Jurisdicción especial para ciber delitos. Derecho Comparado.

Autores

Christine Weidenslaufer
cweidenslaufer@bcn.cl

Juan Pablo Cavada
jcavada@bcn.cl

Pamela Cifuentes
pcifuentes@bcn.cl

Nº SUP: 136163

Resumen

En materia de ciberdelincuencia, las leyes respectivas, en los distintos países, regulan y tipifican conjuntamente, delitos informáticos propiamente tales, que son aquellos en que el objeto de protección se vincula con los datos informáticos a los que se accede mediando falta de la debida autorización o manipulando la seguridad; y los delitos informáticos impropios, que son aquellos en que la informática se utiliza como un medio para la comisión del delito, como por ejemplo, delitos sexuales por medios informáticos.

Los delitos informáticos propiamente tales, más comúnmente tipificados en los países analizados, son:

a) Fraudes cometidos mediante manipulación de computadoras.
b) Manipulación de datos de entrada a la información computarizada.
c) Daños o modificaciones de programas o datos computarizados.

Todos los países analizados cuentan con servicios especializados contra la ciberdelincuencia, consistentes principalmente en unidades policiales especializadas, que a su vez se coordinan con las fiscalías.

Entre las medidas procesales especiales, destacan la existencia de agentes encubiertos y el resguardo de datos en corto plazo.

I. Introducción

La ciberdelincuencia es un área delictiva en crecimiento y rápida evolución, representando una parte sustancial del trabajo de casos de la Agencia de la Unión Europea para la Cooperación en materia de Justicia Penal (Eurojust)[1].

Esta Agencia también observa la creciente superposición entre los delitos que se originan en Internet y los delitos cibernéticos como el terrorismo y el blanqueo de capitales. La creciente sofisticación de las herramientas y prácticas relacionadas con el delito cibernético, como el cifrado, presenta nuevos desafíos para los investigadores y fiscales, ya que permite a los delincuentes evitar la detección y el enjuiciamiento ocultando datos y pruebas. Además, los desarrollos recientes muestran una creciente

[1] Eurojust (s/f).

necesidad de regulación con respecto a las tecnologías emergentes, incluida la Internet de las cosas (IoT, por sus siglas en inglés)[2].

El siguiente documento analiza la legislación comparada en materia de persecución penal de los ciberdelitos, tanto a nivel de ministerio público y tribunales especializados en España, Francia, Reino Unido, Argentina y Alemania.

El informe se tratan los delitos informáticos, directamente, según como se tipifiquen o contemplen en los países analizados, pero debe tenerse en cuenta que en rigor, los delitos informáticos propiamente tales son aquellos en que el objeto de protección se vincula con los datos informáticos a los que se accede mediando falta de la debida autorización o manipulando la seguridad, mientras que los delitos informáticos impropios son aquellos en que la informática es utilizada como un medio para la comisión del delito[3].

Para la elaboración de este informe se revisaron las normativas relevantes en una decena de países, además de la propia de la Unión Europea (UE). Se seleccionaron finalmente los casos de siete naciones más la UE. Se utilizaron también como fuentes revistas científicas y jurídicas, y convenios internacionales. Finalmente, cabe mencionar que, en la mayoría de los países revisados, no existiría legislación específica sobre ID.

Las traducciones son propias.

II. Alemania

1. La regulación de los ciber delitos

En Alemania, las conductas que pueden constituir actos de cibercrimen están reguladas por diversas áreas del derecho. El Código Penal (*Strafgesetzbuch, StGB*) es uno de los cuerpos normativos que contienen delitos de este tipo y son los siguientes: espionaje e interceptación de datos (art. 202a-c StGB), fraude informático (art. 263a StGB), sabotaje informático (art. 303b StGB) y modificación de datos (art. 303a StGB)[4].

Para combatir eficazmente esta conducta delictiva y prevenir el daño correspondiente, el legislador ha extendido parcialmente la responsabilidad penal a los actos preparatorios, como la producción o adquisición de programas informáticos cuyo objeto sea la comisión de fraude informático (art. 202c StGB). El manejo descuidado de las contraseñas también puede dar lugar a la iniciación de procedimientos preliminares.

[2] Eurojust (s/f).
[3] Schurjin (2022:6).
[4] Schlun & Elseven Rechtsanwälte (s/f).

Además, es posible infringir muchas otras disposiciones penales y reglamentarias con la ayuda de Internet, tales como la Ley Federal de Protección de Datos (*BDSG*), la Ley de Derechos de Autor (*UrhG*), la Ley de Derechos de Autor de Arte (*KunstUrhG*), la Ley Alemana de Telemedios (*TMG*) y la Ley de Competencia Desleal (*UWG*).

a) Delitos en contra de sistemas automatizados de tratamiento de datos

El ***hacking*** constituye un delito penal según las secciones 202a y 202b del Código Penal (CP), llamados espionaje de datos e interceptación de datos (*phishing*), respectivamente[5]:

- Según el artículo 202a, quien obtenga ilícitamente para sí mismo o para otro, datos que no estén destinados a él y que estén especialmente protegidos contra el acceso no autorizado, si ha eludido la protección, será sancionado con una pena de prisión no superior a tres años o con una multa.

- El artículo 202b dispone que, quien, sin estar autorizado para ello, intercepte por medios técnicos una transmisión de datos no públicos o una emisión electromagnética de una instalación de procesamiento de datos, que no estén destinado a él, para sí o para otro, incurre en pena de reclusión por hasta dos años o multa, a menos que el delito esté sujeto a una pena más severa bajo otras disposiciones.
  Si el uso de dichos datos es con la intención de obtener un beneficio material ilegal, el artículo 263a CP (fraude informático) lo sanciona con pena de prisión de hasta cinco años o una multa. Si el almacenamiento o la modificación de dichos datos crea un documento falsificado o falsificado, ello puede constituir un delito (art. 269 CP, falsificación de registros técnicos).

Respecto de una conducta preparatoria para los delitos de espionaje de datos y phishing, el artículo 202c CP sanciona la fabricación, venta y adquisición con el fin de utilizar, distribuir o poner a disposición de otro modo un dispositivo, incluidos los programas informáticos, que se diseñaron o prepararon principalmente con el fin de cometer determinados ataques cibernéticos[6].

El artículo 303b CP regula el **sabotaje informático**, esto es, la infección de sistemas de TI con *malware* (incluyendo *ransomware*, *spyware*, gusanos, troyanos y virus). De acuerdo con esta disposición, quien interfiera en las operaciones de procesamiento de datos que sean de importancia sustancial para otro, borrando, suprimiendo, inutilizando o alterando datos, o ingresando o transmitiendo datos con la intención de causar daño a otro, será castigado con pena de prisión hasta por tres años o multa.

Lo mismo se aplica a la destrucción, daño, inutilización, eliminación o modificación de un sistema de procesamiento de datos o un soporte de datos. Asimismo, es importante señalar que la sola tentativa es punible y si la operación de tratamiento de datos reviste una importancia sustancial para el negocio o empresa ajena, o para una autoridad pública, la sanción puede ser de prisión de hasta cinco años o multa.

[5] Niethammer *et al* (2021).
[6] Niethammer *et al* (2021).

La **usurpación de identidad** puede constituir varios delitos penales, dependiendo de cómo el delincuente obtenga acceso a los datos de identidad. Si es mediante métodos de *phishing*, constituye un delito según el artículo 202b CP, ya mencionado. Si lo es mediante el uso de dichos datos de identidad con fines fraudulentos, podría constituir un delito según los artículos 263 CP (fraude) o 263a CP (fraude informático), ambos delitos sancionados con penas de prisión de hasta cinco años, o incluso de hasta 10 años en casos especialmente graves.

