REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 11 NÚM. 1 (2022) • PÁGS. 121-146 • DOI 10.5354/0719-2584.2022.60913
RECIBIDO: 29/1/2021 • APROBADO: 23/10/2021 • PUBLICADO: 30/6/2022

DOCTRINA

Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia

About the reach of the purposes of penalties on the criminal phenomenon of cybercrime

Jon López Gorostidi
Universidad de Deusto, España

RESUMEN En este estudio se lleva a cabo un análisis de uno de los elementos capitales del derecho penal: la pena. Más concretamente, se estudia la adecuación de las construcciones tradicionales sobre los fines de la pena en el ámbito del cibercrimen, un fenómeno con características criminológicas muy diferenciadas de la delincuencia tradicional. Para ello, tras una aproximación inicial a la delincuencia en el ciberespacio, se aborda el encaje de esta en los postulados fundamentales de cada una de las teorías de la pena por separado, con el fin de extraer conclusiones preliminares y peculiaridades propias de los ciberdelitos, siendo conscientes de que estas teorías aportan un parámetro crítico y no una solución inequívoca a la ejecución penal.

PALABRAS CLAVE Ciberdelincuencia, pena, fines de la pena, retribución, prevención.

ABSTRACT This study analyses one of the key elements of criminal law: penalty. More specifically, it studies the adequacy of the traditional constructions on the purposes of penalties in the field of cybercrime, a phenomenon with very different criminological characteristics from traditional crime. To this end, after an initial approach to crime in cyberspace, we address its fit in the fundamental postulates of each of the theories of penalties separately in order to draw preliminary conclusions and peculiarities of cybercrime, being aware that these theories provide a critical parameter and not an unequivocal solution to criminal enforcement.

KEYWORDS Cybercrime, penalty, purposes of penalties, retribution, prevention.

Introducción

Actualmente, pocos ámbitos de nuestra vida privada y en sociedad escapan de la influencia de los sistemas de información y, en especial, de internet. En consecuencia, la proliferación de los ciberdelitos en los últimos años ha sido una constante, junto a las consecuencias jurídicas aparejadas a ellos. En este estudio se lleva a cabo un examen de la vigencia y de la aplicación de las teorías de los fines de la pena a la ciberdelincuencia, observando los caracteres criminológicos propios que presentan estas figuras delictivas.

Introducción a la ciberdelincuencia

La caracterización de la ciberdelincuencia en nuestros días

La ciberdelincuencia o cibercrimen[1] es un fenómeno criminal que se ha visto altamente potenciado en los últimos años dada la democratización del uso de los sistemas informáticos, la redes y, en especial, de internet en nuestra sociedad. Así, la tendencia indica que cada vez empleamos más tiempo de nuestro día en navegar por la red y, en consecuencia, cada vez trasladamos más parcelas de nuestra vida al mundo virtual. En términos penales, esto se traduce en que cada vez introducimos más valores personales en el ciberespacio, lo que permite a los ciberdelincuentes tener disponibles cada vez más bienes jurídicos para su lesión o puesta en peligro. De hecho, desde inicios de siglo, hemos evolucionado de un escenario criminal en el ciberespacio en el que el valor amenazado se trataba casi en exclusiva del patrimonio a que sean habituales ciberdelitos contra bienes jurídicos antes solo relacionados con el espacio delictivo tradicional como la intimidad, el honor, la paz pública, la libertad o la libertad e indemnidad sexual (Romeo Casabona, 2006: 8; Vivó Cabo, 2018: 3; Davara Rodríguez, 2017: 1240-1242; Jewkes y Yar, 2013: 87; Gercke y Brunst, 2009: 8-9). Así las cosas, la doctrina de habla hispana ha definido recientemente a la ciberdelincuencia como la práctica de ilícitos penales que tiene como elemento diferenciador el uso de internet, ya sea como entorno en el que son atacados sus propios sistemas electrónicos o sus archivos o programas, ya sea como medio comisivo de dichas actividades[2] (Barrio Andrés, 2018: 36).

1. El término *ciberdelincuencia* es más común en el ámbito de la dogmática penal, mientras que el vocablo *cibercrimen* es habitual en las ciencias criminológicas.

2. Romeo Casabona (2007: 11), pionero en la identificación del término, lo definía a inicios de siglo como «el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual». Miró Llinares, por su parte, distingue entre las concepciones tipológica y normativa del término cibercrimen. A su juicio, la tipológica hace

Algunas características criminológicas de la ciberdelincuencia y sus correspondientes implicaciones dogmáticas

Volviendo a la ciberdelincuencia, como fenómeno concreto dentro de la delincuencia informática, es básico mencionar que el hecho de que se lleve a cabo en el ciberespacio le otorga características de corte criminológico que la diferencian, de forma latente, de la delincuencia tradicional. Estos caracteres, además, se traducen en ciertas implicaciones dogmáticas que deben ser tenidas muy en cuenta a la hora de llevar a cabo el análisis en función de los fines de la pena que se pretende en este trabajo. De hecho, son precisamente estas peculiaridades de la ciberdelincuencia las que otorgan relevancia y novedad a este trabajo, por lo que analizamos a continuación las más relevantes de cara a este estudio.[3] En primer lugar, como principal característica de uso de las nuevas tecnologías, mencionábamos el altísimo porcentaje de la población mundial que accede a la red a diario y el creciente número de valores personales que estos introducen en el ciberespacio[4] (Valiente García, 2004: 137; Hernández Moreno, 2017: 55).

---

referencia a un comportamiento ilícito con unas determinadas características criminológicas, mientras que perspectiva normativa identifica a un tipo penal concreto que trata de prevenir conductas en el ciberespacio que lesionen o pongan en peligro bienes jurídicos. Por tanto, apunta que el cibercrimen tiene como función principal, junto con la descripción de las nuevas formas de afectación de los bienes más importantes en el ámbito de las tecnologías de la información y la comunicación, la valoración de las soluciones político-criminales adoptadas frente a ellas, partiendo de la revisión de los tipos penales existentes y del juicio de necesidad de su modificación. Acercándose, por ende, al sentido tipológico del término. Su definición de cibercrimen, en consecuencia, es la que sigue: «cualquier delito en el que las tecnologías de la información y la comunicación juegan un papel determinante en su concreta comisión, que es lo mismo que afirmar que lo será cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan» (Miró Llinares, 2012: 39-44).

3. Otra característica no mencionada aquí es la capacidad de albergar, procesar y distribuir ingentes volúmenes de datos que presentan las tecnologías de la información y la comunicación, y la gran velocidad en la que llevan a cabo este cometido (Hilgendorf y Valerius, 2012: 829).

