Todo ello contribuye a que siga siendo, aún hoy, el instrumento internacional de referencia en la lucha contra la ciberdelincuencia. Precisamente en el Convenio de Budapest se observan las dos líneas de actuación principales a las que nos referíamos anteriormente.

Primero, contiene un listado de delitos cometidos contra sistemas informáticos o utilizando tales sistemas y una serie de medidas de investigación tecnológica que los Estados deberán introducir en sus legislaciones nacionales. Los delitos son contra datos y sistemas informáticos (acceso e interceptación ilícitos, interferencia en datos y sistemas, abuso de los dispositivos), falsificación y fraudes informáticos, relacionados con la pornografía infantil y contra la propiedad intelectual. A ellos se añadieron en 2003 otros delitos de índole racista y xenófoba cometidos por medio de sistemas informáticos[3]. Esta regulación ha tenido gran influencia en la posterior configuración de tales delitos en la legislación europea y nacional.

En segundo lugar, el Convenio de Budapest regula distintos mecanismos de cooperación internacional como la extradición, la asistencia mutua, el intercambio espontáneo de información, la conservación de datos o una red 24/7 de puntos de contacto.

Aunque el Convenio de Budapest ha sido realmente exitoso al definir los delitos informáticos, la realidad ha demostrado que sus mecanismos de cooperación internacional no son suficientes. La ciberdelincuencia no ha dejado de aumentar, y en muchos procedimientos penales hoy es necesario recabar pruebas electrónicas. Sin embargo, los instrumentos de asistencia judicial tradicionales son lentos y complejos e impiden una investigación rápida de los ciberdelitos, cuyo esclarecimiento dependerá muchas veces de información volátil, que se puede ver alterada o eliminada en un corto lapso de tiempo (ya sea por el autor del delito o por las empresas proveedoras de servicios en virtud de la normativa sobre conservación de datos). Además, la realidad del mundo digital revela el papel central de unas pocas grandes compañías proveedoras de servicios, la mayor parte de ellas ubicadas en

3. Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo el 28 de enero de 2003.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Estados Unidos, que son las que frecuentemente tendrán la información requerida en las investigaciones por delitos informáticos. Esta situación motivó que en 2022 los Estados parte firmaran un Segundo Protocolo adicional relativo a la cooperación reforzada y la revelación de pruebas electrónicas[4]. Entre otras novedades el protocolo incluye mecanismos para una asistencia mutua más eficiente entre las autoridades, regula la cooperación directa entre las autoridades y los proveedores de servicio y una cooperación especialmente rápida en supuestos de emergencia, y prevé la transmisión electrónica de las solicitudes.

2.2.2. Normativa de la Unión Europea

En el ámbito de la Unión Europea también se han hecho importantes esfuerzos para ofrecer una respuesta penal efectiva contra la ciberdelincuencia. La necesidad de armonización normativa en esta materia ya se puso de manifiesto en el Consejo Europeo de Tampere de 1999, y ha motivado la aprobación de numerosos instrumentos para que los Estados miembros aproximen sus legislaciones penales en la lucha contra distintas manifestaciones de la ciberdelincuencia, como los ataques contra los sistemas de información[5], los abusos sexuales a menores, la pornografía infantil[6] y los fraudes informáticos[7]. Estos instrumentos han determinado la regulación actual de esta materia en nuestro ordenamiento jurídico, y siguen parámetros similares a los del Convenio de Budapest.

Junto a ello, el espacio de libertad, seguridad y justicia que supone la Unión Europea determina que la cooperación judicial penal, basada en el principio de reconocimiento mutuo de las resoluciones judiciales, sea espe-

4. Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas, hecho en Estrasburgo el 12 de mayo de 2022.

5. Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, y Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

6. Decisión marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, y Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.

7. Decisión marco 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, y Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión marco 2001/413/JAI del Consejo.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

cialmente intensa, con múltiples instrumentos con los que las autoridades judiciales se auxilian entre sí, como las órdenes europeas de detención y entrega y las órdenes europeas de investigación. En la cooperación europea contra la ciberdelincuencia no puede olvidarse el importante papel de Europol, Eurojust, el proyecto SIRIUS (de acceso transfronterizo a la prueba electrónica), la Red Judicial Europea (EJN) y la Red Judicial Europea sobre Ciberdelincuencia (EJCN).

