SECCIÓN I – DERECHO PENAL. PARTE GENERAL

SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL

RELACIÓN GENERAL

Thomas WEIGEND*

(A) Introducción: Alcance del informe

Este informe aborda los delitos relacionados con las tecnologías de la información y comunicación (TIC) y el ciberespacio. Estos delitos afectan a intereses individuales y colectivos que, en el siglo XXI, definen la calidad de vida de muchas personas. Por lo tanto, es un esfuerzo oportuno por parte de la AIDP el tratamiento de los temas de la "Sociedad de la Información y Derecho Penal", en su XIX Congreso Internacional de Derecho Penal.

Este informe se basa en las respuestas de 16 sistemas jurídicos[1] al cuestionario aprobado por el Consejo de Dirección de la AIDP y distribuido a los grupos nacionales. El Relator General está sumamente agradecido a los autores de los excelentes informes nacionales, que contienen una gran cantidad de información y consideraciones muy relevantes. Además, el Sr. Stanislaw Tosza ha presentado un informe especial sobre las redes sociales, que también ha sido una fuente muy valiosa para la elaboración de este Informe[2].

Las deliberaciones de la Sección I de los Congresos de la AIDP se han dedicado tradicionalmente a las cuestiones de la parte general del Derecho penal. Pero hay pocas cuestiones relativas a lo que normalmente se considera como la "parte general" que se refieran específicamente a las TIC y al ciberdelito. Por lo tanto, se ha tomado la decisión de definir el ámbito de los debates de la Sección I de manera más amplia y abarcar:

---

* Catedrático de Derecho penal. Universidad de Colonia (Alemania).

[1] Se han recibido informes nacionales de Argentina (AR), Austria (A), Bélgica (B), Brasil (BR), Finlandia (SF), France (F), Alemania (D), Grecia (GR), Hungría (HU), Italia (IT), Japón (J), Países Bajos (NL), Polonia (PL), Rumanía (RO), España (E) y Turquía (TR).

[2] La referencia al informe especial se hará mediante las siglas SNW del inglés “social networks” (redes sociales).

- la protección de los bienes jurídicos específicamente relacionados con las TIC y los desafíos del ciberespacio;

- La expansión de las prohibiciones penales, por ejemplo, a los actos preparatorios y a la posesión de materiales;

- El problema del respeto del principio de legalidad, sobre todo la exigencia de precisión de las prohibiciones penales;

- Los cambios en el concepto de autoría y la responsabilidad accesoria, especialmente con respecto a los proveedores de acceso y a los proveedores de alojamientos;

- La función del derecho penal en relación con otras formas de protección de los bienes jurídicos, sustancialmente mediante mecanismos específicos de internet como el bloqueo del acceso o la eliminación de sitios web;

- Reacciones legislativas al problema de que los usuarios de Internet a menudo permanecen en el anonimato;

- Los esfuerzos internacionales realizados para coordinar y armnozar la legislación en un área que, por definición, trasciende las fronteras nacionales.

La amplitud de la agenda de las deliberaciones de la Sección I es consecuencia de los problemas específicos de las TIC y el ciberdelito, que difieren en muchos aspectos de la criminalidad tradicional. Son precisamente estos retos que plantean las TIC y el ciberdelito los que los hacen interesantes y difíciles. Por lo general, los conceptos desarrollados para los delitos tradicionales no encajan muy bien para las TIC y el ciberdelito y, por lo tanto, pueden requerir una adaptación de forma un tanto flexible. Por otra parte, los principios que protegen contra una excesiva amplitud de la ley penal, como los principios de *última ratio* y de legalidad, pueden tener que ser redefinidos y adaptados a las características específicas de las TIC y el ciberdelito.

Las alusiones a las TIC y al ciberdelito se refieren a fenómenos muy diversos. Podemos distinguir cuatro tipos de conductas delictivas de las que se va a ocupar este informe[3]:

(1) delitos "comunes", por ejemplo, fraude o falsificación, que son cometidos por medio de la tecnología de la información y la comunicación;

(2) delitos dirigidos contra el buen funcionamiento de los sistemas de las TIC, por ejemplo, la piratería, la manipulación de los sistemas informáticos o la destrucción de los datos almacenados[4];

---

[3] Una clasificación similar puede verse en GR 1-2.

[4] En Finlandia solo los números (1) y (2) parecen ser reconducibles a la definición de ciberdelito (SF 1); ver también la definición de “ciberdelito propio” en Brasil (BR 2) y la algo diferente distinción en IT 1-2, 6.

(3) delitos "comunes", por ejemplo, el fraude, el acoso o la difamación, cometidos por medio de la red (*World Wide Web*)[5];

(4) los delitos contra intereses específicos de internet, por ejemplo, el "robo" o la manipulación de personalidades virtuales.

No requiere explicación que los problemas jurídicos y prácticos relacionados con estos cuatro tipos de delitos difieren significativamente entre sí[6]. Es una cuestión abierta si se puede o se debe intentar desarrollar principios comunes para las legislaciones penales relativas a las TIC y el ciberdelito. Este informe no pretende desarrollar un "sistema" de Derecho penal de las TIC y el ciberdelito que contenga normas para todos estos delitos. Por el contrario, el informe general se limita a presentar, de forma muy abreviada y simplificada, el "estado del arte" en relación con algunas de las cuestiones mencionadas en el encabezamiento que se puede extraer de los diversos sistemas jurídicos incluidos en este estudio.

(B) Bienes jurídicos protegidos por las TIC y Derecho penal de la cibercriminalidad

(1) Aspectos generales

(a) Los delitos convencionales "se digitalizan"

Las TIC y el ciberespacio han permitido a los delincuentes ser más "eficientes" que en épocas anteriores, cuando desean cometer fraudes, calumnias, violaciónes de derechos de autor y otros delitos tradicionales. Pueden utilizar las computadoras y / o la web con el fin de abordar, con un solo clic del ratón, millones de víctimas potenciales o para hacer gran daño a la reputación o los derechos de autor protegidos de una sola víctima. Pero en estos casos es solo el *modus operandi* lo que los diferencia de las formas tradicionales de conducta fraudulenta o calumniosa[7]; los bienes jurídicos afectados siguen siendo los mismos[8]. Como señala el informe neerlandés, a la hora de elaborar nuevos tipos penales para los delitos tradicionales "mediante el uso de las computadoras", hay que tener cuidado de evitar superposiciones o duplicidades imprecisas de disposiciones penales que cubren más o menos la misma conducta[9]. También puede haber problemas relacionados con el principio de igualdad cuando un acto que no es punible (o castigado con menos severidad) en el "mundo real" se

---

[5] En cuanto a la dimensión de los delitos cometidos mediante el uso de la web, ver BR 14: Según una encuesta, el 80% de los usuarios adultos de Internet en Brasil fueron víctimas de algún tipo de ciberdelito, como la invasión de perfiles en las redes sociales, phishing y virus.

[6] Una combinación de todos estos tipos de delitos en una ley ver AR 2.

[7] Una lista de bienes jurídicos “tradicionales” protegidos frente a las injerencias de las TIC puede verse en A 1, TR 1.

[8] El informe neerlandés se refiere a “una nueva dimensión del delito clásico”; NL 7.

[9] NL 7.

define como un delito grave cuando el autor emplea la tecnología de las TIC o la web para cometer el delito[10].

Ejemplos de versiones "informatizadas" de delitos tradicionales[11] que figuran en los códigos penales son el fraude mediante el uso de sistemas TIC[12], la revelación de secretos gubernamentales almacenados electrónicamente[13], la falsificación de los datos almacenados digitalmente[14] y la difamación o el acoso ("cyber bullying")[15]. Las infracciones del derecho de autor mediante el ofrecimiento o la descarga ilegal de material protegido en Internet es otro ejemplo de un delito "común" que ha asumido una dimensión cuantitativa diferente (y quizás cualitativa) cuando la comisión se ve facilitada por las oportunidades creadas por la web[16]. En Francia, la comisión de una violación de derechos de autor a través de una red de comunicación en línea o pública es considerada como una circunstancia agravante[17]. Por último, la pornografía (incluida la pornografía infantil) es hoy en día principalmente transmitida y distribuída electrónicamente, por lo que algunos ordenamientos jurídicos han introducido prohibiciones penales especiales relativas a la "pornografía en internet"[18].

---

[10] Cfr. B 13: El Tribunal Constitucional belga consideró una violación del derecho a la igualdad que el delito de ciberacoso llevara aparejadas penas más severas que el delito general de acoso.

[11] Belgica ha introducido un nuevo delito de proporcionar oportunidades ilegales para el juego en la red; B 10.

[12] Cfr. A 5, B 20, GR 11-15, 28-29, SF 6.

[13] Cfr. GR 5, 26-27.

[14] D 6, E 2, GR 28, J 3, SF 5-6. En los Países Bajos los Tribunales han ampliado el delito tradicional de falsificación de documentos escritos a manipulaciones similares de datos almacenados digitalmente; NL 15.

[15] Cfr. SNW 10.