4. Así, los ciberdelitos como las estafas pueden verse claramente beneficiados, en el momento en el que llevamos a cabo en el mundo virtual acciones imprudentes con respecto a nuestro patrimonio que, de ninguna manera, haríamos en el mundo real. También los delitos contra la indemnidad sexual de menores de 16 años son fomentados gracias a estas características, ya que el acceso al ciberespacio se ha democratizado sin entender de clases sociales ni de edades. Del mismo modo, los delitos contra el honor o contra la paz pública (delitos de terrorismo) han sido facilitados por el aumento en el número de usuarios de internet, ya que los contenidos calumniosos, injuriosos o de enaltecimiento terrorista, por ejemplo, son accesibles por un mayor número de personas en la actualidad. No obstante, como adelantábamos antes, la principal tarea político-criminal en este sentido debe ser la de dar respuesta a la introducción de cada vez más valores en la red por parte de los ciudadanos; valores básicos en su desarrollo personal y social. Desde la irrupción en la década del setenta de la delincuencia informática, que afectaba casi exclusivamente al patrimonio de particulares y empresas, la evolución de los usos sociales en torno a internet ha derivado en que en la actualidad la intimidad, el honor, la libertad o la libertad

Una segunda característica de las tecnologías de la información y la comunicación, en el plano técnico, es la posibilidad de anonimato y simulación de identidad (Lessig, 2002: 171; Owen, 2017: 177) que ofrece a sus usuarios.[5] Estos son dos de los caracteres más relevantes de internet y de los que mayor influencia tienen en la decisión delictiva de los cibercriminales. Por ello, se presenta como un elemento clave en la evolución de las oportunidades delictivas en el ciberespacio.

Asimismo, los fenómenos de *permanencia* y *automatismo*[6] del hecho han tenido una influencia importante desde los inicios de la delincuencia informática, como elemento distintivo de los sistemas informáticos en general, sin necesidad de conexión a internet (Rovira del Canto, 2002: 77; Sieber, 1992: 29-30; Fischer, 1979: 14).[7]

En relación con estos dos fenómenos, además, no podemos dejar de mencionar

---

e indemnidad sexual, junto con valores colectivos como la paz pública o el patrimonio estatal, sean amenazados cada día por los ciberdelincuentes. Es por ello por lo que, en la medida en la que los usos en el mundo virtual siguen en constante evolución, debe llevarse a cabo un planteamiento sobre qué valores deben protegerse en el ciberespacio. En la línea de los usos de internet, no debemos desdeñar la irrupción del *internet of things* que, en estos días, se postula como una de las amenazas para la intimidad de los usuarios (Hilgendorf y Valerius, 2012: 830). Dado que esta tecnología copa cada vez más ámbitos de nuestra vida diaria, queda plantearse a qué aspectos de nuestro círculo vital será capaz de afectar.

5. Los delitos cuya comisión se ve beneficiada por esta cuestión son muchos y muy diversos, ya que el hecho de que no se conozca de forma evidente la identidad del cibercriminal invita a la oportunidad delictiva a individuos que jamás tomarían la decisión de cometer un delito en el mundo real. En concreto, los daños e intrusismos informáticos causados por los *hackers* corresponden con un perfil de delincuente muy concreto que concentra su actividad en el ciberespacio. También ciertos delitos contra la indemnidad sexual de menores se ven fomentados por la opción de simulación de identidad que ofrece la red, siendo el *child grooming* el delito paradigmático aquí, ya que los ciberagresores fingen ser jóvenes de edad similar a sus víctimas. En otro plano, el blanqueo de capitales encuentra su principal justificación a su comisión en la red en el anonimato que posibilita el mundo virtual. Del mismo modo, el delito de autoadoctrinamiento terrorista se beneficia de que el acceso a los contenidos ilícitos puede llevarse a cabo de incógnito. Por último, también delitos contra el honor o contra la libertad (amenazas, *stalking*) son cometidos, en ocasiones, bajo identidades falsas en la red.

6. Estos fenómenos implican que las acciones que se llevan a cabo en sistemas informáticos pueden ser facilitadas enormemente por las características que estos presentan. El automatismo, más propio de los sistemas informáticos en general, se trata de que una misma acción puede ser repetida infinitamente con poco o sin ningún esfuerzo posterior al de la primera acción. La permanencia del hecho, distintiva del ciberespacio, es un fenómeno según el cual los efectos de una acción pueden desplegarse más allá del momento temporal en el que esta es cometida.

7. Así pues, ha constituido un elemento básico para la comisión de delitos patrimoniales en masa, como las estafas o los daños informáticos, ya que se trata de delitos que encuentran, en la repetición de conductas delictivas y en la afectación a un alto número de víctimas, la posibilidad de aumentar el beneficio ilícito obtenido por el delincuente. A futuro, este carácter se presenta como un elemento ya incorporado al funcionamiento de las redes y los sistemas de información, en el sentido en que se encuentra ya al alcance de todo usuario la posibilidad de programar, encadenar, repetir acciones virtuales con muy poco esfuerzo. Como, por ejemplo, el envío masivo de correos electrónicos.

la superior capacidad lesiva de los delitos cometidos en la red (Bequai, 1978: 4: De la Cuesta y otros, 2010: 86). Esta capacidad despliega sus efectos principalmente en dos planos diferenciados: en el aumento del perjuicio en los delitos económicos por medio del acceso al *dinero contable*[8] y en la mayor gravedad de delitos ciberintrusivos y de ciberterrorismo por medio de la difusión del contenido.[9] En consecuencia, si versamos sobre los sujetos pasivos en los ciberdelitos, debemos hacer hincapié en que no son pocas las ocasiones en las que un delito en el ciberespacio va a acompañado de la afectación a una pluralidad de víctimas.

Esta peculiaridad nos lleva, irremediablemente, a la construcción dogmática prevista en el artículo 74 del Código Penal[10] de delito continuado, ya que el sujeto activo afecta a una pluralidad de personas «en ejecución de un plan preconcebido o aprovechando idéntica ocasión». Tanto, que una sola ocasión es suficiente para afectar a varios sujetos pasivos, infringiendo el mismo tipo penal. Según Romeo Casabona (2006: 27), el hecho de que el autor recurra a procedimientos automatizados para conseguir la afectación a varias personas no está obstaculizado por la exigencia del elemento subjetivo que apuntamos, ya que, en su ejecución, el sujeto es plenamente consciente y quiere aprovecharse del recurso al procedimiento repetitivo.[11]

Asimismo, es básico tener en cuenta lo fundamental de la contribución de las víctimas en los delitos que se cometen en el ciberespacio. Esta es una distinción de gran

8. El dinero contable es el concepto que se utiliza para denominar a todo el dinero que es accesible desde una plataforma de gestión del patrimonio electrónica que, habitualmente, tan solo encuentra límites en el total que atesore dicha cuenta corriente.