Con las mismas sanciones y dependiendo de los hechos individuales del caso, el uso de la identidad de otra persona puede constituir además un delito según el artículo 267 CP (falsificación de documentos) o el artículo 269 CP (falsificación de datos con valor probatorio)[7].

Otros ciber delitos de este tipo son: el manejo de datos robados (art. 202d CP); la violación de secretos postales y de telecomunicaciones (art. 206 CP); ciertos tipos de violación del Reglamento General de Protección de Datos de la UE con la intención de enriquecer o dañar a alguien (art. 84 RGPD y art. 42 de la Ley Federal Alemana de Protección de Datos, *Bundesdatenschutzgesetz*; y la falsificación de evidencia digital (art. 269 y ss. CP)[8].

2. Medidas procesales

Dependiendo del tipo de autoridad -por ejemplo, el Ministerio Público, la Oficina Federal para la Seguridad de la Información (*Bundesamt für Sicherheit in der Informationstechnik*, *BSI*) o la Autoridad de Protección de Datos (como el Comisionado de Protección de Datos y Libertad de Información)-, los poderes de ejecución varían[9].

Si la conducta investigada pudiera calificarse como delictiva, será el Ministerio Fiscal el que dirija las investigaciones más comúnmente con el auxilio de otras autoridades. Todas las autoridades antes mencionadas tienen la facultad de realizar investigaciones in situ, incluido el acceso a los sistemas informáticos[10].

Bajo ciertas condiciones previas de acuerdo con el artículo 100a del Código de Procedimiento Penal alemán, las telecomunicaciones pueden ser interceptadas y grabadas sin el conocimiento de las personas involucradas, y la Sec. 100b del Código de Procedimiento Penal alemán ofrece la posibilidad de obtener acceso encubierto a los sistemas de tecnología de la información utilizados por las personas interesadas. Más recientemente, el legislador alemán ha ampliado el ámbito de aplicación de las medidas de investigación mencionadas, a partir de julio de 2021, tanto para la vigilancia de las telecomunicaciones como para las búsquedas remotas encubiertas de tecnologías de la información, y se ha modificado el catálogo de posibles delitos que permiten tales medidas de investigación. Por lo tanto, se espera que las autoridades investigadoras lleven a cabo un mayor número de medidas de vigilancia y búsquedas remotas encubiertas que en los años anteriores[11].

[7] Niethammer *et al* (2021).
[8] Niethammer *et al* (2021).
[9] Niethammer *et al* (2021).
[10] Niethammer *et al* (2021).
[11] Niethammer *et al* (2021).

Además, la Ley de Telemedios de Alemania se modificó en abril de 2021 y ahora permite a los proveedores transmitir datos personales, así como la dirección IP de un usuario; a las autoridades encargadas de hacer cumplir la ley para el enjuiciamiento de delitos y, en cierta medida, para el enjuiciamiento de infracciones administrativas graves en caso de que se haya solicitado al proveedor que divulgue dicha información a las autoridades mediante una solicitud formal. En casos de delitos especialmente graves, los proveedores también pueden verse obligados a entregar las contraseñas de sus usuarios[12].

3. Servicios especializados de lucha contra el cibercrimen

En primer lugar, las fuerzas policiales de los Länder alemanes son los entes responsables de investigar los ciberdelitos en Alemania[13].

Como agencia central de la policía alemana, la Oficina de la Policía Criminal Federal (*Bundeskriminalamt*, *BKA*) realiza tareas de coordinación también en el campo de la supresión del ciberdelito, proporciona información y herramientas, y sirve como centro de cooperación internacional. Además, la BKA lleva a cabo investigaciones en el campo del delito cibernético dentro del marco de su jurisdicción original, por ejemplo, cuando las autoridades o instalaciones federales o partes sensibles de infraestructuras críticas se ven afectadas o cuando se ha solicitado u ordenado al Bundeskriminalamt que realice investigaciones[14].

La principal división responsable de realizar las tareas mencionadas anteriormente en la BKA es la División CC - Cibercrimen. Esta se encarga de[15]:

- Investigar a los delincuentes activos en el ciberespacio y desmantela las redes y estructuras delictivas responsables de los ciberataques contra objetivos destacados en Alemania;
- Garantizar la recopilación, el procesamiento y el análisis de información relevante como base de las investigaciones realizadas por las fuerzas policiales de la Federación y los Länder en un entorno de cibertecnologías de alta complejidad;
- Perseguir los ataques cibernéticos a instituciones federales e infraestructuras críticas en Alemania;
- Asesorar a la dirección de la BKA sobre cuestiones de política criminal relacionadas con el ciberdelito en el sentido más estricto; y
- Contribuir activamente al desarrollo ulterior de las disposiciones legales pertinentes, por ejemplo, proporcionando servicios de asesoramiento.

Por su parte, el Centro Nacional de Ciberdefensa es la plataforma -no una autoridad independiente- interinstitucional de cooperación, comunicación y coordinación de las autoridades alemanas (de seguridad) para intercambiar inteligencia relacionada con la situación, se evalúan potenciales amenazas o las acciones que deben tomar políticos, autoridades, la sociedad o el sector empresarial[16].

[12] Niethammer *et al* (2021).
[13] Bundeskriminalamt (s/f).
[14] Art. 4 Ley sobre el *Bundeskriminalamt*, Ley BKA.
[15] Bundeskriminalamt (s/f).
[16] Bundeskriminalamt (s/f).

Creada en 2011, en el marco de la implementación de la Estrategia de Ciberseguridad (CSS) del Gobierno Federal, para intercambiar información relevante rápidamente entre las autoridades participantes y entes asociados, y coordinar las medidas de protección con el fin de garantizar la ciberseguridad en Alemania.

Actualmente, está compuesto por las siguientes ocho autoridades principales: el Servicio de Contrainteligencia Militar; la Oficina de la Policía Criminal Federal (BKA); la Oficina Federal de Seguridad de la Información (BSI); la Oficina Federal para la Protección de la Constitución (BfV); la Oficina Federal de Protección Civil y Asistencia en Casos de Desastre (BBK); el Comando de servicio de dominio de información y cibernético de las Fuerzas Armadas; la Policía Federal (BPOL); y el Servicio Federal de Inteligencia (BND). Son entes asociados: la plataforma bávara de ciberdefensa (*Cyberabwehr Bayern*): el Centro de cibercompetencia de Hessen (Hessen3C); las Fiscalías de Bamberg y Colonia, especializadas en investigaciones de ciberdelincuencia; y la Superintendencia Federal de Supervisión Financiera[17].

III. Argentina

1. La regulación de los ciber delitos

La Ley N° 26.388 de 24 de junio de 2008, llamada Ley de delitos informáticos, introduce diversas modificaciones al Código Penal (CP), algunas de ellas, en materia de delitos informáticos[18].

En materia de daños, el segundo párrafo de su artículo 183[19] contempla pena de prisión de 15 días a 1 año para quien altere, destruya o inutilice datos, documentos, programas o sistemas informáticos, como también para quien venda, distribuya, haga circular o introduzca en un sistema informático, cualquier programa dañino.

Al modificar el artículo 184[20] CP, la norma actual dispone, entre las hipótesis agravadas que prevén prisión de 3 meses a 4 años, la ejecución del daño en datos, documentos, programas o sistemas informáticos públicos; así como su perpetración en sistemas informáticos destinados a la prestación de

[17] Bundeskriminalamt (s/f).
[18] Schurjin (2022:3).
[19] Art. 183 CP: será reprimido con prisión de quince (15) días a un (1) año el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado.
En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.
[20] Art. 184 CP: la pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes: 1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones; 2. Producir infección o contagio en aves u otros animales domésticos; 3. Emplear substancias venenosas o corrosivas; 4. Cometer el delito en despoblado y en banda; 5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Algunos delitos introducidos por esta Ley se clasifican según el bien jurídico protegido.

a) Delitos informáticos contra la integridad sexual

El artículo 128 CP[21] contempla la pena de prisión de 3 a 6 años a quien produzca, financie, ofrezca, comercie, publique, facilite, divulgue o distribuya, a través de los nuevos medios electrónicos (internet), toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales. También prevé prisión de 4 meses a 1 año para quien, con conocimiento, incurriere en la mera tenencia de representaciones como las evocadas. La pena se eleva a prisión de 6 meses a 2 años si esa tenencia tuviese fines inequívocos de distribución o comercialización.