El fenómeno de la ciberdelincuencia ha evidenciado, sin embargo, que estos mecanismos de cooperación resultan insuficientes, y que es imprescindible agilizar las investigaciones penales en las que intervenga prueba electrónica. En un planteamiento similar al del Segundo Protocolo adicional al Convenio de Budapest, se ha concluido que hay que reforzar los mecanismos de cooperación entre autoridades y permitir la cooperación directa con los proveedores de servicio. Para lograrlo, se ha elaborado un paquete legislativo sobre pruebas electrónicas (el conocido como *E-Evidence Package*), que parte de estas premisas y de la idea central de que los proveedores de servicios que ofrezcan servicios en la Unión Europea deben atender las órdenes directas de las autoridades de los Estados miembros para preservar y entregar pruebas electrónicas. Este paquete legislativo consta de dos instrumentos. El primero es un reglamento[8] que regula la orden europea de entrega y la orden europea de conservación, a través de las cuales la autoridad de un Estado miembro podrá ordenar la entrega/preservación de pruebas electrónicas vinculadas a una investigación criminal a los proveedores que ofrezcan sus servicios en territorio de la Unión, con independencia del lugar donde se encuentren ubicados los datos. El segundo es una directiva[9] que, complementando el anterior, obliga a los proveedores de servicios a designar al menos un establecimiento o representante legal en un Estado miembro (que será el responsable de recibir y ejecutar las órdenes europeas de entrega y de conservación) y contiene las normas para tal designación.

8. Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales.

9. Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

2.2.3. Otras iniciativas

La indicada necesidad de armonizar los ordenamientos jurídicos y reforzar los mecanismos de cooperación internacional para luchar de forma eficaz contra la ciberdelincuencia es una tendencia compartida a nivel global.

Estados Unidos aprobó en 2018 la conocida como *CLOUD Act* (*Clarifying Lawful Overseas Use of Data Act*), que facilita el acceso a la prueba electrónica en poder de las grandes compañías proveedoras de servicios estadounidenses por parte de las autoridades judiciales extranjeras en investigaciones criminales. En base a esta norma, los Estados Unidos ya han alcanzado acuerdos con el Reino Unido y Australia para dicho acceso, y están negociando con Canadá y la Unión Europea.

Además, en diciembre de 2024, la Asamblea General de las Naciones Unidas adoptó la Convención de las Naciones Unidas contra la Ciberdelincuencia, que se abrirá a la firma en 2025. El texto reproduce en gran parte las previsiones del Convenio de Budapest, y debería contribuir a mejorar la lucha contra la ciberdelincuencia a nivel mundial, extendiendo un marco normativo común a nuevos países.

3. Ciberdelitos

3.1. Concepto y tipologías de ciberdelitos

La primera cuestión que debemos plantearnos es qué es un ciberdelito. Según el *Diccionario panhispánico del español jurídico*, un ciberdelito o delito informático es una infracción penal cometida utilizando un medio o un instrumento informático. Por lo tanto, lo que caracteriza a estos delitos es su forma comisiva a través de las tecnologías de la información y la comunicación.

Dentro de los delitos informáticos debemos distinguir dos tipologías generales. Por un lado, tenemos conductas que afectan directamente a la seguridad de los datos, redes y sistemas de información. Por otro, hay comportamientos que no atacan directamente a redes y sistemas, pero que se ejecutan a través de las nuevas tecnologías, aprovechando las ventajas que estas ofrecen y que afectan a los más diversos bienes jurídicos. Esta

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

dualidad se puso ya de manifiesto desde los inicios de la lucha contra la ciberdelincuencia[10], y persiste en la actualidad[11].

En este capítulo nos centraremos en la primera tipología: los delitos que atacan la seguridad de una red o un sistema informáticos, afectando así a su disponibilidad, integridad o confidencialidad, y que son propiamente los relativos a la ciberseguridad. Ampliar nuestro análisis al segundo tipo de delitos exigiría un espacio mayor al disponible en este capítulo, puesto que el abanico de conductas es enorme: incluye delitos incluidos en el Convenio de Budapest y que han sido tradicionalmente tratados como delitos informáticos (por ejemplo, los delitos relacionados con la pornografía infantil), pero también se extiende a cualquier conducta delictiva que se cometa usando las nuevas tecnologías, como enviar un mensaje amenazante a la víctima a través de *WhatsApp* o publicar una calumnia en redes sociales. Además, esta segunda tipología no afecta a la ciberseguridad propiamente dicha. Son delitos que hacen del ciberespacio un lugar menos seguro porque tienen lugar en él o a través de él, pero que no comprometen la protección de redes y sistemas informáticos.