9. Así las cosas, son numerosos los ciberdelitos que aprovechan estas circunstancias. Véase, en el plano económico, la estafa, los daños, el espionaje industrial o los delitos contra la propiedad intelectual e industrial y, por la parte de difusión de contenido, los delitos de pornografía infantil, la revelación de secretos, los delitos contra el honor, los delitos de incitación al odio o el delito de enaltecimiento del terrorismo. No cabe duda de que la capacidad de difusión de contenido que proporciona la red en estos casos será un elemento clave a futuro, en la medida en la que ha logrado ser una vía para la afectación por parte de los ciberdelincuentes a bienes jurídicos de la esfera personal de los ciudadanos, como el honor o la libertad sexual, además del patrimonio, junto con otros bienes jurídicos de carácter colectivo como la paz pública.

10. En este trabajo, con la expresión Código Penal, se hace referencia al Código Penal español.

11. Más concretamente, resulta muy recurrente la opción de la subsunción de este tipo de conductas en la figura del delito masa, previsto en el apartado segundo del artículo y que prevé una agravación mayor dependiendo de su nivel de afectación y del perjuicio total causado, en los casos de delitos contra el patrimonio. Este es el caso, por ejemplo, del delito de *phishing* por medio del cual un delincuente logra hacerse con las contraseñas bancarias de una pluralidad de afectados, tras el envío masivo de un correo electrónico con un enlace que, al acceder, redirige a los sujetos pasivos a una página web, que simula ser el portal oficial de su entidad bancaria. De este modo, con tan solo un *clic,* consistente en el envío de cientos de mensajes con idéntico contenido, logra estafar electrónicamente (artículo 248, número 2, del Código Penal) a una pluralidad de víctimas en el momento en el cual se lleva a cabo el acto de disposición patrimonial en su beneficio.

relevancia con respecto al espacio delictivo tradicional, ya que cada individuo toma la decisión sobre qué valores personales introduce en el mundo virtual, dependiendo de qué parcelas de su vida diaria traslada a la red.[12]

También, en relación con las víctimas de los delitos, debemos tener en cuenta el fenómeno de la cifra negra que hemos introducido en las primeras páginas de este estudio. Los factores que fomentan la falta de detección de los ciberdelitos son: el elevado nivel de tecnicidad de las conductas en línea (lo que dificulta su persecución), el desconocimiento de su condición de sujetos pasivos en el que en ocasiones incurren las propias víctimas, la errónea creencia de que ciertos comportamientos sufridos en la red no son constitutivos de delito, la falta de confianza en el sistema judicial, el hecho de que los menores no encuentren un espacio de confianza para comunicar su experiencia y, en el ámbito empresarial, la publicidad negativa que un reconocimiento de haber sido víctima de un ciberdelito puede generar (De la Cuesta y otros, 2010: 116-118).

En último lugar, la contracción del espacio y su relativización (Davara Rodríguez, 2015: 400) ha traído, además de la discusión en torno a la competencia territorial y al tribunal nacional competente en cada caso, la posibilidad de comisión delictual desde cualquier parte del mundo para los cibercriminales y, a su vez, la opción de que los efectos de estos delitos puedan desplegarse también en cualquier lugar.[13]

12. De hecho, son muchos los ciberataques que se realizan en la red sin una víctima concreta, acciones que encuentran su objetivo final en el momento en el que un usuario de internet interactúa con esta y se convierte en víctima. Es decir, el criminal no tiene un papel tan determinante en el ciberespacio como en el espacio tradicional, ya que, para que el cibercrimen exista, es necesario que la potencial víctima esté en la red, que interaccione de alguna manera con el ciberdelincuente y que no esté protegido de un posible ciberataque. Miró Llinares expone tres factores principales por los cuales se puede afirmar que el sujeto pasivo del ciberdelito tiene un papel fundamental en su comisión y, por ende, en su potencial prevención. En primer lugar, apunta que, como decimos, el usuario de la red escoge los valores que introduce en la red y, por tanto, pueden ser potencialmente afectados por un crimen virtual. En segundo lugar, expone que existen ciertas conductas más peligrosas que otras que pueden llevarse a cabo en la red y que, en aras de aumentar nuestra seguridad y evitar ser víctima de un ciberdelito, podríamos evitar. En especial al ser conductas identificables por cualquier usuario medio de internet. Además, afirma que, a diferencia que en un espacio delictivo físico tradicional, el establecimiento de guardianes o barreras para evitar la ciberdelincuencia es extremadamente sencilla en el mundo virtual (*firewalls, software* antivirus o control parental, entre otros) (Miró Llinares, 2012: 91-93).

13. Siendo esto así, la gran mayoría de los ilícitos cometidos en el ciberespacio se han visto de alguna manera beneficiados por esta circunstancia. En especial, la defraudación de telecomunicaciones, el hurto de tiempo o el blanqueo de capitales se han servido de este carácter para llevar a cabo conductas imposibles, o muy difícilmente imaginables, sin la reinvención del espacio que permite elemento cibernético. Otras, como las relativas a los delitos de daños informáticos o contra la propiedad intelectual se han visto ampliamente potenciadas gracias a la red y al componente internacional que otorga esta característica de los ciberdelitos. Por lo tanto, la evolución de los cibercrímenes en esta línea nos lleva a intuir que el elemento transnacional de los delitos será un componente básico, si no lo es ya, en el desarrollo

En estrecha relación con la cuestión del espacio, la relatividad temporal de los ciberdelitos es un elemento que hace tambalear las reglas dogmáticas tal y como las conocíamos antes de la llegada de internet. Dejando de lado la cuestión de la ley aplicable en el tiempo, resulta diferenciadora la cuestión de que no es necesario que víctima y victimario coincidan en la línea temporal para poder consumar la acción delictiva, incluso en los delitos que, en el espacio delictivo tradicional, requieren de una mínima interacción.[14] También es muy relevante la opción de que la red albergue, de forma permanente, un contenido ilícito o aloje un elemento malicioso de forma perenne (Eser, 2002: 309-310; Viota Maestre, 2007: 245).

En consecuencia, es necesario introducir la facilidad de encubrimiento y la dificultad de persecución por parte de las autoridades que preside los ciberdelitos (Mata y Martín, 2001, 26; Hilgendorf y Valerius, 2012: 233; Wernert, 2017: 36). Elementos técnicos como la facilidad de alteración de la huella informática, el anonimato en los cibercrímenes o el simple hecho de que es necesaria una capacidad técnica mínima para navegar con pleno conocimiento de la red ayudan a argumentar la postura de que existe una cifra negra muy importante en la ciberdelincuencia (Morón Lerma, 2002: 27).