[16] Cfr. B 11, GR 22-24, 30-31, NL 21, PL 5, SF 8-10 (mendionando los problemas específicos en la adaptación de las viejas disposiciones sobre las infracciones de los derechos de autor a las nuevas circunstancias), TR 3. Cfr. también E 7 (discutiendo la falta de adaptación de las leyes sobre infracciones de derechos de autor a la distribución de material protegido a través de la red).

[17] F 4.

[18] Cfr. AR 4, BR 6, F 4, J 4, RO 2-3. La legislación alemana todavía requiere la transferencia de algún “material” pornográfico y por lo tanto no llega a cubrir la transmisión (*streaming*) ni otras formas no materiales de transmisión de grabaciones digitales; D 8. El informe polaco (PL 5) señala que la tecnología digital ofrece nuevas posibilidades de creación de material pornográfico: "La promoción y expansión de las tecnologías digitales han contribuido a la elaboración de instrumentos relativamente baratos que permiten crear realidad virtual, incluído material pornográfico, sobre todo pornografía infantil simulada, es decir, materiales generados artificialmente que muestran imágenes más o menos realistas de una persona inexistente o imágenes modificadas de adultos realizadas para parecer niños, o niños utilizados "virtualmente", lo que significa modificar las imágenes de los

Cuando los autores utilizan las redes sociales para establecer contacto con posibles víctimas de delitos sexuales, en especial con los niños, cruzan la línea entre la delincuencia tradicional (contacto con los niños con el fin de cometer actos sexuales con ellos) y el tipo de delito que depende de la existencia de Internet. El "Grooming" o captación de menores para un potencial abuso sexual ha sido tipificado como delito en muchos países[19].

(b) Nuevos delitos

Otras infracciones penales cometidas mediante las TIC y ciberdelito atentan contra intereses que no existían antes de la invención de las computadoras y el advenimiento de la *World Wide Web*. Constituye uno de los retos de la ley penal del siglo XXI definir correctamente los bienes jurídicos, para protegerlos de menoscabos indebidos y al mismo tiempo trazar los límites del ámbito de aplicación de los tipos penales. Esto último es importante porque la invención de las TIC y la creación del ciberespacio han abierto a las personas una serie de nuevas posibilidades y una nueva esfera de la libertad no sólo de reunir información, sino también de pasar su tiempo, de ser creativo, de comunicar con los demás y de pretender intereses comerciales. Si la ley penal se aplica en términos demasiado amplios, las personas se ven privadas de esta nueva libertad y su gran potencial para su propia realización. Sería un alto precio a pagar por la sociedad que sus miembros tengan miedo de navegar por la red o de utilizar la comodidad que ofrecen las TIC en su vida cotidiana por temor a sanciones penales si dan un paso en falso. Por lo tanto, es crucial que las prohibiciones penales se diseñen de tal manera que frenen las conductas gravemente dañosas, pero que no restrinjan demasiado severamente la libertad del mundo cibernético[20].

Varios sistemas jurídicos ponen de relieve la necesidad de proteger el funcionamiento de los sistemas individuales TIC (ordenadores, redes, etc) a través de las leyes penales[21]. En un sentido más amplio, se considera que necesita protección[22] la confianza del público en el "funcionamiento" de los sistemas TIC y del ciberespacio, ya que es "un interés macro supra-individual, que engloba todos los intereses difusos, sin los cuales es imposible la

---

niños". Constituye una cuestión abierta si tales materiales se deben poner al mismo nivel que los materiales que representan niños reales. Mientras que la legislación polaca cubre este tipo de imágenes, el derecho austriaco, por ejemplo, limita la punibilidad de la distribución, exhibición etc. de las imágenes que parecen representar hechos reales (A 6-7).

[19] Cfr., por ejemplo, A 7, E 3.

[20] Cfr. IT 12 sobre la utilidad limitada del concepto de bien jurídico protegido (*Rechtsgut*) para evitar una expansión excesiva del Derecho penal en este ámbito.

[21] Cfr., por ejemplo, TR 1.

[22] Cfr. BR 2-3, E 1, J 1.

comunicación segura en el ciberespacio"[23]. El principal interés que debe protegerse aquí es la confidencialidad, integridad y disponibilidad de los sistemas de información y datos electrónicos[24]. Como señala el informe nacional polaco, existen de hecho libertades individuales en juego cada vez que se pone en peligro el funcionamiento del ciberespacio:

"*El principal bien jurídico protegido por la ley penal en relación con el espacio virtual (ciberespacio) es la tradicional libertad y seguridad de una persona, sin embargo, entendida desde una perspectiva específica, orientada al ciberespacio. Por ello, el derecho es entendido, entre otras cosas, como derecho a la privacidad del individuo, como la confianza de las personas en el sistema electrónico, como la confianza en los documentos y datos almacenados en dicho sistema. También el derecho del individuo a decidir sobre si la información está protegida (es decir, el derecho del individuo a decidir libremente, por ejemplo, en cuanto al derecho libre y exclusivo para administrar la información de que dispone el individuo, así como a decidir libremente sobre el alcance y el tipo de los datos divulgados relativos a la persona), así como el derecho constitucional a la protección de la privacidad y el secreto de las comunicaciones*"[25].

Este interés general en el mantenimiento de la integridad "institucional" de las TIC y el mundo cibernético puede ser dividido en aspectos más específicos, los cuales son sensibles a la interferencia ilegal.

(2) Los intereses particulares

(a) La interferencia con los sistemas de las TIC

Un interés fundamental es la "integridad" de los sistemas TIC privados o públicos, es decir, el funcionamiento de estos sistemas de acuerdo con las normas operativas y el acceso proporcionado por el legítimo propietario. Puesto que cualquier interferencia no autorizada puede provocar un daño grave y amenaza con socavar la confianza en el buen funcionamiento del sistema de las TIC en cuestión, muchos sistemas jurídicos prevén sanciones penales para tal interferencia[26]. La transmisión no autorizada y los cambios en los datos, la eliminación y la destrucción de los datos y el software así como impedir el acceso a un sistema TIC son descripciones típicas de un delito que puede describirse

[23] E 1.
[24] GR 2.
[25] PL 2. Una valoración similar puede verse en F 1. El informe nacional griego señala correctamente que "los datos electrónicos constituyen … los medios de participación en la sociedad de la información"; GR 3.
[26] En relación con los problemas de un sistema jurídico donde no se dispone aún de tal protección cfr. GR 6-10, 25-26.

mejor como "sabotaje informático"[27]. En algunos sistemas jurídicos, la destrucción, falsificación u ocultación de los datos almacenados en algún otro sistema de TIC es considerado como un delito distinto[28]. La infección de un sistema de TIC por parte de un virus o malware similar resulta normalmente abarcada por las disposiciones generales contra la interferencia con los sistemas TIC[29]. En algunos estados se castiga incluso la posesión intencional de este tipo de malware[30], pero la infección no intencional (incluso temeraria) de un sistema por un virus no constituye una infracción penal[31].

(b) Piratería (*Hacking*)

Con el fin de manipular o sabotear un sistema de TIC, es necesario obtener acceso al mismo. Como la mayoría de los sistemas de TIC están protegidos contra el acceso no autorizado, una persona necesita vulnerar el mecanismo de seguridad instalado por el propietario con el fin de obtener información confidencial almacenada en el sistema o eventualmente manipular el sistema[32]. Muchos sistemas jurídicos han tipificado penalmente este acto de "piratería" del sistema de TIC de otro, independientemente de la finalidad del delincuente. Por lo tanto, la legislación moderna describe el delito como la simple entrada en un sistema[33] de TIC protegido sin autorización[34], incluso si el delincuente no obtiene (o incluso puede no desear obtener[35]) información almacenada en el sistema[36]. En cuanto al interés por la "integridad" de un sistema de TIC, la piratería es un delito de peligro, ya que la entrada ilegal en sí misma no afecta al buen funcionamiento del sistema de TIC en cuestión[37].

---

[27] Cfr., por ejemplo, A 2, B 6, BR 3, D 4-5, E 1, F 2, IT 2, J 1-2, PL 3-4, RO 2, SF 4-5, TR 2-3.
[28] Cfr., por ejemplo., A 4, D 7, F 3, IT 3, J 3.
[29] Cfr. AR 3, A 5, B 8, D 7, E 3, PL 4, TR 3.
[30] Cfr. BR 6-7 (*lex ferenda*), F 3-4.
[31] Cfr. SF 4.
[32] Una fenomenología de los métodos de piratería (*hacking*) puede verse en SNW 5-6.
[33] En Grecia solo el acceso no autorizado a los datos almacenados es objeto de sanción penal; GR 4.
[34] Están protegidos los datos *en route* de un ordenador a otro, pero no necesariamente es así cuando se envían entre ordenadores pertenecientes a la misma persona, cfr. GR 4.
[35] De acuerdo con la legislación austríaca, la piratería informática es punible solo si el infractor actúa con la intención de obtener información que pretende utilizar o hacer pública y para causar un perjuicio a otro u obtener un beneficio para sí; A 1-2.
[36] Cfr., por ejemplo, AR 9, B 5 (distinguiendo entre piratería informática “externa” e “interna”), E 1, F 2, IT 3, J 2, PL 2-3, RO 1-2, SF 3-4, TR 2.
[37] Cfr. TR 8.