Todas las escalas penales señaladas se incrementan en un tercio en su mínimo y en su máximo en caso de que la víctima fuere menor de 13 años.

Por su parte, el artículo 131 CP sanciona con pena de prisión de 6 meses a 4 años a quien, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, tomare contacto con una persona menor de edad, con el propósito de cometer cualquier delito contra su integridad sexual.

b) Delitos informáticos contra la libertad

El artículo 153 bis CP[22] sanciona residualmente con prisión de 15 días a 6 meses a quien, a sabiendas, accediere por cualquier medio, sin autorización o en exceso de la existente, a un sistema o dato informático de acceso restringido. La pena es de 1 mes a 1 año de prisión si el acceso se efectúa en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

---

[21] Art. 128 CP: Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.
Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización. − Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.
Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años.

[22] Art. 153 bis CP: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.”,

Los cambios que la ley de delitos informáticos introdujo en el artículo 153 CP[23] argentino habilitaron la punición con prisión de 15 días a 6 meses para quien fuera más allá de un mero acceso ilegítimo y: i) accediere indebidamente a una comunicación electrónica que no le esté dirigida; ii) se apoderare indebidamente de tal tipo de misiva; iii) indebidamente suprimiere o desviare de su destino una comunicación electrónica que no le esté dirigida; iv) indebidamente interceptare o captare comunicaciones electrónicas. La disposición duplica la escala penal para el sujeto activo que, además, comunicare a otro o publicare el contenido de la comunicación electrónica. Asimismo, contempla la inhabilitación especial por el doble del tiempo de la condena si el hecho lo cometiere un funcionario público que abusare de sus funciones.

Dentro de la gama de conductas incorporadas al Código Penal por la ley de delitos informáticos una de las más levemente penadas la encontramos en el artículo 155[24], que prevé multa de 1.500 a 100.000 pesos argentinos para quien poseyere una comunicación electrónica no destinada a la publicidad y la hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros; a menos que hubiere obrado con el propósito inequívoco de proteger un interés público, en cuyo caso está exento de responsabilidad penal.

El artículo 157 del Código Penal[25] también fue objeto de reforma por parte de la ley de delitos informáticos. Actualmente, se sanciona con prisión de 1 mes a 2 años e inhabilitación especial de 1 a 4 años, al funcionario público que revelare documentos (informáticos)[26] o datos que por ley deben ser secretos.

Finalmente, el acceso ilegítimo a banco de datos personales, revelación ilegítima de su información e inserción ilegítima de datos se castiga en el artículo 157 bis CP[27], en función del cual es pasible de ser

---

[23] Art. 153 CP: será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.
La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.
Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

[24] Art. 155: será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.
Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.”.

[25] Art. 157: será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.”.

[26] El artículo 1° de la Ley N° 26.388 incorporó las siguientes definiciones al artículo 77 del Código Penal:
- "documento": toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
- "firma" y "suscripción": la firma digital, la creación de una firma digital o firmar digitalmente.
- "instrumento privado" y "certificado": el documento digital firmado digitalmente.

[27] Art. 157 bis CP: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

penado con prisión de 1 mes a 2 quien ingrese a un banco de datos personales sin autorización ni permiso alguno; quien revelare secretos o archivos registrados en ese banco de datos y quien los modifique por cualquier medio. Se añade la pena de inhabilitación especial de 1 a 4 años si el sujeto activo es un funcionario público.

c) Delitos informáticos contra la propiedad

El artículo 173 inciso 15 CP[28] sanciona con prisión de 1 mes a 6 años para quien defraudare mediante el uso no autorizado de los datos de una tarjeta de compra, crédito o débito, aunque lo hiciere por medio de una operación automática. Luego, el mismo artículo, en su inciso 16, sanciona con prisión de 1 mes a 6 años, la defraudación mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

d) Delitos informáticos contra la seguridad pública que atentan contra los medios de comunicación

El artículo 197[29] CP contempla prisión de 6 meses a 2 años para quien interrumpiere o entorpeciere la comunicación electrónica o resistiere violentamente el restablecimiento de la comunicación electrónica interrumpida.

e) Delitos informáticos contra la administración pública

El artículo 255[30] CP sanciona a quien sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte, registros o documentos electrónicos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público, asignando pena de prisión de 1 mes a 4 años, salvo que el autor fuere el mismo depositario, en cuyo caso sufrirá además inhabilitación especial por doble tiempo; o que el hecho se cometiere por imprudencia o negligencia del depositario, quien –en ese caso– será reprimido con multa.

---

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno (1) a cuatro (4) años.".

[28] Art. 173 CP: sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece (prisión de un mes a seis años): (…) 15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.

[29] Art. 197 CP: será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

[30] Art. 255 CP: será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($750) a pesos doce mil quinientos ($12.500).

2. Medidas procesales

Por tratarse de un país federal, las policías de cada provincia cuentan con sus propios estatutos. Por ejemplo, se puede mencionar el Código Procesal Penal de la provincia de Mendoza, Ley N° 6.730, de 1999, que contempla las siguientes medidas en materia de investigación penal de delitos informáticos:

- El registro de dispositivos informáticos para acceder a los mismos, previa autorización judicial.
- El registro puede ser remoto, autorizada cuando la vida o integridad física o sexual de una persona estén en grave peligro.
- La confiscación de datos informáticos almacenados. El tribunal puede disponer su secuestro, la clonación de los datos informáticos almacenados y la posibilidad de hacerlos inaccesibles desde el sistema informático o el dispositivo tecnológico.
- Se incorpora la posibilidad de facilitar voluntariamente datos informáticos, usuarios y contraseñas.
- Se admite solicitar la conservación rápida de datos informáticos (ya sean básicos, de tráfico o de contenido) a proveedores de servicio, para que estos no sean alterados en el transcurso de la investigación, pudiendo obligar a los proveedores a mantener el secreto para que el usuario no advierta la medida. Luego se puede solicitar y acceder a esos datos posteriormente.
- Se introduce la figura del agente encubierto informático, que puede ser útil en la lucha contra la pornografía infantil y el delito de grooming.

3. Servicios especializados de lucha contra el cibercrimen

La persecución penal de estos delitos corresponde al Ministerio Público Fiscal, y dentro de él, en el caso de los delitos informáticos, a la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)[31]. La UFECI se creó mediante la Resolución PGN N°3743/15 se creó la UFECI, para robustecer la capacidad de respuesta del organismo en materia de detección, persecución y represión de la criminalidad organizada y de los delitos que más menoscaban la seguridad ciudadana.

La UFECI es competente en casos de ilícitos consistentes en ataques a sistemas informáticos, o cuando el medio comisivo principal o accesorio de una conducta delictiva incluya la utilización de sistemas informáticos, con especial atención en el ámbito de la criminalidad organizada, y crímenes en los que sea necesario realizar investigaciones en entornos digitales –aun cuando no hayan sido cometidos contra o mediante un sistema informático-.