Así las cosas, desde una perspectiva estrictamente criminológica, Hayward invita a utilizar la criminología cultural para tratar de explicar el comportamiento de los delincuentes en el ciberespacio. El autor propone centrar el estudio en la dimensión espacial de la ciberdelincuencia y en la posibilidad de conexión, además de en la extraordinaria capacidad de difusión que presentan los sistemas de información y las redes. En concreto, introduce los conceptos de *convergencia* y *telepresencia* como explicativos de la actividad de los usuarios y como herramientas para la lucha y la prevención del cibercrimen (Hayward, 2012: 455-457).

Los ciberdelitos en particular

Como hemos apuntado anteriormente, los delitos informáticos no están situados en un lugar concreto de la legislación penal y, en consecuencia, tampoco se cumple esta condición en relación con los ciberdelitos. Por lo tanto, a la hora de dilucidar qué ilícitos penales pueden entrar dentro de esta clasificación, debemos atenernos a las definiciones antes apuntadas y escoger los delitos que presenten las características comunes que hemos concretado. Así, en suma, será un ciberdelito el injusto en el que la red juegue un papel fundamental en su comisión, ya sea como medio de comisión delictual o

de la ciberdelincuencia en los próximos años.

14. Así, de la primera cuestión se han visto beneficiados delitos como la estafa informática, los delitos contra la libertad o la libertad e indemnidad sexuales y, de la segunda, ilícitos como los daños informáticos o los delitos contra la propiedad intelectual.

como objeto sobre el que recae la acción. Asimismo, existirán ciberdelitos en sentido estricto en los casos en los que solo puedan cometerse en el ciberespacio, y ciberdelitos en sentido amplio cuando existan también en el espacio delictivo tradicional.

Así las cosas, la clasificación más popular de los ciberdelitos es la propuesta por Sieber, quien separa los cibercrímenes en función del valor o conjunto de valores que protege cada uno. Esta separación, compuesta por tres grandes bloques, fue propuesta por el penalista alemán en su obra *Computerkriminalität und Strafrecht* publicada en 1980 y es, a día de hoy, la más utilizada por los autores que abordan la cuestión de la ciberdelincuencia en general: delitos cibereconómicos, delitos ciberintrusivos y delitos de ciberterrorismo (Sieber, 1980: 22).

Como comprobaremos a continuación, los primeros afectan al patrimonio de sus víctimas y es en los que catalogamos, entre otras figuras, a las tradicionales conductas de fraude, sabotaje o manipulación informática, así como los ciberdelitos contra la propiedad intelectual. Los delitos ciberintrusivos, por su lado, dañan la esfera más personal de los ciudadanos, ya que son los relativos a bienes jurídicos personalísimos como la intimidad, la libertad, la libertad sexual o el honor. En tercer lugar, los delitos de ciberterrorismo afectan a la paz pública.

Sin embargo, esto no significa que no existan más posibilidades de clasificación para la ciberdelincuencia. Otra de las más extendidas, en función de cómo inciden las nuevas tecnologías en la conducta criminal, es la introducida por Miró Llinares (2012: 51), seguida por, entre otros, Almenar Pineda (2018: 37), la cual separa los ciberdelitos entre los ilícitos: a) puros, donde las tecnologías de la información y la comunicación son el medio de comisión del ciberdelito y el objetivo de él, como el *hacking,* por ejemplo; b) de réplica, donde la red juega como medio de ataque a bienes jurídico tradicionales, como el *stalking,* entre otros; y c) de contenido, donde el núcleo del injusto está en el material que se divulga por el ciberespacio, como ocurre en los ciberdelitos contra la propiedad intelectual.

Siguiendo la primera clasificación, y a tenor de los ciberdelitos incluidos en las obras especializadas, podemos completar la siguiente clasificación de los ciberdelitos en particular. Todo esto, siendo conscientes de que la evolución de las tecnologías y de los usos que hacemos de ellas llevará a tener que introducir irremediablemente cambios en sus estructuras: a) delitos cibereconómicos: estafa informática (artículo 248.2), defraudación remota de telecomunicaciones (artículo 255), hurto de tiempo (artículo 256), daños informáticos (artículo 264 y siguientes), ciberdelitos contra la propiedad intelectual (artículo 270 y siguientes) e industrial (artículo 273 y siguientes), espionaje industrial (artículo 278), blanqueo de capitales (artículo 301) y falsedad de tarjetas (artículo 399 bis); b) delitos ciberintrusivos: ciberdelitos contra la indemnidad sexual (artículo 183 y siguientes), *stalking* (artículo 172 ter), quebrantamiento de orden de alejamiento (artículo 468.3), descubrimiento y revelación de secretos (artículo 197 y siguientes), ciberdelitos contra el honor (artículo 205 y 208), ciberdelitos contra la

libertad (artículo 169 y siguientes, y 243) y ciberdelitos de incitación al odio (artículo 510); y c) delitos de ciberterrorismo: descubrimiento y revelación de secretos y daños informáticos con fines terroristas, autoadoctrinamiento terrorista y enaltecimiento del terrorismo (artículo 573 y siguientes). Todos estos artículos del Código Penal.

El perfil criminológico del ciberdelincuente

Visto todo lo anterior, y con el objetivo de completar una visión panorámica de la ciberdelincuencia antes de afrontar el estudio de sus implicaciones en los fines de la pena, es preciso acercarse al perfil del ciberdelincuente porque, de nuevo, los caracteres comunes que reúnen los ciberdelitos convierten al criminal en el ciberespacio en un perfil con cualidades muy marcadas.[15]

Tradicionalmente, se ha relacionado la cuestión de los sujetos activos en los ciberdelitos con la figura del *hacker*.[16] Ahora bien, los *hackers,* al menos en sus inicios, defendían un deber ético bajo la creencia de que compartir información era un bien poderoso y positivo, consistente en poner en común su experiencia mediante la programación en código abierto y facilitando el acceso al usuario a los recursos que ofrecían las tecnologías emergentes (Barrio Andrés, 2017: 34-35). En la actualidad, sin embargo, estos han evolucionado hacia tres perfiles principales.[17] No obstante, este no es el único perfil de delincuente habitual existente en la actualidad en el ciberespacio. De hecho, los estudios criminológicos se desmarcan de la concepción del ciberdelincuente actual como un delincuente clásico[18] y dibuja diversos perfiles muy concretos de sujetos que actúan en la red con la nota común de poseer una cierta destreza (aunque no necesariamente muy elevada) de manejo de sistemas informáticos, lo que se aleja totalmente, como decimos, de la figura social, cultural y económica-

15. En el anexo del estudio, para completar el perfil del ciberdelincuente, se incluye una caracterización de algunos los perfiles más significativos dentro de los ciberdelincuentes no mencionados hasta el momento, aparejándolos con los delitos más comunes en cada caso.