(c) Vigilancia ilegal

Un delito relacionado pero diferente es la violación de la confidencialidad de un sistema de TIC mediante la instalación o el uso de dispositivos de vigilancia o software[38]. Las escuchas telefónicas (privadas) ilegales constituyen un precursor anterior de este delito, y en ocasiones ese delito se ha extendido a los sistemas de TIC[39]. La vigilancia ilegal difiere de la piratería (*hacking*) en el hecho de que el autor no sólo entra en un sistema de TIC sin autorización, sino que también persigue obtener la información que se encuentra allí almacenada o que será transmitida a ese sistema.

(d) Prohibiciones penales innovadoras

El mundo cibernético no sólo abre nuevas posibilidades para la comunicación, el comercio y la difusión de información y de opinión, sino que también crea nuevos intereses que puedan verse perjudicados por terceros. El Derecho tiene que reaccionar ante estas nuevas sensibilidades. Por lo tanto, no es de extrañar que algunos sistemas jurídicos hayan creado nuevas definiciones de delitos dirigidos específicamente a la protección de intereses individuales en el mundo cibernético.

En Bélgica se introdujo en 2005 una disposición penal muy general contra el acoso cibernético. De acuerdo con la ley, constituye un delito que puede cometer cualquier persona el "utilizar una red o servicio de comunicaciones electrónicas u otros medios electrónicos para molestar o causar daños a su interlocutor, o instalar cualquier dispositivo destinado a la comisión del delito y la tentativa de cometerlo"[40]. Cabe preguntarse si (y si es así, por qué) molestar a una persona a través de medios electrónicos es más censurable que las molestias realizadas cara a cara.

Otro de los riesgos típicamente asociados a Internet es la difusión rápida de fotos e imágenes de personas sin su consentimiento o contra su voluntad. El legislador español ha abordado este problema mediante la creación del delito de difusión, revelación o cesión a terceros, sin la autorización de la persona afectada de "imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal

---

[38] A 2-3, D 5-6, F 2-3, IT 3, 9, PL 3, SF 3. La futura ley brasileña también castigará la producción, venta y adquisición de códigos de acceso y software que posibilite la entrada en un sistema TIC sin autorización; BR 4. Japón no dispone de una prohibición genera de la vulneración del secreto de las TIC sino solo leyes especiales para estos supuestos, por ejemplo, la ley sobre servicios de telecomunicaciones; J 2-3.

[39] Cfr. B 6-8, E 1-2.

[40] B 7.

de esa persona".[41] Es interesante señalar que este tipo penal no se aplica a la realización no autorizada de fotografías o grabaciones, sino sólo a su difusión no autorizada, que normalmente se lleva a cabo mediante el uso de Internet.

Un delito similar en los Países Bajos contiene una definición más restrictiva pues sólo castiga la "distribución de los datos conseguidos a través de una violación de la confidencialidad". Este tipo penal trata de resolver problemas de prueba cuando la información confidencial se transmite a través de Internet y no está claro si la persona que la ha distribuido era también responsable de la obtención ilegal de la información[42].

El mundo virtual del ciberespacio sin duda es distinto del mundo real, pero hay comunicaciones entre los dos, y las personas pueden verse afectadas por la pérdida de "ciberbienes" de igual forma que por la pérdida de bienes tangibles[43]. Este hecho plantea la cuestión de si las leyes contra el robo y el fraude, que principalmente se refieren a los bienes y propiedades del mundo "real", también se pueden aplicar al mundo cibernético. En un reciente caso neerlandés, un niño había adquirido, invirtiendo mucho tiempo y esfuerzo, un amuleto y una espada en un juego de rol online. Los infractores obligaron al muchacho mediante amenazas (en la vida real) a transferirles a ellos la espada y el amuleto (en el ciberjuego). El Tribunal Supremo holandés confirmó su condena por robo, pero este resultado se basó en una interpretación amplia del término "bienes"[44], que puede no ser aplicable en otras jurisdicciones. Un tribunal de apelaciones de Finlandia, por ejemplo, en un caso muy similar no aceptó la interpretación amplia del delito de robo y llegó a la conclusión de que la adquisición no autorizada de "muebles de hotel" virtuales no era punible[45]. Estos casos muestran que los legisladores pueden tener que introducir disposiciones específicas que castiguen el "robo cibernético" cuando los objetos adquiridos ilegalmente por el autor no son "cosas" tangibles sino imágenes que tienen un valor (sólo) en el mundo cibernético[46].

La usurpación de la identidad virtual que una persona utiliza para la comunicación en la red[47] afecta a una dimensión más "real"; está a menudo - pero no necesariamente - relacionada con los intentos de defraudar en el

---

[41] E 3.
[42] NL 6-7.
[43] See SNW 16-17.
[44] Una discusión de este caso puede verse en NL 7-9.
[45] SF 10-11.
[46] Cfr. también SNW 18.
[47] La enorme incidencia del fraude de identidad puede observarse en las estadísticas contenidas en SNW 2.

comercio real[48]. Por ejemplo, un autor puede obtener ilegalmente datos de acceso de la víctima y realizar pedidos de bienes en una tienda de internet, cargando el pago de la factura a la víctima. Algunos sistemas jurídicos (todavía) no disponen de leyes penales específicas que comprendan este tipo de comportamiento fraudulento[49], mientras que otros tienen definiciones bastante amplias del delito. De acuerdo con el Derecho francés, por ejemplo, constituye delito adoptar ilegalmente la identidad de otra persona o utilizar los datos que permitan identificarle - incluyendo su dirección IP o su apodo en una red social - con el fin de perturbar su calma o la de otra persona o para atacar a su honor o reputación[50]. Disposiciones similares se pueden encontrar en algunos estados de los Estados Unidos de América[51]. La legislación federal de los Estados Unidos así como la de Canadá prevén la punibilidad de la adquisición o uso ilegal del "medio de identificación" de otra persona con la intención de cometer con él un acto ilícito[52]. En otros sistemas jurídicos, los tribunales han aplicado a este tipo de casos los tipos penales de falsificación informática[53], fraude mediante representación falsa[54], la suplantación ilegal de otra persona[55], la difamación o la difusión de información que viola la privacidad personal[56]. El método para obtener acceso a la identidad de otra persona en la red puede, por supuesto, ser por sí mismo delictivo, por ejemplo, piratería o interferencia con la integridad de un sistema de TIC[57].

Dada la gran importancia de la reputación y la integridad de las “ciberpersonalidades” especialmente en las redes sociales, los legisladores

---

[48] Diversas definiciones de fraude de identidad y de robo de identidad pueden verse en SNW 3-4.

[49] Cfr., por ejemplo, A 6, D7, E 3, J 4 (pero es un delito en Japón colarse en una red social protegida usando una identidad falsa; J 11), NL 10 (si bien en los Países Bajos tienen un concepto amplio del delito de "engaño para obtener beneficios", puede abarcar algunos de los casos en cuestión), TR 3 (si bien Turquía tiene delitos de obtención, entrega o difusión ilegal de datos personales y la obtención de beneficios ilegales mediante el abuso de los sistemas TIC).

[50] F 4. Se dice que esta disposición también abarca la intención de causar un daño material, por ejemplo, mediante la solicitud de productos utilizando la ciberidentidad de la víctima. Polonia tiene una disposición muy similar; P 4; y existe un proyecto de ley en el mismo sentido en Argentina; AR 14.

[51] SNW 10.

[52] Citado en SNW 9, 11. Ver también el proyecto de Ley argentina con el mismo efecto; SNW 12.

[53] See B 9.

[54] SNW 15 (en relación con Inglaterra).

[55] SNW 15-16 (en relación con la India, Italia y Polonia).

[56] SF 10-11.

[57] SNW 13-14.

pueden así ver la necesidad de tipificar como delito la usurpación o falsificación de la identidad virtual de una persona aun cuando el autor no tenga la intención de causar daño material. De acuerdo con algunas opiniones, la colocación de anuncios o la difusión de información falsa bajo la ciberidentidad de otra persona puede causar graves daños al "buen nombre" de esa persona en el mundo virtual[58] y puede, por lo tanto, ser considerado como más dañino que la pérdida de dinero a través de órdenes falsas a una tienda online[59]. Sin embargo, puede ser difícil definir correctamente la esencia del delito sin interferir con el anonimato de Internet en general[60].

(C) *Actus reus* y *Mens rea* de los delitos relacionados con las TIC y los ciberdelitos

Dada la novedad de los delitos relacionados con las TIC y los ciberdelitos, es interesante observar cómo los legisladores se enfrentan a la tarea de definirlos. ¿Existen características típicas de las definiciones de los nuevos delitos en el ámbito de las TIC y el ciberdelito?

(1) Definición de *actus reus*

Los delitos tradicionales, como el asesinato, las lesiones corporales o el fraude, a menudo se definen de tal manera que la causación de un cierto efecto perjudicial es parte del *actus reus*. En lo que respecta a los delitos relacionados con las TIC y los ciberdelitos, esta parece ser la excepción y no la regla; en la mayoría de los casos se considera delictivo realizar un cierto acto, independientemente de las consecuencias que el acto puede o no haber causado al bien jurídico protegido. Por ejemplo, se tipifican como delitos la obtención de acceso a una red protegida de las TIC o la transmisión de imágenes pornográficas a través de la red[61]. Estos actos sin duda tienen algún aspecto de "resultado" - por ejemplo, una persona que trata de distribuir imágenes pornográficas, pero no puede obtener acceso a Internet desde su ordenador portátil no ha "transmitido" las imágenes[62]. Pero el daño que el legislador desea evitar - la violación de la confidencialidad de cierta información en el caso de la piratería, el estímulo del mercado de la pornografía infantil - no necesita producirse para sancionar al autor por un delito consumado.