3.2. Análisis de los delitos contra la ciberseguridad en el Código Penal

3.2.1. Consideraciones previas

Hemos delimitado nuestro ámbito de análisis a las conductas que afectan directamente a la ciberseguridad, es decir, a la confidencialidad, la integridad o la disponibilidad de los datos y sistemas de información. Al regular estas conductas el legislador no lo ha hecho de forma conjunta, agrupando en un mismo apartado todos los comportamientos que versan sobre la

10. La Instrucción 2/2011, de la Fiscalía General del Estado, sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de Criminalidad Informática de las Fiscalías, ya indicaba: "Efectivamente junto a tipos penales a través de los cuales el legislador ha protegido específicamente la seguridad de los datos, programas y/o sistemas informáticos, existen otras conductas ilícitas que, afectando a los más diversos bienes jurídicos, se planifican y ejecutan aprovechando las ventajas que ofrecen las nuevas tecnologías de la sociedad de la información y que presentan por tanto, a los efectos de su investigación y/o enjuiciamiento singularidades y dificultades similares a las de los primeramente indicados".

11. El Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, incluye entre los riesgos y amenazas a la seguridad nacional la vulnerabilidad del ciberespacio, y expone: "Se distinguen dos tipologías generales de amenazas en el ciberespacio. Por un lado, los ciberataques, entendidos como acciones disruptivas que actúan contra sistemas y elementos tecnológicos. Ejemplos de ello son los ataques de *ransomware* (secuestro de datos) o la denegación de servicios, entre otros. Y, por otro lado, el uso del ciberespacio para realizar actividades ilícitas, como el cibercrimen, el ciberespionaje, la financiación del terrorismo o el fomento de la radicalización".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

ciberseguridad. En cambio, ha optado por incluirlos en títulos o capítulos del Código Penal que ya existían, tomando en consideración el bien jurídico que considera afectado en última instancia (singularmente la intimidad y el patrimonio).

En nuestro análisis nos centraremos primero en los ataques más relevantes a la confidencialidad de datos y sistemas informáticos (delitos de descubrimiento y revelación de secretos) y a su integridad o disponibilidad (delitos de daños informáticos)[12]. A continuación, veremos las estafas informáticas, un fenómeno de gran relevancia por su volumen e impacto en el sistema económico, y que comprende diversas modalidades, entre las que destacan el empleo de manipulaciones informáticas y el uso fraudulento de datos, vinculados también con la ciberseguridad. Finalmente examinaremos el ciberterrorismo, que ataca a la confidencialidad, integridad o disponibilidad de datos y sistemas de información, pero que se caracteriza por perseguir unas finalidades específicas.

Antes de entrar en el examen de los delitos conviene aclarar dos términos que estos utilizan y cuya definición, contenida en la legislación comunitaria[13] y que no reproduce el Código Penal, es necesaria para comprender el tipo penal: sistema de información y datos informáticos.

Cuando hablamos de sistema de información, nos referimos a 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 a los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento.

Por su parte, los datos informáticos son toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función.

12. Estos delitos son examinados en profundidad por la Circular 3/2017, de 21 de septiembre, de la Fiscalía General del Estado, 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, que ha servido de referente para nuestro estudio de estas figuras delictivas.

13. Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

3.2.2. Delitos de descubrimiento y revelación de secretos

En términos generales, estos delitos tipifican conductas que suponen la vulneración de la intimidad personal y de la privacidad. En el ámbito de la ciberseguridad estos comportamientos se caracterizan por atacar la confidencialidad de datos informáticos y sistemas de información. En función de la forma de vulnerar esta confidencialidad, de si el objetivo era acceder a información y de la naturaleza de esta información, podremos distinguir entre diversas figuras delictivas. Estos delitos se castigan más gravemente si se cometen en el seno de una organización o un grupo criminal (artículo 197 quater), y también se sanciona en su caso a las personas jurídicas (197 quinquies).

- **Descubrimiento y revelación de secretos (197 CP)**

El papel central en materia de descubrimiento y revelación de secretos lo ocupa el artículo 197 del Código Penal. Este precepto, objeto de constantes críticas doctrinales y jurisprudenciales por su redacción[14], castiga en sus apartados primero y segundo conductas de naturaleza muy distinta y que puedan afectar a bienes jurídicos diversos[15].

Centrándonos en las principales conductas relacionadas con la seguridad de los datos y sistemas informáticos, en el apartado primero podemos identificar el apoderamiento de datos, documentos, mensajes de correo y efectos personales (que incluye la captación intelectual, es decir, tomar conocimiento), y la interceptación de comunicaciones personales. En cuanto al apartado segundo, este sanciona al que, en perjuicio de otro[16] y sin estar autorizado, se apodera, utiliza, modifica, altera o accede a datos reservados de carácter personal registrados en cualquier tipo de ficheros o soportes. Estos comportamientos no siempre serán estancos, y en muchas ocasiones habrá conductas que podrán incardinarse en ambos apartados.

14. Entre otras, la STS 538/2021, de 17 de junio, FD 2, habla de "inabarcable amplitud y casuismo", y la STS 412/2020, de 20 de julio, FD 2, indica: "El artículo 197 del Código Penal, es calificado por la doctrina como auténtico galimatías jurídico con diabólica, atormentada e inacabable redacción".