16. *Hacker* como sujeto misterioso que causa estragos en sistemas informáticos de máxima seguridad, ya sea para su propio lucro, ya sea para destapar y revelar información valiosa sobre algún escándalo concerniente a sujetos que se encuentren en las altas esferas de poder (Moore, 2011: 18-19).

17. En Barrio Andrés (2018: 42). Se refiere a quienes trabajan al servicio de organizaciones de delincuencia organizada, los que, manteniéndose fieles al espíritu original, tratan de acceder a información que, de alguna manera, contribuya a la promoción de la clase obrera en contra del poder del capitalismo, y quienes son expertos en seguridad informática y colaboran estrechamente con la fuerzas y cuerpos de seguridad del Estado, tratando de neutralizar los avances de los dos primeros colectivos.

18. Avanzamos, por tanto, de las concepciones *consistency assumption* y *homology assumption* propias del perfil criminológico y sicológico habitual en estas ciencias. La primera hace referencia a que los delitos o la forma de delinquir suele ser habitualmente parecida entre distintos episodios. La segunda, por su lado, hace referencia a que delitos similares son cometidos por criminales parecidos (Huber, 2019: 64-65).

mente marginal del criminal tradicional. Destreza que, combinada con un coeficiente intelectual medio y tanto la creación como el aprovechamiento de la oportunidad delictiva, pueden resultar en la decisión de cometer un cibercrimen (De la Cuesta y Pérez Machío, 2010: 101).

Si nos centramos en la edad como factor en el perfil del ciberdelincuente, es claro que la mayoría de los cibercrímenes son cometidos por personas jóvenes. Las razones que explican este fenómeno son básicamente dos: el hecho de que los jóvenes pueden considerarse nativos digitales y que estos tienen mayor disponibilidad de tiempo para buscar vulnerabilidades en las redes (Diamond y Bachmann, 2015: 24). Lo que nos lleva a concluir que, a medida que pasen los años y dichos nativos digitales envejezcan, también aumentará la edad media del delincuente virtual.

El factor de género resulta muy relevante también en la ciberdelincuencia, ya que diversos estudios apuntan al protagonismo del hombre como sujeto activo en esta clase de ilícitos penales. En el caso concreto holandés, por ejemplo, un estudio llevado a cabo en 2013 mostró un panorama según el cual el 73,4% de los ciberdelitos eran cometidos por hombres, mientras tan solo el 26,6% correspondía a mujeres (Leukfeldt y otros, 2013: 1-17).

Por su parte, los recursos económicos con los que el criminal de internet cuenta son habitualmente de niveles similares. Lo habitual es que el ciberdelincuente se trate de un individuo de clase media o clase media acomodada y que no necesite emplear grandes recursos económicos en el equipamiento técnico que precisa para la actuación delictiva, ya que el acceso a internet es un servicio ampliamente democratizado y extendido en nuestra sociedad actual (Clough, 2010: 6).

Ahora bien, la disuasión de la decisión delictiva en el ciberespacio se trata de una cuestión ampliamente tratada por la doctrina, y en la que los Estados y las entidades privadas se han centrado en los últimos años. De hecho, no solo se han implementado avances y reformas legislativas, sino que también se ha buscado la prevención de la ciberdelincuencia desde el ámbito técnico o de la seguridad estatal, con el foco puesto tanto en víctimas como en victimarios (Maimon, 2020: 23).[19]

Los fines de la pena ante la ciberdelincuencia

En este segundo apartado se pretende introducir, de forma breve, los principales postulados de las distintas teorías de la pena, sobradamente conocidos por todos, e introducir unas consideraciones preliminares sobre el encaje de los ciberdelitos en

19. Maimon, desde un enfoque interdisciplinar, apunta la importancia de que trabajos académicos analicen la efectividad de la disuasión en el ciberespacio. De hecho, este estudio encaja en esa recomendación, desde la perspectiva de la vigencia de la teoría de los fines de la pena en la ciberdelincuencia y la efectividad de las sanciones penales.

estos planteamientos, teniendo en cuenta las peculiaridades de la delincuencia en la red que hemos incluido en el primer apartado de este trabajo. Así, para lograr la extracción de conclusiones lo más concretas y funcionales posible, se aborda el estudio de cada teoría del fin de la pena por separado, siendo conscientes de que la evolución de estos postulados lleva a la doctrina a acordar, en su mayoría, que lo adecuado es seguir las teorías eclécticas, unificadores o mixtas,[20] las cuales defienden una posición intermedia y global donde se conjugan los distintos fines de la pena con especial consideración para la reeducación y reinserción social del reo reconocida, en el caso español, en el artículo 25.2 de la Constitución.

El alcance de la retribución

Para empezar, las teorías absolutas o retributivas se corresponden con una visión del ser humano como ideal y entienden la pena como un elemento independiente o desvinculado de sus efectos sociales (Castro Moreno, 2008: 15-16; Demetrio Crespo, 1999: 59; Hassemer, 1984: 348; Cutiño Raya, 2017: 15). Es precisamente de esta concepción desde donde proviene la palabra latina *absolutus*. Esta teoría, como es sabido, presenta una doble vertiente. La primera, la más obvia, se concreta en la compensación del mal creado por la acción del sujeto criminal y se dirige al suceso externo, al acto injusto, el cual es compensado con el mal que supone la pena. La segunda, desde una visión interna, se centra en la expiación del sujeto, quien, a través de la pena, se reconcilia consigo mismo en busca de la libertad moral.[21]

Las teorías retribucionistas, además, han despertado el interés de la doctrina en la última década, con especial protagonismo para los principios distributivos introducidos por Robinson. En particular, el autor norteamericano propone acudir al «me-

20. Estas teorías, a su vez, pueden presentar dos concepciones diferenciadas. La teoría aditiva, que se basa en la retribución, la cual establece el marco penal y la prevención ejerce de complemento; y la teoría dialéctica, la cual encuentra su fundamento en las estrategias preventivas y estas, a su vez, el límite en la retribución (Röder, 1876: 28; Antón Oneca, 1965: 14).