Entre las principales funciones de la Unidad Fiscal Especializada en Ciberdelincuencia se encuentran:

- Intervenir en los casos de su competencia y asistir a los/as fiscales;
- Recibir denuncias y realizar investigaciones preliminares y genéricas;
- Actuar como nexo con los diferentes actores e instituciones nacionales e internacionales con incidencia en cuestiones vinculadas a la temática;
- Articular con las procuradurías, unidades fiscales y demás áreas de la Procuración General, a los efectos de la implementación de estrategias eficaces para el abordaje de la ciberdelincuencia.

[31] UFECI (s/f).

- Asesorar a los/as fiscales sobre los recursos tecnológicos y herramientas de apoyo técnico, laboratorios, métodos de investigación, obtención, análisis y preservación de la prueba, disponibles en el país;
- Desarrollar estudios acerca de las reformas reglamentarias y legislativas necesarias;
- laborar informes y diagnósticos sobre esta clase especial de criminalidad; y
- Desarrollar actividades de cooperación, divulgación y capacitación sobre cibercrimen.

IV. España

1. La regulación de los ciber delitos

El Código Penal contempla los delitos informáticos o ciber delitos, agrupando delitos informáticos propiamente tales con delitos informáticos impropios, con la particularidad de que, en vez de construir tipos penales especiales, ha sumado al medio informático como un medio más de comisión. Es decir, todos ellos contemplan como variables y medios empleados en la comisión del delito los siguientes: Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

La tipificación de las conductas sigue las mismas conceptuaciones que emplea el Convenio de Budapest, a los que se le ha añadido los delitos contra el honor y las amenazas y coacciones[32].

A continuación se enumeran los delitos informáticos existentes y sus subtipos.

a) Delitos en contra de sistemas automatizados de tratamiento de datos

En este ámbito se incluyen el acceso e interceptación ilícita se regulan los delitos de descubrimiento y revelación de secretos (arts. 197 a 201 CP) y los delitos relativos al mercado y los consumidores o espionaje industrial (arts. 278 a 286); el delito de interferencia en los datos y en el sistema (ataques informáticos y daños), regulados en los arts. 263 a 267 y 625.1 CP, la falsificación informática (arts. 388-389, 399 bis, 400 y 401 CP), el fraude Informático (arts. 248 a 251 y 623.4 CP),

b) Delitos informáticos en contra de personas

En este caso se refiere a los delitos sexuales siguientes: exhibicionismo, provocación sexual, acoso sexual, abuso sexual, corrupción de menores/incapacitados, pornografía de menores, y delito de contacto mediante tecnología con menor de 13 años con fines sexuales (arts. 181, 183.1, 183.bis, 184, 185, 186 y 189 CP).

Luego se encuentran los delitos contra la propiedad industrial e intelectual (arts. 270 a 277 y 623.5 CP), delitos contra el honor -calumnias e injurias- (arts. 205 a 210 y 620.2 CP); los delitos contra la salud

[32] Dirección General de Coordinación y Estudios Secretaría de Estado de Seguridad (2021:6).

pública, como el tráfico de drogas (arts. 359 a 371 CP); y los delitos de amenazas y coacciones (arts. 169 a 172 y 620 CP).

2. Medidas procesales

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, modificó el artículo 118 de la ley señalada, cuyo contenido primordial es de regulación del derecho de defensa.

La reforma señalada fortalece los derechos procesales según las exigencias del Derecho de la Unión Europea y la regulación de las medidas de investigación tecnológica en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados por la Constitución. La reforma de la Ley de Enjuiciamiento Criminal comprende medidas que desarrollan derechos fundamentales y otras de naturaleza estrictamente procesal.

Se estima que las materias directamente relacionadas con ciber delitos son las siguientes:

Se toma como referencia el artículo 16 del Convenio sobre la Ciberdelincuencia, de 23 de noviembre de 2001, ratificado por España el 20 de mayo de 2010, y se establece un plazo máximo de vigencia de la orden de noventa días prorrogable hasta que se autorice la cesión o se cumplan ciento ochenta días.

Existe el agente encubierto a efectos de la persecución de determinadas modalidades delictivas. La reforma actualiza el uso de tales recursos por el agente encubierto en las tareas que tiene encomendadas. En concreto, se prevé la posibilidad de que los agentes encubiertos puedan obtener imágenes y grabar conversaciones, siempre que recaben específicamente una autorización judicial para ello.

Se regula la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación (puesto que en los canales abiertos, por su propia naturaleza, no es necesaria) y que a su vez, requerirá una autorización especial (sea en la misma resolución judicial, con motivación separada y suficiente, sea en otra distinta) para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación.

3. Servicios especializados de lucha contra el cibercrimen

La Brigada Central de Investigación Tecnológica (BCIT) es la Unidad policial destinada a responder a los retos que plantean las nuevas formas de delincuencia, tales como pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería, etc.[33]

La BCIT está encuadrada en la Unidad de Investigación Tecnológica (CGPJ), que es el órgano de la Dirección General de la Policía encargado de la investigación y persecución del ciberdelito de ámbito

[33] Policía Nacional de España (s/f).

nacional y transnacional. Actuará como Centro de Prevención y Respuesta E-Crime de la Policía Nacional[34].

Su misión consiste en obtener las pruebas, perseguir a los delincuentes y poner a unas y otros a disposición judicial. Sus herramientas son la formación continua de los investigadores, la colaboración de las más punteras instituciones públicas y privadas, la participación activa en los foros internacionales de cooperación policial y la colaboración ciudadana[35].

Las funciones de la BCIT son[36]:

- La realización directa de las investigaciones especialmente complejas.
- La coordinación de las operaciones que involucren a diversas Jefaturas Superiores.
- La formación del personal de la Policía Nacional y otros cuerpos de Policía extranjeros.
- La representación internacional y la ejecución y/o coordinación de las investigaciones que tengan su origen en otros países.

Adicionalmente, en 2012 un acuerdo entre la Secretaría de Estado de Seguridad y la Secretaría de Estado para la Sociedad de la Información favoreció la creación del Centro de Respuesta a Incidentes Informáticos para Empresas, RedIRIS, Profesionales de TI e Infraestructuras críticas (CERTSI). En 2017 este organismo detectó 19.275 accesos informáticos no autorizados, 11.959 casos de fraude, 81.090 troyanos, 7.957 casos de spam, 514 denegación de servicios, 1.435 escaneos de red, 47 robos de información y 767 infracciones de otro tipo. Además, se ha detectado un aumento del 24% del código dañino, un 148% más de accesos no autorizados y un 96% más de ataques de denegación de servicio respecto al año 2016[37].

Otras entidades encargadas de la ciber seguridad son las siguientes[38]:

- La Oficina de Coordinación de Ciberseguridad (OCC) es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad[39].
  La OCC, al interior de la Dirección General de Coordinación y Estudios, opera como canal específico de comunicación entre los Centros de Respuesta a Incidentes de Seguridad Informáticas (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad, desempeñando la coordinación técnica en materia de ciberseguridad entre dicha Secretaría de Estado y sus organismos dependientes. Además, es el punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros, según lo establecido por la Directiva 2013/40/UE, de 12 de julio, relativa a los ataques contra los Sistemas de Información.

[34] Policía Nacional de España (s/f).
[35] Policía Nacional de España (s/f).
[36] Policía Nacional de España (s/f).
[37] Colegio Criminológico de Madrid (2018).
[38] Dirección General de Coordinación y Estudios Secretaría de Estado de Seguridad (2021:36).
[39] Sus funciones se regulan por el Real Decreto 734/2020, de 4 de agosto, que desarrolla la estructura orgánica básica del Ministerio del Interior y su posterior modificación en el Real Decreto 146/2021, de 9 de marzo.

Por otro lado, la OCC es el organismo encargado de recibir todas aquellas notificaciones de incidentes que tengan carácter obligatorio al amparo de ese Real Decreto-Ley y de la Guía Nacional de Notificación y Gestión de Ciberincidentes.