---

[58] Cfr. SNW 7.

[59] En un caso decidido en Finlandia, el autor había colocado un anuncio online con el (ciber) nombre de un niño de 12 años de edad, presuntamente en busca de sexo con otro chico; SF 10-11.

[60] Cf. NL 10, SNW 19.

[61] Cfr, por ejemplo, F 5, PL 5-6.

[62] Por esta razón, el informe nacional español mantiene que todos los delitos relacionados con las TIC son delitos de “resultado”; E 4. Pero esto se aplica solo si se utiliza el término “resultado” en un sentido empírico: obtener acceso a un sistema TIC protegido constituye así el “resultado” de la actividad del autor realizada con la finalidad de conseguir dicho acceso.

La mayoría de los delitos relativos a las TIC y los ciberdelitos por lo tanto pueden ser catalogados como delitos como delitos de peligro ("abstracto")[63]. Sólo una minoría de las definiciones legales requiere un menoscabo real de un sistema de TIC para la condena[64]. A menudo, la causación del daño que el tipo penal pretende evitar - por ejemplo, dañar los datos a través de la interferencia de un sistema de TIC - es considerada como una circunstancia agravante[65].

La mayoría de los delitos relacionados con las TIC y los ciberdelitos pueden ser cometidos por cualquier persona, si bien una posición especial de responsabilidad especial puede llevar a una condena mayor. Por ejemplo, en Grecia, una persona que viole el secreto de los datos puede ser castigado con mayor severidad si es un proveedor de servicios de telecomunicaciones o su representante legal o un responsable de la protección del secreto[66].

(2) Definición de *mens rea*

La gran mayoría de los típicos delitos relativos a las TIC y exigen la intención por parte del autor[67]. Esto incluye, en muchos sistemas jurídicos, la variante del dolo eventual, es decir, la toma consciente y voluntaria de un riesgo de que el acto o resultado prohibido suceda[68]. Pero varios ordenamientos jurídicos prevén también la sanción del delito imprudente. Por lo general, basta la imprudencia con respecto la causación del daño a los datos o a un sistema de TIC después de haber obtenido acceso a él ilegalmente (y deliberadamente) [69]. De acuerdo con el Derecho neerlandés, los profesionales (pero no los usuarios normales) son penalmente responsables por la distribución imprudente de malware[70]. La violación de las leyes de protección de datos y la posesión de dispositivos para la recogida secreta de información también puede ser cometida por imprudencia de acuerdo con el Derecho francés[71], y en Italia la omisión de adoptar medidas para asegurar la privacidad puede ser cometida por imprudencia[72]. Sin embargo, estas

---

[63] Cfr. TR 4.

[64] Cfr. A 8, PL 6, RO 3. En Italia, se ha criminalizado cualquier acto significa destruir información, programas o datos usados por el Estado y otro organismo público o datos que tienen una utilidad pública; IT 9.

[65] Cfr. B 11, IT 2.

[66] GR 32.

[67] Cfr. BR 9, D 9, J 5, RO 4.

[68] Cfr. I 5, J 5, SF 2. Sin embargo, con relación a la posesión de pornografía infantil la legislación austriaca exige al menos conocimiento por parte del autor de que el archivo que visiona o descarga contiene imágenes pornográficas; A 9.

[69] Cfr. B 12, TR 5; ver también PL 6.

[70] NL 27; cfr. también AR 7 para el delito de destrucción imprudente de documentos oficiales.

[71] F 6-7; cfr. también GR 34.

[72] IT 5.

disposiciones aisladas parecen ser excepciones a la regla general de que las violaciónes de las leyes relacioandas con las TIC e informáticas sólo pueden ser castigadas cuando el autor ha actuado intencionadamente.

(D) Extensión de la criminalización: Preparación y posesión

(1) Preparación

El carácter algo esquivo de los delitos relativos a las TIC y los ciberdelitos, que puede generar problemas de prueba del daño real o del peligro, parece haber dado lugar a una práctica legislativa generalizada consistente en la incriminación de actos preparatorios de la conducta lesiva, incluida la mera posesión de dispositivos o software que pueden ser utilizados para ataques a la integridad de los sistemas de TIC. Esto es excepcional, ya que la mayoría de sistemas jurídicos generalmente no consideran la simple preparación de una conducta delictiva como merecedora de sanción penal, salvo que se trate de unl delito muy grave o de la conspiración de dos o más personas[73]. Pero en el ámbito de los delitos relativos a las TIC y del ciberdelito muchos sistemas jurídicos han seguido la solicitud del artículo 6 del Convenio sobre la Ciberdelincuencia para criminalizar la producción, venta, obtención para su utilización, importación, distribución o de otro modo puesta a disposición de dispositivos, incluidos los programas informáticos, destinados o adaptados principalmente para el propósito de cometer cualquiera de los delitos relativos a las TIC enumerados en el Convenio, así como de las contraseñas del ordenador, los códigos de acceso o datos similares mediante los cuales la totalidad o una parte de un sistema informático es accesible, con la intención de que sean utilizos con el fin de cometer cualquiera de estos delitos.

Algunos ordenamientos jurídicos han copiado casi literalmente esta amplia definición de los actos preparatorios del Convenio sobre la Ciberdelincuencia[74]. Ejemplos típicos de actos preparatorios a lo largo de estas líneas son el "phishing" de direcciones web u otros datos personales (por ejemplo, cuentas bancarias y números de tarjetas de crédito, contraseñas) que se puede utilizar con el fin de defraudar a las personas o para causar daño a otros en sus en la red[75]. Lo mismo se aplica a la producción o la venta de dispositivos o software

---

[73] Cfr. NL 18.

[74] Cfr. B 24, BR 10 (proyecto de ley de brasil), IT 3, NL 19, RO 5-6, SF 15; ver también SNW 4-5.

[75] Cfr., por ejemplo, D 7, IT 4, 6-7, J 8-9. Las leyes italiana y polaca extienden la punibilidad a la producción, adquisición, venta o puesta a disposición de otras personas de contraseñas de ordenador, códigos de acceso o cualquier otro dato que permita a alguien tener acceso a un sistema de información protegido mediante medidas de seguridad; IT 8, PL 8.

que pueden ser utilizados para la piratería[76], para interceptar las comunicaciones[77] o para eludir la protección de material con derechos de autor[78]. En Japón, una disposición similar se refiere a la información sobre registros electromagnéticos codificados en tarjetas de crédito o de pago[79]. El Derecho austriaco castiga únicamente la venta o posesión de software que ha sido específicamente diseñado o adaptado para la comisión de hechos punibles; pero la doctrina ha criticado esta restricción como demasiado limitada y exige que el software en cuestión sea "idóneo" para ser utilizado en la comisión de delitos[80]. La ley austriaca prevé expresamente la posibilidad de desistimiento del delito (y quedar así impune) mediante la evitación del uso del software en cuestión[81]. Otra limitación es el requisito de que el autor actúe con la intención de cometer un delito relacionado con las TIC o un ciberdelito, que excluye a los expertos en seguridad informática del alcance de la prohibición penal[82].

Una forma especial de acto preparatorio que se ha tipificado como delito en algunos ordenamientos jurídicos es el "acoso" (*grooming*) de niños, es decir, entrar en contacto con ellos a través de internet, con la intención de un posterior abuso sexual o de producción de pornografía infantil[83].

La extensión de la responsabilidad penal a los actos preparatorios, como consecuencia del Convenio sobre la Ciberdelincuencia, parece no haber encontrado mucha oposición, con la excepción de la doctrina de España que critica que se castigue con la misma pena la preparación y la consumación del delito relacionado con las TIC[84].

(2) Posesión

La criminalización se extiende no sólo a los que producen o distribuyen dispositivos o software que son idóneos para ser utilizados para la comisión de delitos relacionados con las TIC o ciberdelitos, sino que en muchos sistemas jurídicos también comprende la mera posesión de este tipo de herramientas, incluidas las que se van a utilizar para interceptar las comunicaciones[85]. Una excepción es Grecia, donde el legislador se ha mostrado contrario a la tipificación

---

[76] A 6 (exigiendo una finalidad comercial), B 24, D 7, HU 8, J 6-7.
[77] B 24.
[78] B 25, E 7, F 8, TR 8.
[79] J 7.
[80] A 10-11. Una disposición similar puede verse en RO 5.
[81] A 11.
[82] NL 20.
[83] NL 21
[84] E 7. Ver también las críticas en IT 8.
[85] Cfr., por ejemplo, A 12, B 24-26, HU 8, IT 8-9, RO 6.

penal de la mera posesión de herramientas electrónicas que pueden ser utilizados para la piratería[86].