21. Sus principales teóricos, son Kant y Hegel. El primero, defensor de la retribución moral, entendía el concepto de culpabilidad moral como fundamento y como límite para la extensión de la pena. El segundo, centrado en la retribución jurídica, concebía la pena como reflejo de la reprochabilidad de la acción ilícita y como elemento restaurador del ordenamiento jurídico y de su vigencia, ante la negación del derecho que supone el delito. Ahora bien, esta teoría no está exenta de críticas. La más común es la que pone en tela de juicio la compatibilidad de esta teoría con la dignidad humana que debe garantizar un Estado democrático, vista la imposición coactiva de exigencias éticas que supone la concepción exclusivamente retributiva de la pena. También es criticable la falta de demostración empírica que presenta su principal fundamento, la culpabilidad, basada en la mera venganza por el injusto cometido (Bustos Ramírez y Hormazabal Malarée, 1997: 46-47). Asimismo, es débil la idea de compensación del mal creado con el mal proveniente de la pena, ya que este segundo mal no consigue, en ningún caso, en virtud de estas teorías, eliminar el primero (Marqués de Beccaria, 1993: 45).

recimiento empírico» (o a la intuición de justicia de la comunidad) para justificar el castigo penal, reforzando su credibilidad moral, en el momento en el que concluye que ninguna de las finalidades de la pena es una guía adecuada para esta tarea. Ahora bien, descarta el peligro del populismo punitivo al otorgar la tarea a la comunidad de determinar la medida de la culpabilidad, con base en su experiencia personal (Robinson, 2012: 18-19).

En la doctrina de habla hispana, Mañalich Raffo defiende la fundamentación retributiva de la pena como correcta porque el sentido de la pena descansa, a su juicio, en la expresión de reproche merecido entre ciudadanos moralmente iguales, como manifestación del utilitarismo penal. Para ello, propone huir de la definición actual de la pena, que, lejos de la neutralidad, la presenta como la irrogación coercitiva de un mal con desaprobación por parte del estado (Mañalich Raffo, 2007b: 114-115).

Dicho todo esto, de una aplicación preliminar de las teorías absolutas a los ciberdelitos es posible extraer dos puntos de análisis. El primero se fundamenta en los fenómenos de permanencia y automatismo del hecho que hemos introducido en el apartado anterior y la consiguiente superior capacidad lesiva que presentan los ciberdelitos. Como hemos adelantado, este carácter se ve particularmente potenciado, por un lado, en los delitos cibereconómicos y, por otro, en los delitos ciberintrusivos y de ciberterrorismo cuando la conducta típica requiere una difusión de contenido.

Así, en los delitos cibereconómicos, el hecho de que sean cometidos en el ciberespacio o por medios cibernéticos permite al sujeto activo causar un perjuicio mayor en el patrimonio de sus víctimas. De esta forma, por ejemplo, centrándonos en la estafa informática y, en concreto, en el supuesto de las cartas nigerianas, es plausible llevar a cabo el envío de la comunicación que trata de producir el engaño a las potenciales víctimas de la estafa tanto por correo postal como por correo electrónico. Eso sí, para enviar el mensaje por carta es necesario preparar cada sobre, cada sello, escribir cada dirección y acudir a la entidad de correo en cada ocasión y por cada víctima potencial. En el caso del correo electrónico, por el contrario, es suficiente con el envío del mismo mensaje a un número indefinido de cuentas diferentes, todas ellas potenciales víctimas. En el caso de estafa de las cartas nigerianas, por lo tanto, el componente cibernético aumenta la lesividad de la conducta, en el sentido en el que una acción es capaz de afectar a una pluralidad de víctimas.

Si analizamos el ejemplo del *phishing*, llegamos a una conclusión diferente ante la posibilidad de los cibercriminales de hacerse con las contraseñas de acceso a la banca en línea de sus víctimas. En comparación con la estafa tradicional, continúa siendo una conducta más lesiva por poder afectar al patrimonio de muchas personas con una sola acción, es decir, con un simple envío masivo de un correo electrónico, pero, además, se trata de un supuesto en el que el estafador puede obtener acceso al dinero contable y no tan solo al dinero del que dispone la víctima en el momento concreto del error producido por el engaño. Es decir, el cibercriminal, al tener acceso

a la cuenta del sujeto pasivo, puede hacerse con todo el dinero que este tenga en su cuenta, en vez de apoderarse del dinero físico que pueda tener en un momento dado, aumentando considerablemente la potencial lesividad de la estafa.

Por su lado, cuando el elemento cibernético apoya en la difusión de contenido, el hecho de que los delitos sean cometidos en el ciberespacio aporta la extraordinaria capacidad de difusión que proporciona internet.[22] Esto permite a los cibercriminales propagar sus mensajes y contenidos por todo el planeta con un esfuerzo y coste mínimos, y de forma prácticamente automática, además de anónima, en caso de elegirlo así. Este es el caso, por ejemplo, de los delitos de incitación al odio, en cuya regulación está prevista esta circunstancia cuando, en la agravante por difusión del artículo 510.3, se contemplan los supuestos en los que el discurso de odio se canalice «por un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información» y, además, esto implique que «aquel se hiciera accesible a un elevado número de personas». También es el supuesto del delito de enaltecimiento del terrorismo por medio de internet cuando, en el artículo 578.2 del Código Penal, se lleva a cabo una mención a internet como medio de difusión de contenido: «mediante la difusión de servicios o contenidos accesibles al público a través de medios de comunicación, internet, o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información». Esta previsión de una superior lesividad es válida tanto para la afectación que este delito presenta en el bien jurídico paz pública, como para el valor del honor de los familiares de las víctimas y de las propias víctimas.[23]

En consecuencia, en el marco de las teorías retributivas, cuando la lesividad causada por los ciberdelitos sea, gracias a sus caracteres distintivos, de un nivel superior, el límite que marca la culpabilidad del injusto será también más alto y, por consiguiente, la pena deberá ser más severa.

El segundo punto de análisis se centra en la medida de la culpabilidad de los cibercrímenes y en su relación con la contribución del sujeto pasivo a los ciberdelitos que hemos introducido con anterioridad. El posible planteamiento aquí es que, teniendo en cuenta que parte de la culpabilidad o reprochabilidad del hecho corresponde con una acción despreocupada o negligente del usuario de internet, más tarde víctima del ciberdelito, el nivel de la culpabilidad del autor pueda descender y la pena pueda resultar de una extensión inferior, en comparación con el mismo delito en el espacio delictivo tradicional.

22. Por supuesto, en estos casos, la apreciación de la conducta delictiva requerirá de un examen previo de si el supuesto se encuentra amparado en el derecho fundamental de libertad de expresión.

23. Incluimos esta última apreciación porque el delito de enaltecimiento del terrorismo incluye tanto el ensalzamiento de los actos de los terroristas como la humillación de las víctimas y de sus familiares.

El alcance de la prevención general negativa

En segundo término, y comenzando con las teorías relativas, analizamos la prevención general negativa o intimidatoria en relación con la ciberdelincuencia.