- El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, es el CSIRT al que corresponde la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre, conforme el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, es decir las entidades privadas.
  El INCIBE-CERT está operado conjuntamente por el INCIBE y la Oficina de Coordinación de Ciberseguridad en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.

- El Centro Criptológico Nacional, es el CSIRT de referencia para el sector público sujeto a la Ley 40/2015, y según el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

V. Francia

1. La regulación de los ciber delitos

En Francia el tema se ha abordado principalmente desde la legislación penal, distinguiendo entre aquellos delitos en contra de sistemas automatizados de tratamientos de datos y aquellos delitos en que se usa tecnología para cometer delitos directamente contra personas, tales como pornografía infantil, usurpación de identidad y ciberacoso.

En el caso de delitos en contra de sistemas automatizados de tratamientos de datos, las sanciones son más graves cuando estos sistemas de datos personales son del Estado. A nivel procesal se contemplan medidas para facilitar la investigación de este tipo de delitos. Finalmente, la Policía Judicial cuenta con oficinas especializadas sobre la materia.

El Código Penal francés, sanciona los ciberdelitos distinguiendo entre:

a) Delitos en contra de sistemas automatizados de tratamiento de datos

Es lo que se conoce como delitos *STAD* (*Système de traitement automatisé de données*), por lo tanto, los actos de ciberespionaje en la red informática de una empresa, el ataque de un *hacker* a un sitio web institucional, son acciones que pueden ser perseguidos por la vía de este tipo de delitos STAD.

El artículo 323-1 y siguientes del Código Penal, señala diversas acciones sujetas a las siguientes sanciones penales para estos delitos:

El acceso o la permanencia fraudulenta en todo o parte de un sistema de tratamiento automatizado de datos, es sancionado con 2 años de prisión y multa de 60.000 euros. Si como consecuencia de lo anterior se produce la supresión o modificación de datos contenidos en el sistema, o la alteración del funcionamiento de esta, la sanción aumenta de 3 años de prisión y multa de 100.000 euros. Ahora bien, si las infracciones señaladas se han cometido contra un sistema automatizado de tratamiento de datos personales implantado por el Estado, la pena se eleva a 5 años de prisión y multa de 150.000 euros.

- La obstrucción o alteración del funcionamiento de un sistema automatizado de tratamiento de datos, se castiga con 5 años de prisión y multa de 150.000 euros. Si este delito se cometiere contra un sistema automatizado de tratamiento de datos personales implantado por el Estado, la pena se aumenta a 7 años de prisión y 300.000 euros de multa.
- La introducción fraudulenta de datos en un sistema de tratamiento automatizado, la extracción, retención, reproducción, transmisión, supresión o modificación fraudulenta de los datos que contienen, está sancionado con 5 años de prisión y multa de 150.000 euros. Ahora bien, cuando este delito se comete contra un sistema automatizado de tratamiento de datos personales implantado por el Estado, la pena se aumenta a 7 años de prisión y multa de 300.000 euros.
- El hecho, sin motivo legítimo, en particular de investigación o seguridad informática, de importar, poseer, ofrecer, transferir o poner a disposición un equipo, un instrumento, un programa de ordenador o cualquier dato diseñado o especialmente adaptado para cometer uno o más de los delitos previstos anteriormente, es castigado con las penas previstas anteriormente o con la pena del delito más severamente castigado.
- La participación en una banda organizada para cometer los hechos anteriores descritos se castiga con las penas previstas para el delito mismo o para el delito más severamente castigado. Ahora bien, si el delito cometido por la banda organizada es contra un sistema automatizado de tratamiento de datos personales implantado por el Estado, la pena se agrava con 10 años de prisión y multa de 300.000 euros.

Junto con lo anterior, las personas que cometen alguno de los delitos señalados incurren, además, en las siguientes penas adicionales:

- Prohibición, por un período máximo de 5 años, de los derechos cívicos, civiles y familiares (*droits civiques, civils et de famille)*, esto es: derecho de voto; derecho a cargos de elegibilidad o de función pública; derecho a ejercer una función judicial o a ser perito ante un tribunal; derecho a representar o asistir a una de las partes ante los tribunales; derecho a testificar en juicio, salvo para hacer simples declaraciones; derecho a ser tutor o curador; claro que esta prohibición no excluye el derecho, previo dictamen conforme del juez de tutela, oído el consejo de familia, a ser tutor o curador de los propios hijos.
- Prohibición, hasta por 5 años, de ejercer una función pública o ejercer la actividad profesional o social en cuyo ejercicio o con motivo de la cual se cometió la infracción;
- El decomiso del objeto que se usó o estuvo destinada a cometer el delito o del objeto que es producto del mismo, con excepción de los objetos sujetos a restitución;
- La clausura, por un período máximo de cinco años, de los establecimientos o de uno o más de los establecimientos de la empresa utilizados para la comisión de los hechos imputados;
- Exclusión, hasta por cinco años, de los contratos públicos;

- Prohibición, hasta por cinco años, de emitir cheques distintos de los que permitan al girador retirar fondos del girado o de los que estén certificados;
- La publicación o difusión de la decisión dictada.

b) Delitos informáticos en contra de personas

El Código Penal establece también delitos específicos y circunstancias agravantes respecto a aquellas acciones en que se usa Internet para dañar a las personas en su ámbito privado. Particularmente, existen medidas de protección respecto a los menores de edad.

El artículo 227-23 del Código Penal, por ejemplo, sanciona la **pornografía infantil**, estableciendo cinco años de prisión y multa de 75.000 euros, el hecho de grabar o transmitir la representación pornográfica de un menor con el objetivo de su difusión. Las penas se aumentan a siete años de prisión y 100.000 euros de multa, cuando la difusión se realice a través de una red de comunicaciones electrónicas. Las penas previstas en este artículo se aumentan a diez años de prisión y 500.000 euros multa cuando los hechos se cometan en banda organizada.

También en el contexto de protección a los menores de edad se debe tener en consideración una ley recientemente dictada (*Loi N° 2021-478 du 21 avril 2021 visant à protéger les mineurs des crimes et délits sexuels et de l'inceste*), y que modificó el Código Penal, estableciendo un delito para luchar contra la "sextorsión", castigando el hecho de que un adulto incite a un menor a realizar prácticas sexuales en Internet, con 7 años de prisión y 10 años si la víctima es menor de 15 años.

Por otra parte, el artículo 226-4-1 del Código Penal establece que el **acto de usurpación de la identidad de un tercero**, cuando este delito se comete en una red pública de comunicación en línea, se castiga con un año de prisión y multa de 15.000 euros. Si el acto es cometido por el cónyuge o pareja de la víctima o por la pareja vinculada a la víctima por pacto civil, aumenta la sanción a dos años de prisión y multa de 30.000 euros.

En relación a la lucha contra la violencia sexual y de género, en 2018 la *Loi n° 2018-703* introdujo un nuevo artículo 226-3-1 en el Código Penal para sancionar la práctica de lo que se conoce como ***upskirting***, esto es, filmar o fotografiar las partes íntimas de una persona sin que ésta sepa, a menudo con el objetivo de publicar las imágenes en Internet. La sanción establecida es de dos años de prisión y 30.000 euros de multa si las imágenes hayan sido grabadas o transmitidas.

Junto con lo anterior, el legislador ha establecido castigar con mayor severidad al autor del delito cuando ha entrado en contacto con la víctima a través de una red de comunicación electrónica, como es el caso de los delitos de violación, agresión sexual, compra de servicios sexuales a un menor o persona vulnerable, corrupción de menores y en caso de ciberacoso o acoso moral.