Con respecto a la pornografía infantil, la mera posesión de ciertos materiales, también en forma de archivos de datos, se define con frecuencia como delito[87]. Si bien existe un amplio consenso sobre que el almacenamiento de estos materiales en la propia computadora es un delito, porque la venta y adquisición de pornografía infantil perpetúa el mercado ilícito de estos materiales y, por lo tanto, promueve el abuso de los niños[88], las opiniones están divididas en cuanto a si "la posesión" se extiende (o debería extenderse) a la simple visualización de material pornográfico en la red. Algunos Estados incluyen en el tipo penal el hecho de acceder a sabiendas a materiales de pornografía infantil en Internet[89], mientras que otros requieren algún tipo de posesión permanente[90]. Otro tema polémico se refiere a la cuestión de si la prohibición sólo se extiende a las imágenes "reales" de los niños en poses o actividades sexuales o también comprende las imágenes virtuales, por ejemplo, dibujos generados por ordenador o ilustraciones[91].

(3) Responsabilidad de los proveedores

Muchos delitos pueden ser cometidos mediante la publicación en Internet de cierta información, imágenes o declaraciones. Libelo y difamación, incitación al odio racial, fraude, violaciones de las leyes de derechos de autor y sobre pornografía son los tipos más comunes de tales delitos. Por razones técnicas, su comisión no es posible sin la actividad de los proveedores de servicios de Internet (ISP) de diversos tipos, que actúan como intermediarios entre las personas que desean publicar información y los que la reciben. ¿Hasta qué punto puede un ISP ser penalmente responsable? Los sistemas legales han dado diferentes respuestas a esta pregunta, pero la tendencia se dirige a limitar la punibilidad a situaciones en las que un proveedor ha tenido conocimiento de los

---

[86] Una exposición de los motivos y de las propuestas de reforma puede verse en GR 44-50.

[87] La legislación polaca extiende la prohibición de poseer datos de propaganda fascista u otros regímenes totalitarios fascistas así como de datos que inciten al odio por motivos nacionales, étnicos, raciales, religiosos, PL 8-9. La legislación turca extiende la prohibición a la pornografía que implique violencia, animales, cadáveres humanos o comportamientos sexuales "no naturales" (que puede incluir el fetichismo y la homosexualidad); TR 9.

[88] Cfr. B 27.

[89] Esto se aplica, por ejemplo, en Austria (A 11), Finlandia (SF 8) y Alemania (D 13-14).

[90] Cfr. B 26-27, argumentando que un simple espectador no posee "a sabiendas" materiales pornográficos a pesar de que se almacenen temporalmente en la memoria RAM de su ordenador; ver también E 8, F9, GR 50-53, IT 10, RO 6, PL 9.

[91] Este es el enfoque, por ejemplo, del Derecho belga, griego e italiano; B 27, GR 18-21, IT 4.

contenidos delictivos en un sitio sometido a su cuidado y no adopta las medidas adecuadas.

La primera cuestión se refiere al tipo de potencial responsabilidad penal de los ISP de acuerdo con las normas generales del Derecho penal. Los ISP pueden ser calificados como colaboradores o cómplices en cualquier delito cometido mediante la publicación de información ilícita en los sitios que alojan oa los que dan acceso, y pueden ser penalmente responsables de la omisión de intervenir (por ejemplo, eliminar contenido censurable de su sitio) y así (hipotéticamente) causar un resultado penalmente sancionado por la ley. Pero este último concepto plantea la pregunta relativa al fundamento jurídico que puede existir para el deber de actuar del ISP[92], y si la responsabilidad por omisión se puede reconocer en absoluto cuando la definición del delito no exige un resultado, sino (sólo) la realización de ciertos actos[93]. La responsabilidad accesoria y la responsabilidad por omisión requieren el conocimiento de la existencia de la información cuestionable en el sitio web proporcionado por el ISP en cuestión. En los sistemas jurídicos que no tienen reglas especiales sobre la responsabilidad de los ISP, su falta de conocimiento normalmente excluye cualquier responsabilidad penal, ya que, como señala el informe nacional de Japón, "los proveedores de servicios y similares no están obligados a realizar una vigilancia continua de la información ilegal que se suba a la red"[94].

Muchos sistemas jurídicos europeos han adaptado su legislación al modelo establecido por la Directiva sobre el comercio electrónico de la UE de 2000[95]. La Directiva establece que los Estados miembros no podrán imponer una obligación general a los ISP -incluidos los proveedores de acceso, proveedores de sistemas almacenamiento y proveedores de sitios web[96]- "de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas

---

[92] Un análisis extenso de este tema puede verse en GR 54-59. Un alto tribunal italiano declaró la responsabilidad penal de un ISP en calidad de cómplice por omisión, de una violación a la privacidad cometida por uno de sus usuarios, ya que no había informado específicamente a los usuarios de sus obligaciones en materia de información confidencial de acuerdo con lo dispuesto en la Ley. Ahora bien, en la medida en que esta obligación se aplica sólo para el área de la privacidad de los datos, esta sentencia no puede ser extrapolada a otras áreas del Derecho; IT 10-11.

[93] Un breve análisis de estos problemas puede verse en A 12-14, NL 26, TR 10.

[94] J 9. Afirmaciones similares pueden verse en HU 8, RO 6.

[95] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

[96] El informe nacional turco señala correctamente que en la Web 2.0 puede ser difícil distinguir entre simples hosts y proveedores de contenidos; TR 11.

de hechos o circunstancias que indiquen actividades ilícitas"[97]. La Directiva pretendía evitar la censura proactiva y los consiguientes efectos amedrentadores en materia de libre circulación de información[98]. Pero este privilegio para los ISP, que normalmente excluye la responsabilidad criminal de los proveedores, se ha limitado de varias maneras.

En primer lugar, los proveedores pierden la protección del privilegio tan pronto como van más allá de su función de servir como un mero conducto o de proporcionar una memoria caché para la comunicación en la red, por ejemplo mediante el inicio de la transmisión de los datos, la selección del receptor o la modificación de la información transmitida o almacenada[99]. En segundo lugar, el ISP puede ser penalmente responsable cuando ha sido informado de los contenidos ilícitos específicos existentes en su dominio y que no elimina inmediatamente[100]. Esta información puede provenir de organismos oficiales[101] o de los usuarios[102]. En Francia, los ISP están obligados a invitar a los usuarios de manera positiva a alertarles de determinados contenidos prohibidos, como pornografía infantil, incitación a la violencia y ataques a la dignidad humana, y deben retirar inmediatamente de sus sitios los contenidos que son "manifiestamente ilegales"[103].

El privilegio de los ISP no se aplica a las personas que establecen hipervínculos a otros sitios web. Generalmente, se considera que una persona que enlaza su sitio web a otro proporciona el contenido de la otra página web[104]. Pero el establecimiento consciente de enlaces debe diferenciarse de simples listados de páginas web, como hacen habitualmente por los motores de búsqueda.

En general, la ley en muchos Estados parece dejar suficiente libertad para los ISP de varios tipos y evita hacerles responsables de los contenidos que no

---

[97] Artículo 15 (1) Directiva 2000/31/CE.

[98] NL 23; ver también la jurisprudencia del Tribunal de Justicia de la Unión Europea citada en IT 11.

[99] Cfr. artículos 12 (1), 13 (1) (a) Directiva 2000/31/CE. Ver también A 13-14, B 22, 28-29, F 11-12, PL 9-10, TR 9-10.

[100] A 13-14, BR 10, D 18, F 12-13, PL 10, TR 9-10. Ejemplos prácticos de condenas penales con este fundamento pueden verse en E 8, NL 25.

[101] En los Países Bajos el fiscal puede ordenar a un ISP a hacer inaccesible un contenido ilegal; NL 23.

[102] E 9.

[103] Cfr. F 9-10. El informe nacional de Finlandia (SF 13) establece que el operador puede ser hecho responsable por el material ilegal y racista si "no *elimina* claramente por iniciativa propia el material ilegal". No está muy claro si esta obligación requiere que el proveedor de Internet busque activamente estos materiales – lo que sería una excepción a la regla general - o si debe actuar sólo si es alertado de la existencia de material ofensivo.

[104] Cfr. NL 26, TR 9.

pueden controlar y que no pueden ni siquiera conocer. Se puede considerar, sin embargo, en qué medida se debe alentar a los ISP a ser proactivos en la recopilación de información sobre ciertos materiales ofensivos.

(E) Sanciones específicas

Además de las penas de prisión y de multa, algunos ordenamientos jurídicos prevén sanciones específicas para los delitos aquí analizados. Los dispositivos ofensivos pueden ser decomisados[105]. Más en concreto, en Bélgica, el fiscal puede utilizar todos los medios técnicos para que los datos sea inaccesibles si estos datos "son el objeto del delito o han sido producidos por el delito y si son contrarios al orden público o a las buenas costumbres o constituyen un peligro para la integridad de los sistemas informáticos o de datos almacenados, procesados o transmitidos a través de dicho sistema." Utilizando esta potestad, los fiscales pueden ordenar a un proveedor de servicios de Internet que borren el nombre del dominio de un sitio que infrinja la ley, por ejemplo, mediante la distribución de pornografía infantil[106]. En Francia, el tribunal puede, como una sanción adicional por la violación de los derechos de autor, prohibir al infractor utilizar las comunicaciones online por un máximo de un año[107]. Una sanción similar puede ser impuesta de acuerdo con las leyes turcas como una alternativa a la pena de prisión de hasta un año[108].