15. La STS 538/2021, de 17 de junio, FD 2, dice: "El art. 197 sanciona conductas que pueden afectar a la inviolabilidad de las comunicaciones, al derecho a la protección de datos -entendido éste como el derecho a controlar los datos automatizados que los demás conocen de nosotros, habeas data- y los derechos a la intimidad y a la propia imagen, preservando su integridad frente a la injustificada difusión de esos datos".

16. Es necesario acreditar este perjuicio, pero si se trata de datos sensibles el mero conocimiento derivado del simple acceso ya se considera que conlleva un perjuicio.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Los supuestos en que estos delitos se producen son muy diversos, circunscribiéndose muchos de ellos a casos individuales, como acceder al contenido del teléfono móvil de la pareja para descubrir una infidelidad, o que un funcionario de la Agencia Tributaria consulte en la base de datos de esta la información fiscal sobre un vecino con el que tiene mala relación. Sin embargo, hoy en día están aumentando y son una grave amenaza para la ciberseguridad los ataques informáticos de diversa índole en que el objetivo es la exfiltración o extracción masiva de datos, sea para su uso por el propio atacante o para comercializar con ellos (y que los compradores después utilizarán para cometer delitos). Ejemplos habituales de robo de datos son ataques a los sistemas informáticos de empresas o instituciones de los que se extraen los datos, o bien el uso de mecanismos de *phishing* para engañar a las víctimas y hacer que compartan sus datos personales.

A continuación, el artículo 197 prevé agravaciones de las penas para los siguientes supuestos: si se difunden, revelan o ceden a terceros los datos, hechos o imágenes a que se refieren los números anteriores (197.3 CP); si los hechos se han cometido por los encargados o responsables de los ficheros o soportes, o si para hacerlo se han utilizado sin autorización datos personales de la víctima, como contraseñas (197.4 CP); si se afecta a datos sensibles —sobre ideología, religión, creencias, salud, origen racial o vida sexual—, o si la víctima es menor o una persona con discapacidad necesitada de especial protección (197.5 CP); y si los hechos se han realizado con fines lucrativos (197.6 CP).

- **Acceso ilegal a sistemas informáticos (197 bis.1 CP)**

Denominado por el Tribunal Supremo como "*hacking* de desafío"[17], este delito está previsto para sancionar a quien, 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 derecho a excluirlo.

La conducta típica recae sobre el conjunto o una parte de un sistema de información, y se consuma con la simple entrada en el mismo. Por lo tanto, en este delito no es necesario tomar contacto con datos o programas que contengan informaciones concretas, ni que se vean afectados datos de carácter personal o la intimidad de otro de manera directa. Para la comi-

17. STS 494/2020, de 8 de octubre de 2020, FD 6.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

sión del delito necesariamente debe tratarse de un acceso no autorizado, y debe lograrse vulnerando medidas de seguridad, entendiendo por tales aquellas establecidas para impedir el acceso al sistema, con independencia de su solidez o complejidad, siempre que se mantengan operativas. Además de acceder, se castiga facilitar el acceso a otro y mantenerse en el sistema contra la voluntad de quien tenga derecho a excluir. Como ejemplos de este delito, la Circular 3/2017, de 21 de septiembre, de la Fiscalía General del Estado, 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, indica que podría constituirlo el acceso a un *router* —pues forma parte de un sistema de información— vulnerando su contraseña de seguridad.

La misma circular expone que en la práctica será frecuente que concurra este delito con alguna de las conductas de los apartados primero y segundo del artículo 197, con un delito del artículo 278 (si el objetivo fuera el descubrimiento de secretos de empresa) o con un delito del artículo 598 y siguientes (si el objetivo fuera el descubrimiento de secretos oficiales).

- **Interceptación ilícita (197 bis.2 CP)**

Comete este delito quien, mediante la utilización de artificios o instrumentos técnicos y sin estar autorizado, intercepta transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos.

La conducta delictiva requiere el uso de artificios o instrumentos técnicos (como dispositivos, *software*, contraseñas o códigos), y consiste en interceptar transmisiones automáticas de datos informáticos. Estas transmisiones pueden ser entre dos o más sistemas informáticos, entre distintos ordenadores dentro de un mismo sistema o incluso entre una persona y un ordenador, como las que se establecen a través del teclado. Se trata de transmisiones no públicas, en el sentido de que por la naturaleza del proceso de comunicación quedan excluidas del conocimiento de terceros, ya sea por producirse a través de redes privadas o por realizarse a través de redes públicas cuando se haya establecido algún mecanismo para garantizar la privacidad y excluir a terceros. Ejemplos de estas transmisiones son las que se producen dentro de una red de área local o una red privada virtual.