Por último, cabe señalar que el **ciberacoso** es una forma de acoso moral definida por el artículo 222-33-2-2 del Código Penal, que se refiere a "hostigar a una persona mediante comentarios o conductas reiteradas que tengan por objeto o efecto el deterioro de sus condiciones de vida que produzcan una alteración de su salud física o psíquica", y se sanciona con dos años de prisión y multa de 30.000 euros

o tres años de prisión y multa de 45.000 euros si la víctima es menor de 15 años, si las acciones han sido cometidas mediante el uso de un servicio público de comunicación en línea o a través de un medio digital o electrónico.

2. Medidas procesales

Existen una serie de medidas procesales cuyo objetivo es reunir evidencias en la investigación, principalmente aplicables a este tipo de delitos son:

a) Investigación bajo seudónimo (*De l'enquête sous pseudonyme*)

El artículo 230-46 del Código Procesal Penal permite, para el solo efecto de registrar los crímenes y delitos sancionados con pena privativa de libertad cometidos por medios de comunicaciones electrónicas y siempre que las exigencias de la instrucción o investigación lo justifiquen, que los oficiales o agentes de la policía judicial (*police judiciaire*), que actúen en el curso de la instrucción o investigación que estén adscritos a un servicio especializado y especialmente autorizados para este fin y en las condiciones que se determinen por orden del Ministro de Justicia y del Ministro del Interior, puedan proceder bajo seudónimo a los siguientes actos, sin ser penalmente responsables:

1° Participar en intercambios electrónicos, incluso con personas que puedan ser los autores de estos delitos;
2° Extraer o almacenar por este medio datos sobre las personas que puedan ser los autores de estos delitos y cualquier evidencia; y,
3° Adquirir cualquier contenido, producto, sustancia, muestra o servicio, incluidos los ilícitos, previa autorización del Ministerio Público o del juez de instrucción que conozca de los hechos, o transmitir contenidos ilícitos en respuesta a una solicitud expresa. En este caso, esta autorización puede darse por cualquier medio, lo que se mencionará o se hará constar en el expediente del procedimiento, y los actos autorizados no pueden constituir incitación a la comisión de estos delitos, todo esto bajo pena de nulidad.

Se debe tener en consideración que la policía judicial tiene dentro de sus misiones la investigación de los delitos, y se distingue de la policía administrativa (*police administrative*) ya que esta última tiene la misión de prevenir los delitos y mantener el orden. La policía judicial es controlada por el Ministerio Público, durante la fase de investigación, o por el juez de instrucción, durante la instrucción. Por lo tanto, tal como señala expresamente el artículo mencionado, los actos de investigación bajo seudónimo se llevan siempre a cabo bajo la supervisión del fiscal o del juez de instrucción.

a) Interceptación de comunicaciones electrónicas (*L'interception des communications électroniques)*

Los artículos 100 y siguientes del Código Procesal Penal se refieren a esta materia. Se señala que si la pena impuesta fuere igual o superior a tres años de prisión, el juez de instrucción puede, cuando las exigencias de la información así lo exijan, disponer la interceptación, grabación y transcripción de la

correspondencia enviada por medios de comunicación electrónicos. Estas operaciones se realizan bajo su autoridad y control.

En caso de delitos cuya infracción es sancionada con pena privativa de libertad, y cuyas acciones fueron cometidas mediante comunicaciones electrónicas a la víctima, podrá la víctima solicitar la interceptación en los mismos términos señalados.

3. Servicios especializados de lucha contra el cibercrimen

Dentro de la lucha por combatir el cibercrimen, algunas de las instituciones encargadas de pesquisar y sancionar estos delitos han creado oficinas especializadas, como es el caso de la policía judicial, la cual creó la Subdirección de lucha contra el ciberdelito (*Sous-direction de lutte contre la cybercriminalité, SDLC*)[40].

La SDLC, creada por *Arrêté du 29 avril 2014*, está integrada por aproximadamente 150 personas, entre policías, gendarmes, administrativos, ingenieros, técnicos y contratistas[41].

La subdirección tiene como objetivo la lucha contra la ciberdelincuencia en un contexto de aumento de los delitos cometidos en Internet, facilitado por la generalización del uso de las nuevas tecnologías por parte de particulares y empresas. Como centro de competencia nacional, desarrolla una política global integrando misiones de investigación, apoyo, detección e inteligencia[42].

La SDLC define las estrategias operativas e investigaciones digitales en correferencia o en asistencia, de los servicios de la policía nacional, la gendarmería nacional, la Dirección General de Aduanas, así como de la Dirección General de Competencia, Consumo y Prevención del Fraude. También se encarga de gestionar los recursos digitales y coordinar la lucha contra el cibercrimen. Finalmente, establece y ejecuta cursos de formación nacionales en su área de especialización[43].

Por su parte, el Centro Judicial de la Gendarmería Nacional[44] (*Pôle judiciaire de la Gendarmerie nationale,* PJGN), cuenta en específico con el C3N: Centro de Lucha contra los Delitos Digitales (*Centre de lutte Contre les Criminalités Numériques*). El Centro brinda orientación y apoyo especializado en la lucha contra el cibercrimen y el crimen digital en general. Realiza o coordina las investigaciones de la Gendarmería Nacional relacionadas con esta nueva forma de delincuencia y realiza la vigilancia de los espacios públicos en Internet para detectar y recabar indicios de los delitos que en ellos se puedan producir.

[40] Police nationale (2022).
[41] Police nationale (2022).
[42] Police nationale (2022).
[43] Police nationale (2022).
[44] La Gendarmería Nacional, forma parte de las Fuerzas Armadas francesas, instituida para velar por la ejecución de las leyes, garantizar la seguridad pública y el orden público, particularmente en las zonas rurales, así como en las vías de comunicación. La policía judicial es una de sus misiones esenciales (Disponible en: https://www.gendarmerie.interieur.gouv.fr/).

VI. Reino Unido

1. La regulación de los ciber delitos

Al igual que en el resto del mundo, los llamados ciber delitos adoptan una serie de formatos diferentes, desde *hacking* y el uso de la web oscura hasta el troleo en las redes sociales y el *phishing* o robo de identidad. Los objetivos de tales actividades pueden ser cometer delitos sexuales, como *grooming* o compartir imágenes pornográficas, controlar o interrumpir los sistemas informáticos, o robar dinero, información o datos.

Dada la variedad de formas que estos delitos pueden adoptar, se encuentran contenidos en diversos cuerpos legales, según el ámbito legal de que se trate: *Computer Misuse Act 1990, Regulation of Investigatory Powers Act 2000 (RIPA), Data Protection Act 1998, Forgery and Counterfeiting Act 1981, Video Recordings Act 2010, Registered Designs Act 1949, Malicious Communications Act 1988, Communications Act 2003,* y *Protection From Harassment Act 1997.* Asi, una misma conducta puede ser sancionada bajo más de un cuerpo normativo. Por ejemplo, el troleo, que es una forma de hostigamiento en línea que consiste en enviar comentarios abusivos e hirientes a través de plataformas de redes sociales, puede ser perseguido bajo la Ley de Comunicación Maliciosa de 1988 y la Ley de Comunicaciones de 2003[45].

De acuerdo a la Estrategia Nacional de Ciberseguridad 2016-2021, los ciber delitos se clasifican en dos ámbitos[46]:

a) Delitos dependientes de la cibernética

Estos delitos solo pueden cometerse mediante el uso de dispositivos en línea, los que son tanto la herramienta para cometer el delito como el objetivo del mismo. Por ejemplo, un delito de este tipo es el *hacking*, esto es, el uso no autorizado o el acceso a dispositivos o redes mediante el uso de vulnerabilidades de seguridad o eludiendo los pasos de seguridad habituales para obtener acceso. Los delincuentes pueden piratear sistemas o redes para robar dinero o información, o simplemente para interrumpir negocios[47].