Debe poners énfasis aquí en l principio general de que las sanciones no deben ser desproporcionadas en relación con la gravedad del delito. En algunos Estados los legisladores tienden a reaccionar de forma exagerada a la amenaza de los delitos relacionados con las TIC y los ciberdelitos estableciendo penas excesivamente altas para estos nuevos delitos[109].

(F) Retos y límites de la legislación penal

Los legisladores que se acercan a la tarea de definir los delitos relacionados con las TIC y los ciberdelitos a menudo se enfrentan a problemas específicos. Se encuentran en un dilema: deben definir la acción penal correspondiente, de tal manera que la disposición no devenga obsoleta cuando se inventen nuevas tecnologías, nuevos dispositivos de hardware o simplemente nuevos términos y se incorporen al mercado; y, por otro lado, los legisladores deben respetar el principio de legalidad, que exige que las leyes penales sean precisas y que describan con una terminología clara la exacta conducta prohibida. Una preocupación política se refiere al riesgo de que las leyes penales excesivamente amplias puedan disuadir a las personas, que temen la responsabilidad penal, de

---

[105] Cfr. A 14.
[106] B 33.
[107] F 8, 16.
[108] TR 11.
[109] Cfr. GR 60.

hacer uso de las oportunidades que ofrecen las TIC y el ciberespacio. En el fondo, existe una preocupación porque las prohibiciones penales en el ámbito de las TIC y el ciberespacio pueden interferir con importantes derechos y libertades civiles.

(1) Teniendo en cuenta el progreso tecnológico

Ante el riesgo de que los avances tecnológicos y terminológicos pueden dejar rápidamente obseleta la redacción de una ley penal, algunos legisladores tratan de mantenerse al tanto de los últimos avances; por ejemplo, una ley penal francesa se refiere a la transferencia de datos a "le nuage Internet"[110]. Otros legisladores tratan de usar lenguaje no técnico, genérico[111] referido en general al derecho civil o administrativo, o emplear ficciones jurídicas expresas. Por ejemplo, en el código penal alemán los "escritos" se definen como comprensivos - entre otros objetos – de dispositivos de almacenamiento de datos, imágenes y otras representaciones[112]. Esta extensión, no obstante, deja lagunas en lo que respecta a la pornografía, ya que sin duda no llega a cubrir la transmisión de videos[113]. El legislador argentino ha abordado el problema frontalmente; una ley penal se refiere a ciertas tecnologías y añade las palabras "o la tecnología que en el futuro la remplace"[114].

(2) Respeto del principio de legalidad

El enfoque argentino claramente está en contradicción con el ideal de precisión de las prohibiciones penales, pero también lo es el uso de términos genéricos amplios tales como "interferencia" como descripción de una conducta penal[115], e incluso los términos "datos", "sistema de información" e "interceptación" pueden ser vagos a menos sean definidos específicamente en la ley[116]. Los ordenamientos jurídicos difieren con respecto a su sensibilidad en este tema, que por lo general afecta a los legisladores que intentan hacer frente a fenómenos multifacéticos y cambiantes, como los delitos relacionados con las TIC y los ciberdelitos. Cuando el legislador evita formulaciones excesivamente amplias de la conducta prohibida, los tribunales se sienten en ocasiones obligados a extender las disposiciones restrictivas existentes mediante el recurso a la

---

110 F 8.

111 Cfr., por ejemplo, A 10, GR 37, 43, NL 16, RO 5.

112 § 11 sec. 3 Código penal alemán. Cfr. también B 18-19 (discutiendo el empleo del término genérico "système informatique" en el derecho belga).

113 D 12.

114 AR 8. Una formulación similar ("comparable con aquellos de cualquier otra forma") puede verse en SF 1, 12.

115 Ver NL 6, 16. Otros ejemplos son las "definiciones" legales abiertas relativas a la pornografía infantil en la legislación brasileña (BR 7); ver adicionalmente RO 4, TR 6-7 (discutiendo las expresiones "datos personales" y "comunicaciones").

116 Cfr. GR 31-32, 35-36, 38.

analogía con el fin de adaptarse a un mundo cambiante. En ese sentido, los tribunales neerlandeses han interpretado el término "bienes" contenido en el delito de robo como comprensivo también de los datos[117], un enfoque que corre el riesgo de entrar en conflicto con la "interpretación literal" que exige el principio de legalidad.

Si las prohibiciones penales se definen en términos generales, vagos o los tribunales los extienden más allá del sentido natural de las palabras[118], pueden disuadir a las personas de hacer uso de los derechos que las normas penales sólo pretenden limitar. Para evitar este efecto amedrentador de las leyes penales, los legisladores italianos y japoneses han limitado ciertos delitos a los actos que se realizan "sin motivos justificados"[119], Grecia ha limitado algunos delitos a los actos realizados "sin derecho"[120], y en España una determinada conducta es punible solamente cuando produce graves perjuicios[121]. Exigir una intención (específica) puede ser también una medida para evitar un exceso de disuasión[122]. La introducción de la discreción del fiscal para no procesar[123], sin embargo, probablemente no resuelve el problema, pues el individuo no puede determinar de antemano si el fiscal se abstendrá de perseguir su caso. Sería preferible limitar de la manera más restricitva posible la conducta prohibida, y si se producen cambios tecnológicos pertinentes, el legislador pueda adaptar la redacción de las leyes a la nueva situación.

(3) Respeto de los límites constitucionales

Cualquier criminalización de la comunicación en el ciberespacio está en conflicto latente con la libertad de expresar las propias opiniones[124], protegida en las constituciones de la mayoría de los países, y puede afectar también a la libertad de prensa[125] y la libertad de creación artística[126]. Las violaciones de estas libertades solo son admisibles en la medida en que sean proporcionadas al mal

---

117 NL 6; cfr. también, sobre la misma cuestion, B 13, GR 6-8, y adicionalmente en IT 11, J 6.

118 Otro ejemplo de una reacción excesivamente restrictiva a los peligros percibidos es la práctica antigua de Turquía de bloquear el acceso a dominios enteros tras encontrarse allí un archivo objetable; cfr. TR 7.

119 IT 7, J 6-7.

120 Un análisis de este término y críticas relativas a su vaguedad puede verse en GR 41-43.

121 E 6.

122 Cfr. D 11, IT 7, 9.

123 Cfr. B 18.

124 Cfr. GR 64-65.

125 Cfr., por ejemplo, AR 10-11, BR 11-12, D 19, E 10, GR 63-65, J 10, PL 11, TR 10.

126 GR 62-63.

que pretenden combatir[127]. Algunos ordenamientos jurídicos han consagrado en sus constituciones el "principio del lesividad", que limita el alcance de la ley penal a las conductas que lesionan o ponen en peligro inminente un bien jurídico digno de protección. En estos países, se puede argumentar que algunos delitos relacionados con las TIC violan este principio, como por ejemplo la piratería sin más efectos perjudiciales[128]. La criminalización de la simple posesión de herramientas que pueden ser utilizadas para la piratería también puede poner en peligro la libertad de investigación[129].

La aplicación actual de las leyes penales a los delitos relacionados con las TIC y los ciberdelitos puede violar el principio de culpabilidad, cuando los tribunales tratan de evitar problemas de prueba condenando a personas cuyo número IP ha sido identificado como uno de los que sirven para introducir determinados datos ofensivos en el sistema, pero sin pruebas de que hayan cometido intencionalmente el delito o hayan colaborado en su comisión[130]. Si bien dicha aplicación injusta de las leyes penales no es específica de los delitos relacionados con las TIC y los ciberdelitos, ciertas prohibiciones penales relativas a las comunicaciones en Internet por lo general entran en conflicto con la libertad de expresión. Los legisladores deben ser conscientes de este potencial conflicto y deben respetar el libre mercado de la comunicación que ofrece el ciberespacio.

(G) Alternativas a la criminalización

De acuerdo con el principio de *ultima ratio*, el Derecho penal debe emplearse sólo como un último recurso para abordar un problema social. Sin embargo, varios informes nacionales han señalado que los legisladores de sus respectivos ordenamientos jurídicos parecen considerar que las leyes penales constituyen el principal medio de lucha contra los delitos relacionados con las TIC y los ciberdelitos[131].

Existen mecanismos administrativos y civiles para hacer frente al fenómeno de la delincuencia cibernética y las TIC.

(1) Medidas administrativas

Una herramienta importante para las agencias administrativas es ordenar la retirada de determinados contenidos o "cerrar" páginas web ofensivas. En varios

---

[127] Cfr. la jurisprudencia del Consejo constitucional francés en relación con la lucha contra las violaciones del derecho de autor; F 15.
[128] Cfr. TR 10.
[129] Cfr. GR 61.
[130] Cfr. TR 10.
[131] Cfr. E 11, PL 11, RO 7, TR 11. El número de condenas por estos delitos no parece ser muy elevado, de acuerdo con el informe nacional austriaco, las condenas por delitos informáticos - con la excepción de la pornografía infantil - en 2007 se encontraban en el rango de un dígito; A 15.