La conducta delictiva se extiende también a la captación de emisiones electromagnéticas de un sistema de información, que se generan por

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

la corriente al circular por el mismo. Usando los equipos apropiados pueden captarse estas emisiones y a partir de ellas reconstruirse datos informáticos.

- **Abuso de los dispositivos (197 ter CP)**

Denominado de esta forma en el Convenio de Budapest, consiste en producir, adquirir o facilitar herramientas e instrumentos preparados y diseñados para cometer alguno de los delitos de descubrimiento de secretos, acceso ilegal e interceptación ilegal. El objetivo de la tipificación es adelantar la barrera de protección del derecho penal. Es decir, con el fin primordial de evitar ciberataques a gran escala contra sistemas informáticos, se sancionan las fases previas de estos ataques, consistentes en la producción, adquisición y distribución de las herramientas o los instrumentos utilizados para cometerlos. En función de si el fin pretendido es el espionaje o el sabotaje informático, el Código Penal castiga estos comportamientos entre los delitos de descubrimiento y revelación de secretos (artículo 197 ter) o entre los delitos de daños informáticos (artículo 264 ter). Por ejemplo, en abril de 2023 tuvo lugar una operación de las fuerzas policiales de 17 países para desmantelar *Genesis Market*, un mercado de venta de credenciales robadas en el que se ofrecían bots que habían infectado dispositivos y recopilaban sus datos a tiempo real, datos que los compradores podían utilizar posteriormente para suplantar la identidad de la víctima y cometer estafas informáticas u otros delitos[18].

Las primeras herramientas que contempla el artículo son programas informáticos concebidos o adaptados principalmente para cometer los delitos indicados. Por lo tanto, consisten en un *software* malicioso o *malware*, diseñado para infiltrarse, obtener información y/o dañar un dispositivo o un sistema de información sin el consentimiento de su propietario. Entre ellos podemos incluir los programas espía o *spyware*, para recolectar información almacenada en un sistema informático y enviarla, como el *malware ZeuS* (utilizado en los ataques de *phishing* bancario para obtener credenciales de usuarios de banca electrónica) y los programas *keylogger* (que registran las pulsaciones en un teclado y así permiten conocer las contraseñas personales). Otros ejemplos son los conocidos *ransomware*, utilizados para cifrar archivos concretos o la totalidad del contenido de un sistema, como *Cryptolocker*, *WannaCry* o *NotPetya*.

18. Nota de prensa de Europol de 5 de abril de 2023. Disponible en https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

En segundo lugar, estas herramientas o instrumentos pueden consistir en una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información. En otras palabras, se trata de medidas de seguridad para evitar la intromisión en archivos o sistemas, legítimamente creadas y utilizadas para el acceso regular a los mismos, que el autor adquiere o facilita con la finalidad de utilizarlas para cometer los delitos indicados.

3.2.3. Delitos de daños informáticos

Son diversas conductas relacionadas con ataques a la integridad y la disponibilidad de los datos y sistemas informáticos. También se sanciona a las personas jurídicas si fueran responsables (artículo 264 quater).

- **Daños informáticos (264 CP)**

En su apartado primero se castiga a quien, por cualquier medio, sin autorización y de manera grave, borre, dañe, deteriore, altere, suprima o haga inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido sea grave.

Se sancionan, por lo tanto, todas las conductas susceptibles de afectar a la integridad de los elementos informáticos, destruyéndolos o modificándolos, pero también hacer inaccesibles estos elementos, comprometiendo su disponibilidad. Ejemplo de esto último es un ataque con un programa *ransomware*, que cifra los archivos del sistema infectado, pidiendo frecuentemente los autores un rescate a la víctima para descifrarlos.

Las penas previstas para estas conductas se agravan en el apartado segundo del artículo, cuando los hechos se cometan en el marco de una organización criminal; se ocasionen daños de especial gravedad o se afecte a un número elevado de sistemas informáticos; se perjudique gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad; se afecte al sistema informático de una infraestructura crítica (esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bien económico y social) o se cree una situación de peligro grave para la seguridad de la Unión Europea o de uno de sus Estados miembros; se utilice un programa informático concebido o adaptado para ello o una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a un sistema de información; o los hechos hubieran resultado de extrema gravedad. Por último, en el

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

apartado tercero se incrementan las penas si los hechos se cometen mediante la utilización ilícita de datos personales de otra persona para facilitar el acceso al sistema informático o para ganarse la confianza de alguien.