Es preciso apuntar, ahora bien, que las teorías relativas se diferencian de las absolutas en que buscan motivaciones sociales (prevención general) e individuales (prevención especial), más allá de los planteamientos de retribución pura y con el fin de complementarlos. En concreto, la prevención general negativa concibe a la pena como un mal que atemoriza a la sociedad desde la garantía que reconoce el principio de legalidad. Así, para que la amenaza que supone la pena sea eficaz, preventivamente se requiere el conocimiento más exacto posible sobre la norma de la sociedad[24] (Lardizábal y Uribe, 1997: 46; Castro Moreno, 2008: 36-38; Luzón Peña, 1979: 25).

Si cruzamos estos postulados básicos con los caracteres de los ciberdelitos, podemos extraer varias consideraciones. La primera es que, a pesar de que tampoco existe en ellos legitimación empírica de que la prevención general negativa atesora real-

24. Sus principales defensores son, entre otros, Beccaria, Feuerbach, Bentham o Lardizábal. El primero añadía que el fin de las penas era impedir al reo causar nuevos daños a los ciudadanos y retraer a los demás de la comisión de los mismos, apuntillando que el temor de las leyes es saludable. Lardizábal recomendaba la ejecución pública de la pena con el fin de utilizarlo como instrumento con una mayor eficacia preventiva. Según el segundo de los autores mencionados, y en virtud de su teoría de la coacción sicológica, la norma penal intimida o coacciona a los individuos para la evitación de la comisión de delitos futuros por medio de la amenaza abstracta y general de la pena y la efectiva imposición y ejecución de la misma refuerza su veracidad. En cuarto lugar, Bentham abogaba por que el fin primordial de las penas debería ser la prevención de delitos futuros. De nuevo, sus planteamientos no podían estar exentos de críticas. La principal es la ausencia de legitimación empírica de que el fin preventivo intimidatorio funciona en la práctica, ya que se trata de un argumento preliminar de lo que se prevé que ocurra en la mente de los ciudadanos y no existen estudios científicos ni estadísticas sobre este extremo. De hecho, los estudios criminológicos al respecto apuntan a que los criminales no calculan ventajas y desventajas a la hora de tomar la decisión criminal, sino que se trata, por lo general, de un comportamiento mucho más impulsivo de lo que puede parecer en un primer momento (Alcácer Guirao, 2001: 37-38). Además, no todos los delincuentes son iguales y no es posible afirmar que la amenaza de la pena les influye a todos de igual manera. Por ejemplo, en el caso de un ciudadano con un arraigo social fuerte, lo más seguro es que su decisión de no delinquir no se base en la coacción penal, sino en su convicción y vocación de vivir en sociedad y de respetar las normas. De hecho, resulta más determinante el miedo al hecho de ser descubierto en la comisión de un delito que a la propia pena. También es criticada esta teoría por la instrumentalización del individuo que implica, ya que se utiliza al ciudadano con una motivación exterior, como un experimento social. Asimismo, los críticos también se centran en la ausencia de límites penales en la prevención general negativa, puesto que no existe una medida máxima en el castigo al reo que podamos extraer de estos planteamientos preventivos. Por último, son obvios los problemas para explicar los supuestos de inexigibilidad de otra conducta en virtud de esta teoría: en concreto en los casos de los sujetos inimputables, de error de prohibición o en los delitos imprudentes. Esto es así porque la impunidad que puede derivar de la apreciación de estas figuras a la hora de depurar la responsabilidad penal del delito merma la eficacia preventiva de la norma.

mente utilidad coactiva, la decisión criminal en el ciberespacio es, en general, menos visceral que en el mundo físico, ya que el hecho de que no sea necesario coincidir ni en el espacio ni en el tiempo con la víctima del ilícito elimina, en muchos casos, ese componente sorpresivo, de cierta agresividad, que es más complicado que sea determinante es un cibercrimen.

La segunda es que, vistos los distintos y tan alejados perfiles de ciberdelincuentes que hemos dibujado en el apartado anterior (complementados en el anexo), aquí se cumple la premisa que hemos expuesto de que no es posible afirmar con certeza cómo afecta a cada perfil criminológico en el ciberespacio la amenaza de la pena. De hecho, como apuntan Bustos Ramírez y Hormazábal Malarée (1997: 49) en relación con los delitos económicos de escasa entidad, el efecto conminatorio de las penas es realmente escaso. Esto es, sin duda, extrapolable a los ciberdelitos de escasa entidad, al ser ambas manifestaciones del derecho penal moderno y de los nuevos riesgos que acarrean las sociedades posindustriales, y al tratarse de grupos de delitos llevados a cabo por sujetos que no se corresponden con la figura del delincuente clásico, sin un gran desarraigo social como punto fundamental de su iniciación en la delincuencia.

En el marco del ciberespacio es reseñable también que, si tenemos en cuenta que en ocasiones los individuos se sienten más atemorizados por la posibilidad de ser descubiertos que por la amenaza de la pena en sí, la prevención general negativa jugará un papel menos relevante en los ciberdelitos, dadas las dificultades de persecución y enjuiciamiento que se dan en estos ilícitos, por las razones antes expuestas en este estudio. En consecuencia, además, la percepción por parte de la sociedad de que existe una cifra negra muy importante en la ciberdelincuencia rebaja la eficacia coactiva de la pena y de su futura ejecución en términos preventivos y generales.

El alcance de la prevención general positiva

La prevención general, en su vertiente positiva, entiende que la pena busca reafirmar la adhesión y la fidelidad de los ciudadanos al ordenamiento jurídico-penal vigente en cada caso. Dicho de otra forma, se centra en promover la confianza de los individuos en la inquebrantabilidad de las normas penales (Gómez Benítez, 1980: 143; Castro Moreno, 2008: 62-65; Alcácer Guirao, 2001: 50).[25]

25. Sus principales teóricos son Roxin, Hassemer o Jakobs, entre muchos otros. Ahora bien, el principal exponente de esta teoría es el primero de estos tres autores, quien defendía la teoría dialéctica de la unión donde, partiendo de la culpabilidad (la cual juega como fundamento y límite para la concreción de la pena), atendía a fines preventivo-generales y preventivo-especiales. La principal distinción entre estos planteamientos y los de Jakobs es que el segundo de los teóricos encontraba la base de la intervención penal en la protección de la vigencia de la norma y no de bienes jurídicos, como valores esenciales para el desarrollo individual y social de los ciudadanos. Esta teoría ha sido objeto de opiniones contrarias que critican su función autoritaria y expansiva, que no la diferencia demasiado del mero retribu-