Estados existe esta posibilidad, por ejemplo, con respecto a sitios web que muestran pornografía infantil: un organismo administrativo puede ordenar al proveedor de acceso el bloqueo del acceso al sitio web en cuestión[132]. Estas órdenes están dirigidas a los proveedores de acceso nacionales, pero efectivamente cubren también el acceso a sitios web operados en el extranjero. En Japón, una empresa privada se encarga de filtrar y bloquear sitios web peligrosos[133], y en los Países Bajos el sector privado de ISP se ha comprometido a cerrar sitios ofensivos cuando existan denuncias formuladas por los usuarios[134]. Sin embargo, en algunos países existe una fuerte oposición a tales leyes y prácticas por el temor a que puedan abrir la puerta a la censura en Internet. Por ejemplo, las leyes de Alemania y Polonia, que prevén el establecimiento de una lista de sitios web pornográficos a bloquear, se enfrentaron a tantas críticas que las leyes respectivas nunca entraron en vigor[135].

(2) Medidas de Derecho civil

En muchos sistemas jurídicos las víctimas individuales pueden demandar por daños y perjuicios ocasionados por la actividad ilícita en la red[136]. Sin embargo, parece que este camino es difícil y engorroso para las víctimas privadas y, por lo tanto, rara vez se utiliza[137], con la única excepción de las violaciónes de los derechos de autor[138]. En los Países Bajos existe una alternativa interesante al proceso judicial ante un tribunal, donde el sector privado de ISP ha establecido un procedimiento de notificación y retirada: cuando una persona o una institución se encuentra con una actividad o información ilícita en un sitio web, puede informar de ello al proveedor de servicios. La queja se envía entonces al cliente. Si no obtiene una respuesta satisfactoria, el ISP puede retirar el sitio o eliminar la información ofensiva[139]. Existe un sistema similar de autorregulación en Hungría,

---

[132] F 17, IT 14, RO 7, SF 13, TR 12; cfr. también HU 9. En Bélgica, el juez de instrucción de Bruselas puede ordenar a los proveedores el bloqueo de sus servicios cada vez que considere que existe un peligro para la salud pública, la seguridad pública, la seguridad nacional, la defensa nacional o los intereses de los consumidores; B 32-33.

[133] J 11.

[134] NL 31.

[135] D 20, PL 12-13. Del mismo modo, en Grecia se dice que el derecho constitucionalmente protegido de la participación en la sociedad de la información impide cualquier bloqueo general del acceso a la web; GR 68.

[136] Cfr., por ejemplo, A 15, BR 12, GR 67, IT 13 (señalando que la responsabilidad civil sólo requiere negligencia, mientras que se necesita prueba de la intención en casos penales paralelos).

[137] Cfr. F 16, PL 11. En Turquía, los particulares pueden demandar la retirada de contenidos y que se publique una respuesta; TR 11.

[138] D 19, NL 29. En Grecia, el titular de los derechos de autor perjudicado puede exigir que el acceso al sitio web infractor sea bloqueado por el ISP correspondiente; GR 67-68.

[139] NL 30.

pero allí actúa la Asociación de Proveedores de Contenido húngara que puede eliminar el contenido ilícito o incluso imponer una prohibición temporal a los miembros que violen las normas[140].

(3) Limitar el anonimato de los usuarios

Una forma indirecta de obviar los delitos relacionados con las TIC y especialmente los ciberdelitos es limitar el anonimato de los usuarios, ya que el manto del anonimato incita a las personas a realizar o recibir contenidos ilícitos, pensando que no han de temer su detección. Si se consigue que los usuarios se muevan en la red usando su verdadero nombre y / o divulgando sus datos de identificación, el atractivo del ciberdelito podría reducirse significativamente. Por otro lado, es parte de la atracción del mundo cibernético que las personas pueden cambiar de identidad y jugar con ella; la eliminación de esta libertad, sin duda, tiene un grave impacto en lo que se concibe como la libertad en la red.

Un camino intermedio podría ser, bien exigir a los usuarios que se registren ante los proveedores de acceso revelando su verdadera identidad, o bien exigir a los proveedores de acceso que almacenen datos (como números IP) que posibiliten la posterior identificación de los usuarios individuales siempre que surja una sospecha de conducta criminal en la red. Por último, se podría considerar una prohibición de ficheros cifrados o, al menos, la obligación de que los usuarios revelen contraseñas y códigos de cifrado con el fin de una investigación penal.

(a) Registro de usuarios

En la medida en que el acceso a Internet es de pago, los proveedores de acceso tienen normalmente relaciones contractuales con las personas que utilizan sus servicios. Pero este tipo de contratos no requieren la determinación fiable de la verdadera identidad del usuario, sobre todo cuando se utilizan dispositivos de acceso prepago[141]. Por otra parte, el hecho de que una persona tenga un contrato de servicio con un proveedor de acceso no prueba que en un momento dado dicha persona haya utilizado los servicios de ese proveedor. Por lo tanto, el registro de usuarios tiene poco impacto en la facilitación de la investigación (y, en consecuencia, en un incremento de la disuasión) del ciberdelito.

(b) Almacenamiento de datos de acceso

Un método más fiable de conectar a los usuarios individuales con ciertas actividades en la red (por ejemplo, la colocación de contenido ofensivo en un sitio web o el visionado de una página web con este contenido) es registrar y almacenar los números IP. Con la ayuda de los números IP y las respectivas

---

[140] HU 10. Hungría también cuenta con un Centro Nacional de Ciberseguridad que coordina las respuestas a las graves violaciones de la seguridad de las TI contra las redes del gobierno y las infraestructuras críticas de información.

[141] Cfr. D 18, F 19, GR 74, PL 15, SF 16.

direcciones, es posible rastrear las actividades en la red de dispositivos individuales TIC, tales como ordenadores o teléfonos móviles.

Las leyes nacionales difieren en cuanto a la obligación de los proveedores de acceso de almacenar temporalmente los números IP. En Japón no se requiere dicho almacenamiento y, por tanto, sólo es posible un control posterior del uso de Internet de un individuo si el proveedor ha grabado y almacenado los datos relevantes para fines comerciales[142]. La situación es similar en Alemania, donde una ley que preveía el almacenamiento automático de números IP ha sido declarada inconstitucional y los partidos gobernantes no han sido capaces de ponerse de acuerdo sobre una nueva ley[143]. Pero la gran mayoría de los Estados han impuesto una obligación legal a los proveedores de acceso de almacenar datos de acceso individualizados por períodos de entre tres meses y dos años[144]. Los proveedores están obligados a facilitar estos datos a las agencias de aplicación de la ley y los tribunales cuando así lo soliciten en el marco de una investigación criminal[145]. Estas leyes constituyen una excepción al principio general del secreto de las telecomunicaciones, que impide a los proveedores la revelación de los datos relativos a las conexiones realizadas o intentadas por sus clientes[146]. Mediante la aprobación de leyes sobre el almacenamiento obligatorio de datos de acceso, los Estados miembros de la UE han cumplido con la obligación impuesta por la Directiva de la UE 2006/24/CE de 2006[147].

(c) Limitación de cifrado de archivos

El cifrado de archivos en sí no está prohibido en ninguno de los Estados que han presentado informe. La mayoría de los sistemas jurídicos también aceptan que el cifrado de archivos supone un obstáculo para las investigaciones penales; obligar mediante coacción a un sospechoso a revelar sus contraseñas o a decodificar sus archivos podría ser considerado, en estos Estados, como una violación del principio de que nadie puede ser obligado a declarar contra sí mismo[148]. Pero hay

---

142 J 12.

143 Cfr. D 21.

144 Cfr. A 17 (6 meses), B 19 (un año), BR 11 (un año), F 10, 13-14 (un año; en Francia esta obligación se extiende a los propietarios de cibercafés e incluso a los empresarios privados que ofrecen a sus empleados acceso a internet; F 18), HU 11 (un año), IT 15-16 (un año, y dos años para el tráfico de datos telefónicos), PL 15 (2 años), RO 8 (6 meses), SF 15-16 (3 meses), TR 9 (un año).

145 A 17, B 29-30, E 11, F 18, GR 73, HU 11, PL 15, RO 6, SF 16.

146 Cfr. PL 14.

147 Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.

148 Cfr. AR 12, A 18, D 21, E 11, GR 75, J 12, RO 9, SF 16, TR 13.

Estados que permiten a las fuerzas del orden contar con la ayuda de expertos[149] y de los ISP[150] para descifrar los archivos si es necesario para una investigación criminal. El Derecho francés va más allá. No sólo se considera el cifrado de un documento como una circunstancia agravante cuando el documento ha sido utilizado para cometer o facilitar la comisión de un delito[151]; la legislación francesa considera delito que una persona se niegue a revelar a las autoridades judiciales el código secreto - conocido por él - de un documento cifrado que haya sido utilizado para la preparación, facilitación o comisión de un delito, o que podría ser utilizado para impedir la comisión de un delito[152]. No está claro si este delito de negativa a proporcionar un código secreto también puede ser cometido por el acusado en un caso penal, si él indirectamente puede autoincriminarse proporcionando el código secreto.