- **Obstaculización o interrupción del funcionamiento de sistemas informáticos (264 bis CP)**

Este delito consiste en obstaculizar o interrumpir la normal actividad de un sistema informático, de manera grave, a través de alguna de las conductas del artículo 264 (borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos, programas o documentos), introduciendo o transmitiendo datos, o destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

El delito es similar al de daños informáticos, pero la diferencia esencial es que en el artículo 264 se castigan las acciones ilícitas contra datos, programas informáticos y documentos electrónicos ajenos, y en el artículo 264 bis, aquellas cuyo objeto son los sistemas en sí mismos considerados, como conjunto interconectado de elementos informáticos.

Las penas para esta conducta se agravan si se hubiera perjudicado de forma relevante la actividad normal de una empresa, un negocio o una Administración pública (264 bis.1, inciso final); cuando concurra alguna de las ya mencionadas circunstancias del apartado segundo del artículo 264 (264 bis.2); y cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitar el acceso al sistema informático o ganarse la confianza de un tercero (264 bis.3).

Un ejemplo de este delito sería un ataque de denegación de servicio, o *DDoS*, en el que se ataca un sistema informático desde muchos equipos a la vez mediante la entrada masiva de tráfico, hasta colapsar el sistema. Otro ejemplo fue el de una bomba lógica que inutilizó más de tres mil equipos informáticos de un banco[19].

- **Abuso de los dispositivos (264 ter CP)**

Es equivalente al delito del artículo 197 ter que hemos visto anteriormente. La diferencia es que en este se sanciona la producción, adquisición y distri-

19. STS 183/2024, de 29 de febrero de 2024.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

bución de herramientas e instrumentos para cometer un delito de daños informáticos, o un delito de obstaculización o interrupción del funcionamiento de sistemas informáticos. Es decir, para determinar si estamos ante el delito del artículo 197 ter o el del artículo 264 ter, habrá que ver qué delito se tiene la intención de facilitar, cuestión que no siempre será fácil de dilucidar, sin que pueda descartarse que muchas veces concurran ambas finalidades.

3.2.4. Estafas informáticas

El delito de estafa es uno de los que, a raíz del uso de las nuevas tecnologías de la información y comunicación, han experimentado mayores evolución y crecimiento. Así, el Informe sobre la cibercriminalidad en España 2023 destaca que el 90,5 % de los delitos informáticos conocidos ese año fueron estafas. Sin embargo, bajo la denominación genérica de estafas informáticas tenemos que distinguir entre las dos tipologías generales de la cibercriminalidad a las que aludíamos anteriormente.

Desde una perspectiva amplia hablamos de estafas informáticas para referirnos a las estafas tradicionales —que consisten en engañar a otro induciéndole a realizar un acto de disposición en perjuicio propio o ajeno— cuando se cometen a través de las nuevas tecnologías, supuesto cada vez más frecuente. En estos casos no se afecta necesariamente a redes y sistemas informáticos, pero los autores aprovechan las ventajas que ofrecen las tecnologías de la información y comunicación para lograr su propósito criminal. La casuística es enorme: desde modalidades simples, como la publicación *online* de falsas ofertas de venta de bienes o de alquiler vacacional, hasta estafas más complejas, como los fraudes BEC[20]. Estas estafas se castigan en el artículo 248 del Código Penal, y en función de si el importe supera o no los 400 euros estaremos ante un delito menos grave o un delito leve.

En cambio, las estafas informáticas propiamente dichas se sancionan en el apartado primero del artículo 249. En él se castiga conseguir una transferencia no consentida valiéndose de cualquier tipo de manipulación informática, o utilizar fraudulentamente cualquier instrumento de pago distinto del efectivo o sus datos para hacer operaciones de todo tipo. Se tra-

20. Los fraudes BEC (*Business Email Compromise*) afectan a correos electrónicos empresariales: el ciberdelincuente se hace pasar, por ejemplo, por un superior jerárquico de la misma empresa, y ordena que se haga una transferencia de dinero, o bien por otra empresa con la que se mantienen relaciones comerciales, y envía una factura por unos servicios en la que ha cambiado el número de cuenta de destino. Este tipo de fraudes habitualmente se cometen por los autores usando una dirección de correo electrónico falsa, pero muy similar a la auténtica.

ta de comportamientos en los que lo determinante es que la transferencia u operación no la hace un tercero engañado (como ocurre con las estafas tradicionales, aunque se realicen por medios informáticos), sino que la realiza el autor utilizando distintos mecanismos y en perjuicio de otro. En estos supuestos es indiferente que el importe exceda o no de 400 euros.