Por su parte, el software malicioso, o malware, se puede propagar entre computadoras e interferir con las operaciones de las computadoras. Puede ser destructivo, provocar fallas en el sistema o eliminar archivos, o usarse para robar datos personales. Los virus, gusanos, troyanos, spyware y ransomware son todos tipos de malware[48].

Los ataques de denegación de servicio distribuido (DDoS) se producen cuando se utilizan más de una, y a menudo miles, de direcciones IP únicas para inundar un servidor de Internet con tantas solicitudes que no pueden responder lo suficientemente rápido. Esto puede hacer que un servidor se sobrecargue

[45] The Crown Prosecution Service (s/f).
[46] HM Government (2016).
[47] The Crown Prosecution Service (s/f).
[48] The Crown Prosecution Service (s/f).

y se congele o bloquee, haciendo que los sitios web y los servicios basados en la web no estén disponibles[49].

La principal norma del Reino Unido relacionada con delitos o ataques contra sistemas informáticos, como el *hacking* o la denegación de servicio, es el *Computer Misuse Act 1990 (CMA)*. Son delitos bajo la CMA los siguientes[50]:

- Sección 1: Hacer que una computadora realice una función con la intención de asegurar el acceso no autorizado a material informático Este delito implica el "acceso sin derecho" y, a menudo, es el precursor de delitos más graves. Tiene que haber conocimiento por parte del infractor de que el acceso no está autorizado; la mera imprudencia no es suficiente. También debe haber habido una intención de acceder a un programa o datos guardados en una computadora.
  Este delito se sanciona, en juicio sumario, con prisión hasta por 12 meses y/o a una multa que no exceda el máximo legal; en caso de condena por acusación, a prisión por un período de hasta dos años y/o una multa.

- Sección 2: acceso no autorizado con la intención de cometer o facilitar la comisión de otro delito. Las penas asignadas a este delito son: en juicio sumario, prisión hasta por 12 meses y/o a una multa que no exceda el máximo legal; en caso de condena por acusación, prisión por hasta cinco años y/o multa.

- Sección 3: actos no autorizados con la intención de perjudicar el funcionamiento de una computadora. El delito se comete si la persona se comporta con imprudencia en cuanto a si el acto perjudicará, impedirá el acceso o entorpecerá las operaciones de una computadora. Se aplica a casos de DDoS.
  En juicio sumario, la sanción es prisión hasta por 12 meses y/o a una multa que no exceda el máximo legal; en caso de condena por acusación, prisión hasta por diez años y/o multa.

- Sección 3ZA: actos no autorizados que causen o creen un riesgo de daño grave, por ejemplo, al bienestar humano, el medio ambiente, la economía o la seguridad nacional. Esta sección está dirigida a quienes buscan atacar la infraestructura crítica nacional.
  Una persona culpable de un delito bajo esta sección puede ser sancionado, si es condenado por acusación, a una pena de prisión por hasta 14 años y/o una multa. Sin embargo, si el delito se comete como resultado de un acto que causa o crea un riesgo significativo de daños graves al bienestar humano o daños graves a la seguridad nacional, la pena puede ser cadena perpetua y/o una multa.

- Sección 3: fabricación, suministro u obtención de artículos para su uso en delitos contrarios a las secciones 1.3 o 3ZA. Según la sección 3(1) de la *Investigatory Powers Act 2016* (IPA), que entró en vigor el 27 de junio de 2018, es un delito interceptar intencionalmente una comunicación (en el Reino Unido y sin autoridad legal) en el curso de su transmisión por medio de un sistema de telecomunicaciones público o privado o un servicio postal público. La Sección 3A se ocupa de quienes fabrican o suministran malware.

[49] The Crown Prosecution Service (s/f).
[50] The Crown Prosecution Service (2019).

Este delito se sanciona, en juicio sumario, con prisión hasta por 12 meses y/o a una multa que no exceda el máximo legal; en caso de condena por acusación, a prisión por un período de hasta dos años y/o una multa.

b) Delitos facilitados por la cibernética

Se trata de delitos tradicionales, es decir, no dependen de computadoras o redes, sino que han sido transformados en escala o forma por el uso de Internet y la tecnología de las comunicaciones[51].

Entre estos ciber delitos se encuentran aquellos relacionados con la economía, como el fraude y los delitos contra la propiedad intelectual (piratería, falsificación, contrabando), los mercados en línea para artículos ilegales; las comunicaciones maliciosas y ofensivas, que incluyen aquéllas enviadas a través de las redes sociales (ciberacoso / troleo, *mobbing*); delitos dirigidos específicamente a personas, incluida la violencia cibernética contra mujeres y niñas (VAWG, por sus siglas en inglés), como revelar imágenes sexuales privadas sin consentimiento; los delitos sexuales contra niños (*grooming*, pornografía infantil), etc.[52]

Por ejemplo, el fraude informático utiliza Internet para obtener información personal confidencial de la víctima para que use un sitio web malicioso o instale malware en su dispositivo. Esto puede conducir al robo de identidad: los delincuentes recopilan suficiente información sobre una víctima para tomar su identidad y cometer fraude. Los datos personales se pueden utilizar para obtener documentos como pasaportes o permisos de conducir, abrir cuentas bancarias o cuentas de tarjetas de crédito, o hacerse cargo de cuentas bancarias existentes[53].

El fraude en línea se puede cometer de varias maneras. Por ejemplo: fraudes financieros electrónicos, como fraudes bancarios en línea y fraude de tarjeta-no-presente (CNP) habilitada para Internet; ventas fraudulentas a través de subastas en línea o sitios minoristas o a través de sitios web falsos; fraudes de marketing masivo y estafas al consumidor, incluidas las estafas de phishing y pharming; y fraudes de redes sociales / sitios web de citas)[54].

Los delitos bajo la *Fraud Act 2006* son aplicables a una amplia gama de fraudes cibernéticos al centrarse en la deshonestidad y el engaño subyacentes. La naturaleza del delito determinará los cargos que correspondan y los fiscales también pueden considerar delitos bajo las Theft Act de 1968 y 1978, la CMA, la *Forgery and Counterfeiting Act 1981* y la *Proceeds of Crime Act 2002 (POCA)*[55].

2. Medidas procesales

De acuerdo a la legislación británica, las autoridades encargadas de hacer cumplir la ley cuentan con diversos poderes de vigilancia. Por ejemplo, la *Police Act 1997* autoriza a la policía la entrada encubierta

[51] The Crown Prosecution Service (2019).
[52] The Crown Prosecution Service (2019).
[53] The Crown Prosecution Service (s/f).
[54] The Crown Prosecution Service (2019).
[55] The Crown Prosecution Service (2019).

e interferencia en sistemas de comunicaciones, y los servicios de seguridad tienen facultades similares en virtud de la *Security Service Act 1989* y la *Intelligence Services Act 1994*[56].

Otros poderes de vigilancia e interceptación de datos de comunicaciones están sujetos a la IPA 2016 y RIPA. Por ejemplo, IPA 2016 permite que ciertas autoridades públicas emitan órdenes de interceptación específicas, órdenes de interceptación masivas y órdenes de asistencia mutua. Las órdenes de interceptación selectiva pueden autorizar actividades por parte de organismos públicos autorizados para obtener datos secundarios y pueden obligar a organismos privados (incluidos los operadores de telecomunicaciones) a colaborar con las autoridades para realizar actividades de recopilación de inteligencia. Ciertas órdenes bajo la IPA de 2016 requieren aprobación dual ministerial y judicial, o (además) la aprobación del Primer Ministro[57].

Por último, en julio de 2018 el gobierno del Reino Unido anunció la construcción de un nuevo tribunal de vanguardia, diseñado específicamente para abordar los delitos cibernéticos, el fraude y los delitos económicos. El moderno centro legal con 18 salas de audiencia, desarrollado en asociación con la Corporación de la Ciudad de Londres y el poder judicial, el tribunal también se ocuparía de temas comerciales y de propiedad, así como de casos civiles, y reemplazaría a varios organismos jurisdiccionales, como la Corte de Magistrados de la Ciudad de Londres[58].