(4) Desplazamiento de la carga de la protección hacia los usuarios

Algunos delitos en el ámbito de las TIC y el ciberespacio pueden ser fácilmente impedidos mediante la debida precaución por parte de las personas que sean víctimas de estos delitos, en particular, mediante el uso de software antivirus y la protección del propio ordenador y el acceso a Internet y a determinados sitios web mediante el uso de contraseñas seguras. Esto plantea la cuestión de si la carga de la evitación de los delitos relacionados con las TIC y el ciberdelito se puede desplazar al usuario, haciéndole responsable de proteger sus propios intereses en lugar de imponer sanciones a los autores de crímenes que habrían sido fáciles de evitar.

Varios Estados animan a los usuarios a emplear las posibilidades de autoprotección[153]. Sólo unos pocos Estados, sin embargo, van tan lejos como para que sea un delito no usar la protección adecuada y, por lo tanto, posibilitar no sólo la propia victimización, sino también el uso de los propios dispositivos TIC para la distribución de software malicioso a los demás o para otras infracciones de la ley[154].

---

[149] B 34.

[150] PL 16.

[151] F 6.

[152] F 20.

[153] Cfr., por ejemplo, B 33.

[154] Este es el caso de Austria, pero el relato nacional considera que es poco probable que una multa administrativa por infringir la obligación de utilizar una protección adecuada para las instalaciones de telecomunicaciones jamás se impondría a un usuario privado; A 16. En Francia, un usuario de Internet que no puede proteger su acceso del uso no autorizado de terceros, después de haber sido advertido por la autoridad competente para hacerlo, comete una infracción si se produce una violación de los derechos de autor utilizando su conexión a internet, F 17-18. En Italia, es punible el hecho der no adoptar medidas de seguridad para la protección de la privacidad de acuerdo con lo dispuesto por la ley; IT 5.

Por otro lado, el descuido de la víctima con respecto a la seguridad de la web no proporciona una defensa general para los acusados de delitos relacionados con las TIC y los ciberdelitos. En algunos sistemas jurídicos, la piratería o el hecho de interferir con algún otro sistema de TIC se castigan con independencia de que estuviera protegido[155]. Pero en otros Estados, los delitos de acceso ilegal a sistemas de TIC se define de tal manera que no se puede cometer a menos que hubiera habido algún tipo de protección que el delincuente logró burlar[156], y esta la solución podría acomodarse mejor al principio de que el Derecho penal debe ser la *última ratio* en la protección de bienes jurídicos[157].

(H) Aspectos de la internacionalización

La ciberdelincuencia, casi por definición, trasciende las fronteras nacionales. Este hecho plantea cuestiones relativas a la competencia jurisdiccional y a la aplicación de las leyes nacionales a conductas transnacionales. También convierte en una necesidad la cooperación internacional en la lucha contra la ciberdelincuencia.

(1) Competencia jurisdiccional

La mayoría de los Estados ejercen su jurisdicción y aplican sus leyes penales a los delitos cometidos en su territorio. Esto también es válido para los ciberdelitos cuando el autor actúa (por ejemplo, utiliza un dispositivo para obtener ilegalmente el acceso a una red TIC) en el territorio del Estado de que se trate. Los Estados también ejercen su competencia jurisdiccional si el autor actúa en el extranjero, pero el resultado, de acuerdo con lo dispuesto en el tipo delictivo aplicable, tiene lugar en el territorio del Estado[158]. Las opiniones difieren en cuanto a lo que significa "resultado" en el contexto de la ciberdelincuencia. En algunos sistemas jurídicos, el mero hecho de que un sitio web con contenido penal pueda ser visto en un Estado es considerado como motivo suficiente para que ese Estado ejerza su competencia jurisdiccional[159]; mientras que otros requieren que se produzca en dicho Estado un "daño" más directo, como la pérdida de bienes por un

---

En Turquía, se exige a los "proveedores de uso masivo" de acceso a Internet (tales como cibercafés) que apliquen y utilicen herramientas de filtrado para bloquear el acceso a contenidos ilícitos en Internet; TR 12.

155 Cfr. A 16, RO 8, TR 13. En Grecia, el imputado acusado de acceder ilegalmente a un sitio web sin protección puede, sin embargo, alegar un error de hecho o de derecho sobre el consentimiento del propietario que le exima de responsabilidad criminal; GR 69.

156 Cfr., por ejemplo, D 20 (§ 202a Código penal alemán sobre espionage de datos), E 11, HU 10, IT 14, PL 13.

157 Cfr. GR 70.

158 Cfr., por ejemplo, A 18, BR 13, §§ 3, 9 (1) Código penal alemán, IT 16, RO 9.

159 Cfr. D 21-22, TR 13-14.

persona que reside en el Estado, o la interferencia de un sistema informático situado en el territorio del Estado[160].

Con respecto a los actos realizados en el extranjero, algunos Estados extienden su jurisdicción a estos actos si el autor tiene la ciudadanía del Estado del foro y el acto es punible tanto en el Estado del foro como en el que se realizó[161]. El Convenio sobre la Ciberdelincuencia, de hecho, requiere en esta situación la aplicación de la jurisdicción del Estado[162].

Otro fundamento reconocido para el ejercicio de la jurisdicción es el hecho de que el delito cometido en el extranjero haya afectado negativamente al Estado que reivindica la competencia jurisdiccional o a uno de sus ciudadanos. En este último caso, existe normalmente el requisito de la "doble incriminación", es decir, el acto debe ser punible donde se ha cometido y en el Estado del foro[163].

Puede ser conveniente definir reglas de competencia que tengan en cuenta la calidad "intangible" de ciertos ciberdelitos y, por lo tanto, abandonar la conexión tradicional de la jurisdicción al "territorio". Por otro lado, se debe evitar la creación de un sistema de jurisdicción universal para todos los ciberdelitos con el fundamento de que estos se cometen allí donde los sitios web delictivos pueden ser vistos[164].

(2) Armonización internacional

Casi todos los informes nacionales han mencionado la importante influencia que ciertos instrumentos jurídicos internacionales ha tenido en la legislación sobre la materia de sus Estados. El máximo común denominador es el Convenio sobre la Ciberdelincuencia de 2001, que ha tenido un impacto en la legislación, incluso en aquellos Estados que no lo han ratificado[165]. En la Unión Europea e incluso más allá[166], la Decisión marco 2005/222/JAI de la UE relativa a los ataques contra los sistemas de información ha tenido una influencia de similar importancia en la legislación nacional. La Directiva 2006/24/CE de conservación de datos también ha sido incorporada a la legislación de la mayoría de los Estados miembros. Además, han sido de relevancia ciertos instrumentos de la UE relativos a la lucha contra concretos delitos, como la Decisión marco 2004/68/JAI relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, ya que algunos

---

160 Cfr. A 18, SF 16.
161 Cfr., por ejemplo, § 7 (2) Código penal alemán, J 13, NL 32.
162 Artículo 21 (1) (d) del Convenio sobre la Cibercriminalidad.
163 Cfr., por ejemplo, § 7 (1) Código penal alemán, PL 16. En Turquía no se exige el requisito de la doble incriminación (T 14), y en los Países Bajos no se aplica a todos los delitos (NL 32).
164 De acuerdo, GR 76-77.
165 Cfr. AR 13, BR 13, GR 78-79, IT 17, TR 15.
166 Cfr. TR 14.

de los delitos a los que se refieren estas directivas se cometen normalmente a través de internet[167]. Los representantes de varios Estados continúan trabajando activamente de manera conjunta con el fin de adaptar la legislación armonizada a los últimos avances en las TIC y el ciberespacio.

(l) Tendencias de futuro

Los informes nacionales han señalado varias ideas sobre las tendencias de futuro de los delitos relacionados con las TIC y los ciberdelitos y la legislación en la materia. Algunas de estas ideas son:

- La necesidad de establecer requisitos intencionales menos exigentes, que permita a los Tribunales superar los problemas de prueba de otro modo insuperables[168];

- La voluntad de conciliar los intereses de los titulares de los derechos de autor y de los usuarios con respecto al acceso a bajo costo a música protegida[169];

- La necesidad de tipificar nuevos comportamientos nocivos tales como el ciberacoso escolar, el ciberacoso, el robo de identidad, el *spam* o correo no deseado, y la adquisición y distribución ilegales de datos[170];

- La necesidad de proteger los sistemas de información y la red en su conjunto contra el robo y otros delitos[171];

- La cuestión de si se debe ampliar la responsabilidad penal de los ISP[172];

- La necesidad de una legislación sistemática y amplia sobre la ciberdelincuencia[173].

El relator nacional de los Países Bajos señaló que, por el momento, la balanza se inclina hacia una mayor supervisión y control, y que es difícil predecir cuándo la balanza volverá a la libre circulación de la información como principio básico del Estado de Derecho[174]. El próximo Congreso de la AIDP puede ayudar a lograr un retorno al ideal de la libertad de Internet y a reducir los esfuerzos de algunos Estados por obtener un control excesivo sobre el ciberespacio mediante la ampliación excesiva de la ley penal.

---

[167] Cfr. PL 17.
[168] A 20.
[169] FR 21.
[170] AR 14-15, E 12, SF 20.
[171] J 14, SF 20.
[172] IT 17.
[173] BR 15.
[174] NL 32.