A continuación, y de manera similar a los anteriormente vistos artículos 197 ter y 264 ter, en los apartados segundo y tercero del artículo 249 se adelantan las barreras de protección penal para castigar actos preparatorios de las estafas informáticas. El fundamento radica en la gravedad de esta tipología delictiva, que pone en grave peligro el mercado digital, genera gran desconfianza en el uso de los nuevos medios de pago y supone un importante riesgo para el funcionamiento del sistema financiero. De este modo, en el apartado segundo se castiga fabricar, adquirir, poseer y facilitar dispositivos, instrumentos informáticos o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo, así como adquirir de forma ilícita cualquier instrumento de pago distinto del efectivo para su utilización fraudulenta. Y en el apartado tercero se sanciona, si bien con una pena más reducida, poseer, adquirir o poner a disposición de terceros cualquier instrumento de pago distinto del efectivo, para su utilización fraudulenta y sabiendo que se obtuvo ilícitamente.

Tanto para las estafas del artículo 248 como para las del artículo 249 se prevén penas agravadas en los supuestos específicamente previstos en el artículo 250, entre los que hay que destacar, tratándose de estafas informáticas, aquellos en que el valor de la defraudación supere los 50 000 euros o afecte a un elevado número de personas, y un supuesto hiperagravado cuando el valor de la defraudación supere los 250 000 euros.

3.2.5. Ciberterrorismo

En los últimos años están aumentando los ataques informáticos que, más allá de perseguir un beneficio económico o perjudicar individuos o empresas concretas, tienen el objetivo de perturbar nuestra sociedad, generando intranquilidad o miedo y contribuyendo a generar una situación de desestabilización.

El ciberterrorismo está específicamente castigado en el artículo 573.2 del Código Penal, y consiste en la comisión de los delitos informáticos de acceso e interceptación ilegal, daños informáticos y abuso de dispositivos que hemos visto anteriormente (artículos 197 bis, 197 ter y 264 a 264 quater), cuando la finalidad perseguida por los autores sea cualquiera de las

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

previstas en el artículo 573.1: subvertir el orden constitucional, suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo, alterar gravemente la paz pública, desestabilizar gravemente el funcionamiento de una organización internacional o provocar un estado de terror en la población o en una parte de ella.

Por lo tanto, el ciberterrorismo se caracteriza por dos elementos: uno externo, que es la comisión de un delito informático de los anteriormente mencionados, y otro tendencial o teleológico, consistente en perseguir una de las finalidades indicadas[21]. Esta intencionalidad será determinante para distinguir los delitos informáticos ordinarios de acceso e interceptación ilegal, daños informáticos y abuso de dispositivos analizados en el apartado anterior de los supuestos de ciberterrorismo, en que la pena impuesta por estas conductas será mayor (artículo 573 bis.3).

Un ejemplo que podría encuadrarse en el concepto de ciberterrorismo sería la actividad del grupo NoName057(16). A raíz de la guerra de Ucrania este grupo ha venido realizando ataques informáticos, sobre todo ataques de denegación de servicio o DDoS, contra páginas web de instituciones públicas y empresas de sectores estratégicos de aquellos países que se han posicionado a favor de Ucrania[22].

Sin embargo, la delimitación entre ciberterrorismo y cibercriminalidad genérica no siempre será fácil. Imaginemos un ataque informático con *ransomware* a una infraestructura crítica. Puede que los autores exijan o no un rescate por los archivos cifrados. Pedir un rescate no significa que no sea ciberterrorismo, puesto que pueden coexistir una finalidad terrorista y un ánimo de lucro personal, o incluso puede que el rescate sea una vía de

21. El ATS de 29-02-24, FD 4, señala: "En efecto, tal como acordó la Junta de Sección de Fiscales de la Fiscalía del Tribunal Supremo, Acta de 6-2-2024: "el concepto de terrorismo del articulo 573 CP se construye en la actualidad sobre dos elementos o requisitos: el elemento objetivo o material, es decir, la ejecución de unas determinadas acciones previstas como tales por el Código (las enumeradas en los ap. 1, 2 y 3 del precepto), y un elemento teleológico o tendencial (la acción debe ejecutarse con una específica finalidad o propósito que se describe en el ap. 1 del art.). No es necesario que el autor pertenezca o forme parte de una organización o grupo terrorista, o actúe de manera asociada u organizada, de modo que cualquier persona que ejecute, aunque sea individualmente, o bien colectivamente, alguna de las acciones previstas con las finalidades expresadas en el precepto, será autor o partícipe de un delito de terrorismo".

22. Nota de prensa de la Guardia Civil de 20 de julio de 2024. Disponible en https://web.guardiacivil.es/es/destacados/noticias/Tres-detenidos-por-delitos-de-danos-informaticos-con-fines-terroristas/.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

financiación del grupo. Asimismo, la falta de exigencia de rescate no implica necesariamente que se trate de ciberterrorismo; para ello es necesario que persiga una de las finalidades indicadas. En esta línea cabe destacar la dificultad de distinguir entre el ciberterrorismo y los actos de *hacktivismo*, que consisten en ciberataques realizados por razones ideológicas y con impacto mediático o social, pero sin perseguir los fines recogidos en el artículo 573.1.