En el anuncio, se señaló que el cronograma para la construcción del nuevo complejo judicial estaba sujeto a la finalización de los arreglos de financiamiento y la obtención del permiso de planificación, se esperaba esté terminado en 2025[59]. Si bien el proyecto fue presentado en diciembre de 2020, el año pasado, éste habría sido objetado por diversas organizaciones civiles de defensa del patrimonio arquitectónico de Londres[60]. No hay información reciente del estado de avance del proyecto.

3. Servicios especializados de lucha contra el cibercrimen

La *National Crime Agency* (NCA) es la principal agencia del Reino Unido contra el crimen organizado; la trata de personas, armas y drogas; el ciber crimen; y los delitos económicos que cruzan las fronteras regionales e internacionales[61].

Action Fraud, el centro nacional de denuncia de ciber delitos, monitorea los ataques cibernéticos, el fraude en línea u otros incidentes de seguridad informática. También entrega orientación sobre los tipos de delitos cibernéticos en el Reino Unido y consejos de prevención[62].

Sin embargo, si se trata de informar un incidente de ciberseguridad por parte de una empresa, es posible que deba informarlo a la oficina del Comisionado de Información (ICO). Según las nuevas reglas del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) de la UE, a partir del 25

[56] Parker y Scrace (2021).
[57] Parker y Scrace (2021).
[58] Gov.uk (2018).
[59] Gov.uk (2018).
[60] Jessel (2021).
[61] National Crime Agency (2020).
[62] Howland (2021).

de mayo de 2018 es obligatorio que también informe las violaciones de datos al ICO dentro de las 72 horas desde ocurrido el incidente[63].

Junto a *Action Fraud*, la Oficina Nacional de Inteligencia contra el Fraude (*National Fraud Intelligence Bureau*, NFIB), que es parte de la Policía de la Ciudad de Londres, es el principal investigador de delitos económicos. La NFIB analiza los informes de delitos cibernéticos para detectar cualquier patrón emergente, como nuevos tipos de delitos en línea, o delitos en serie y reincidentes, o incluso crimen organizado[64].

Referencias normativas

Alemania:

German Criminal Code (Strafgesetzbuch – StGB). Disponible en: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html (noviembre, 2022).

Argentina:

Código Penal de la Nación Argentina. Disponible en: http://bcn.cl/24dgu (noviembre, 2022).

Código Procesal Penal de Mendoza, Ley N° 6.730, de 1999. Disponible en: http://bcn.cl/38zzc (noviembre, 2022).

España:

Código Penal. Disponible en: http://bcn.cl/1m8ob (Noviembre, 2022).

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Disponible en: http://bcn.cl/395qz (noviembre, 2022).

Francia:

Code penal. Disponible en: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2022-10-21/ (noviembre, 2022).

Code de procédure pénale. Disponible en: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/2022-10-21/ (noviembre, 2022).

[63] Action Fraud (s/f).
[64] Howland (2021).

Arrêté du 29 avril 2014 modifiant l'arrêté du 5 août 2009 relatif aux missions et à l'organisation de la direction centrale de la police judiciaire. Disponible en: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028911344 (noviembre, 2022).

Reino Unido:

Computer Misuse Act 1990. Disponible en: https://www.legislation.gov.uk/ukpga/1990/18/contents (noviembre, 2022).

Referencias bibliográficas

Action Fraud (s/f). Reporting fraud and cybercrime. Disponible en: https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime (noviembre, 2022).

Bundeskriminalamt (s/f). Cyber-crime. Disponible en: https://www.bka.de/EN/OurTasks/AreasOfCrime/Cybercrime/cybercrime_node.html (noviembre, 2022).

Colegio Criminológico de Madrid, España (2018). Disponible en: http://bcn.cl/395sf (noviembre, 2022).

Dirección General de Coordinación y Estudios Secretaría de Estado de Seguridad, Gobierno de España, Secretaría de Estado de Seguridad, Dirección General de Coordinación y Estudios (2021). Informe sobre la Cibercriminalidad en España. Disponible en: http://bcn.cl/395rm (noviembre, 2022).

Eurojust, European Union Agency for Criminal Justice Cooperation (s/f). Cybercrime. Disponible en: https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime (noviembre, 2022).

Gov.uk (2018). World-class fraud and cybercrime court approved for London's Fleetbank House site. Press release: Ministry of Justice and HM Courts & Tribunals Service. Disponible en: https://www.gov.uk/government/news/worldclass-fraud-and-cybercrime-court-approved-for-londons-fleetbank-house-site (noviembre, 2022).

HM Government (2016). National Cyber Security Strategy 2016-2021. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (noviembre, 2022).

Howland, Louise (2021). A guide to UK cybercrime legislation + helpful links. Ramsac. Disponible en: https://www.ramsac.com/blog/cybercrime-legislation-uk/ (noviembre, 2022).

Jessel (2021). City faces backlash after 'destructive' Parry scheme is tipped for approval. Architect's Journal. Disponible en: https://www.architectsjournal.co.uk/news/city-faces-backlash-after-destructive-parry-scheme-tipped-for-approval (noviembre, 2022).

Joissains, Sophie et bigot, M. Jacques (2020. Rapport d'information n° 613 (2019-2020) de, fait au nom de la commission des affaires européennes et de la commission des lois, déposé le 9 juillet 2020. Cybercriminalité: un défi à relever aux niveaux national et européen. Disponible en: http://www.senat.fr/rap/r19-613/r19-6133.html#toc101 (noviembre, 2022).

Ministerio Público Fiscal (s/f). UFECI. Disponible en: https://www.mpf.gob.ar/ufeci/ (noviembre, 2022).

National Crime Agency (2020). National Strategic Assessment of Serious and Organised Crime 2020. Disponible en: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file (noviembre, 2022).

Niethammer, Alexander; Rieks, David; Herfurth, Constantin, y Saerbeck, Stefan (2021). Cybersecurity Laws and Regulations Germany 2022. International Comparative Legal Guides, ICLG.com. Disponible en: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany (noviembre, 2022).

Parker, Nigel y Scrace, Benjamin (2021). Cybersecurity Laws and Regulations England & Wales 2022. International Comparative Legal Guides, ICLG.com. Disponible en: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/england-and-wales (noviembre, 2022).

Police nationale (2022). Sous-direction de lutte contre la cybercriminalité. Disponible en: http://bcn.cl/38m10 (noviembre, 2022).

Policía Nacional de España (s/f). Brigada Central de Investigación Tecnológica (B.C.I.T.). Disponible en: http://bcn.cl/395t0 (noviembre, 2022).

Schlun & Elseven Rechtsanwälte (s/f). Cybercrime, Internet Criminal Law and Computer Criminal Law in Germany. Disponible en: https://se-legal.de/criminal-defense-lawyer/cybercrime-internet-offences-in-germany/?lang=en#How-does-German-Law-Legislate-for-Cybercrime (noviembre, 2022).

The Crown Prosecution Service (s/f). Cyber / online crime. Disponible en: https://www.cps.gov.uk/crime-info/cyber-online-crime (noviembre, 2022).

-- (2019). Cybercrime - prosecution guidance. Disponible en: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (noviembre, 2022).

Disclaimer

Asesoría Técnica Parlamentaria, está enfocada en apoyar preferentemente el trabajo de las Comisiones Legislativas de ambas Cámaras, con especial atención al seguimiento de los proyectos de ley. Con lo cual se pretende contribuir a la certeza legislativa y a disminuir la brecha de disponibilidad de información y análisis entre Legislativo y Ejecutivo.