También hay que distinguir el ciberterrorismo en sentido estricto o ciberterrorismo genuino del uso de internet con fines terroristas. Las organizaciones o los grupos terroristas, como cualquier colectivo, han pasado a utilizar las nuevas tecnologías para desarrollar sus actividades, dadas las ventajas que estas ofrecen. Entre estos usos debemos destacar, puesto que nuestro Código Penal los castiga expresamente, el autoadoctrinamiento terrorista por medios telemáticos (artículo 575.2) y el enaltecimiento terrorista y la humillación a las víctimas por medios telemáticos (artículo 578.2). Se trata de conductas en las que se usa el ciberespacio para la comisión de actividades delictivas terroristas. Sin embargo, ni cabe incluirlas en el concepto de ciberterrorismo tal y como lo configura el artículo 573.2 ni afectan a la confidencialidad, integridad y disponibilidad de sistemas informáticos, por lo que no atacan a la ciberseguridad.

4. Conclusión

La vulnerabilidad del ciberespacio es uno de los principales riesgos a los que nos enfrentamos. A diferencia del plano físico, relativamente estable y al que miles de años de evolución nos han permitido adaptarnos como individuos y como sociedades, el ciberespacio constituye una realidad que cuenta con pocas décadas, está en constante cambio, y en la que una minoría de personas con avanzados conocimientos técnicos son capaces de moverse con una ventaja abrumadora sobre la generalidad de usuarios, sean particulares, empresas o instituciones. No podemos sustraernos a esta realidad. El ciberespacio ha venido para quedarse y todos estamos en él.

Tampoco podemos resignarnos a que el ciberespacio sea un lugar en el que los delincuentes campen a sus anchas, y a ser potenciales víctimas de ataques informáticos de la más diversa índole. Con nuestras luces y sombras, la historia de la humanidad nos demuestra que hemos sido capaces de ir extendiendo progresivamente el estado de derecho y la protección de los derechos humanos. El ciberespacio no puede ser la excepción.

En esta lucha el derecho penal no es suficiente, pero es necesario. Para poner freno a la vulnerabilidad del ciberespacio es responsabilidad de to-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

dos adoptar medidas para proteger nuestros datos y sistemas de información. Sin embargo, el riesgo cero no existe, y debemos dotarnos de un sistema penal que dé una respuesta efectiva a los ataques a la ciberseguridad.

La irrupción de la cibercriminalidad ha sido impresionante, y en ocasiones puede dar la impresión de que nos desborda. Legislaciones nacionales divergentes y tratados internacionales que no se suscriben por la gran mayoría de países habilitan la existencia de nichos desde donde los ciberdelincuentes pueden actuar impunemente. Los sistemas penales requieren tiempo para adaptarse y dar respuesta a las nuevas realidades. Ante un fenómeno como la ciberdelincuencia, que opera con carácter transnacional desde cualquier lugar del mundo, esta respuesta debe ser global. A nivel sustantivo se están haciendo grandes esfuerzos para identificar y sancionar de manera armonizada entre los distintos Estados las conductas que lesionan o amenazan la ciberseguridad. Al mismo tiempo hemos visto que se están incorporando nuevos mecanismos para mejorar la cooperación internacional entre autoridades policiales y judiciales y poder llevar a cabo operaciones coordinadas contra la ciberdelincuencia, como de hecho se está haciendo de forma exitosa en los últimos años. Hay razones para ser optimistas.

5. Bibliografía

Conal, I. (2022). *Ciberseguridad y derecho penal*. Navarra: Thomson Reuters Aranzadi.

Delgado, J. (2023). *Apuntes sobre el derecho penal en los nuevos escenarios tecnológicos: inteligencia artificial, ciberseguridad y ciberterrorismo*. Madrid: Consejo General del Poder Judicial - Cuadernos digitales de formación.

López-Muñoz, J. (2020). Ciberterrorismo. En J. López-Muñoz. *Cibercriminalidad e investigación tecnológica* (pp. 165-184). Madrid: Dykinson.

Martín, A. (2023). Prueba digital. Marco normativo para la obtención de evidencias en la investigación de delitos cometidos a través de sistemas informáticos en la Unión Europea. Articulación y utilización de herramientas de investigación tecnológica. En E. Velasco Núñez (dir.). *Marco normativo de la UE para la transformación digital*. Las Rozas, Madrid: La Ley.

Tejada, E. (2023). Marco normativo frente a la ciberdelincuencia en la Unión Europea: impulso de la armonización en el ámbito penal - sustantivo como presupuesto para el fortalecimiento de la cooperación transnacional. En E. Velasco Núñez (dir.). *Marco normativo de la UE para la transformación digital*. Las Rozas, Madrid: La Ley.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6