La principal implicación de esta teoría en la ciberdelincuencia se trata del desarrollo, que aún se encuentra pendiente en el sentido de reafirmar la vigencia de la norma penal también en el ciberespacio. Afirmamos esto por diversas razones. La primera es que aún existe un gran desconocimiento sobre si el ordenamiento penal rige de la misma manera en el mundo virtual que en el espacio delictivo tradicional, prueba de ello son los casos introducidos en el apartado primero, en los cuales el propio sujeto pasivo no es consciente de haber sido víctima de un ciberdelito. La segunda es la cifra negra de los cibercrímenes que hemos mencionado a lo largo de todo el trabajo, lo que no hace más que contribuir a una sensación de impunidad y a la creencia de que la norma penal no presenta la misma vigencia férrea en el ciberespacio. Una tercera razón es la dificultad de investigación y enjuiciamiento que presentan los ciberdelitos, derivada de la reinterpretación de las reglas de espacio y tiempo. En este caso concreto, cobra especial importancia la cuestión de la competencia territorial y la falta de concreción que a veces existe sobre la nacionalidad del tribunal competente para el conocimiento de cada caso.[26] En definitiva, es necesario un desarrollo y una consolidación del fin preventivo-general positivo de la pena en el ciberespacio y que los individuos tomen conciencia de que no existen diferencias entre la aplicación de la normativa penal con respecto al espacio delictivo tradicional.

El alcance de la prevención especial negativa

Continuamos el análisis con la prevención especial negativa, la cual busca, desde su función intimidatoria, asegurar que el delincuente no vuelva a cometer delitos

cionismo, al perseguir fundamentalmente la autoafirmación del poder punitivo del Estado, huyendo de su función crítica. Además, se trata de un fin de la pena que mira al pasado en lugar de al futuro y se centra en los beneficios y no en los efectos negativos que puede acarrear la pena. Otras voces afirman que se trata de una teoría con función moralizante, ya que trata de imponer una moral determinada a los individuos que conforman una sociedad y confunde, peligrosamente, el derecho con la moral. También es peligroso el planteamiento según el cual el mero fin preventivo-general positivo no encuentra límites a la hora de determinar la pena para conseguir su efecto de reafirmar la vigencia de la norma, algo que podría derivar en una pena desproporcionada si seguimos las pautas que puede exigirnos la sociedad en tiempos de populismo punitivo. Es por esto por lo que parecen adecuados los planteamientos mixtos como los de Roxin, en los que la culpabilidad actúa como fundamento y límite para las penas (Bustos Ramírez y Hormazábal Malarée, 1997: 50; Mir Puig: 1994: 39, por todos).

26. La literatura sobre esta cuestión es muy extensa y demasiado compleja como para abordarla en este trabajo. No obstante, cabe decir que, dependiendo de la teoría que escojamos (actividad, resultado o ubicuidad), obtendremos una respuesta u otra en lo que a la determinación del tribunal competente se refiere. Ahora bien, parece que existe acuerdo en la doctrina internacional en anteponer el principio de justicia universal a los principios de personalidad y territorialidad, en busca de aumentar la cooperación internacional entre los Estados a la hora de perseguir los cibercrímenes (Miró Llinares, 2012: 148; Fernández Teruelo, 2007: 20; Gutiérrez Francés, 2005: 74; Corcoy Bidasolo, 2007: 31; Flor, 2019: 142).

en el futuro. Tanto físicamente, en el tiempo en el que dura la condena privativa de libertad, como sicológicamente con la amenaza de la pena (Gómez Benítez, 1980: 153; Bustos Ramírez y Hormazábal Malarée, 1997: 50-51; Cutiño Raya, 2017: 86).[27]

Del cruce entre esta teoría del fin de la pena y las particularidades de la ciberdelincuencia, es posible cuestionar la vigencia de esta función inocuizadora de las sanciones penales en los cibercrímenes. Decimos esto porque, como hemos visto en las últimas líneas del primer apartado del trabajo, el perfil del ciberdelincuente no corresponde con el criminal clásico con cierto desarraigo social, sino que se trata de sujetos con una estructura socioeconómica estable, en su mayoría. Así, es posible plantearse que la medida de extensión de la pena que marca la prevención especial negativa debe ser menor en los ciberdelitos, según el caso.

El alcance de la prevención especial positiva

Por último, la prevención especial positiva encuentra el fundamento de la pena en la reinserción, la reeducación y la resocialización de los penados como forma de evitación de la comisión de nuevos delitos (Gómez Benítez, 1980: 153; Bustos Ramírez y Hormazábal Malarée, 1997: 50-51; Castro Moreno, 2008: 80).[28]

27. Han teorizado y defendido la prevención especial negativa (también la positiva) autores como Röder o von Liszt, como representante de la Escuela Sociológica Alemana, o Lombroso, Garófalo y Ferri, de la Scuola Positiva italiana, entre muchos otros. Por ejemplo, von Liszt abogaba por la inocuización hacia los criminales habituales como seres incorregibles, por lo que defendía la cadena perpetua para estos casos. Ferri, por su parte, opinaba que el cálculo de la extensión de la pena debía hacerse con base en la peligrosidad del sujeto y no en el hecho ilícito cometido, puesto que el fin de la pena es la evitación de la reincidencia. De lo contrario, estaremos ante una mera retribución moral, a su juicio. En España, Mir Puig (1998: 53) consideraba a los criminales como pacientes sanitarios que precisaban de una medida correctora para ser sanados de su enfermedad. Las críticas sobre esta concepción del fin de la pena se centran en que la prevención especial negativa, por sí sola, no funciona como límite para la extensión penal, ya que la necesidad de inocuización del sujeto puede ser mayor a la medida de la culpabilidad (Demetrio Crespo, 1999: 98). Además, siempre han existido voces detractoras con respecto a las penas privativas de libertad y su compatibilidad con el fin preventivo-especial positivo de las penas, esto es, la reeducación y resocialización del reo, considerándolo como un atentado al libre desarrollo del sujeto (Röder, 1876: 287-288).

28. Los principales teóricos de este pensamiento son los ya introducidos en el subapartado anterior. En el panorama español, Mir Puig introdujo la posibilidad de sustituir las penas por medidas de seguridad para fomentar la resocialización del reo. Ahora bien, la crisis de la prevención especial afectó también a estos postulados cuando surgieron las primeras voces que dejaban en evidencia la falta de medios de los que dispone la Administración Penitenciaria para lograr la reeducación efectiva de los penados. Asimismo, se criticaba abiertamente el componente ideológico que podían imprimir los funcionarios encargados del centro penitenciario en el programa de tratamiento. De nuevo, era cuestionable lo indefinido de los conceptos de reeducación y resocialización de los criminales, lejos de constituir términos exactos cuantificables y determinables científicamente. Además, a día de hoy aún existe el debate sobre

En este caso, y en relación con la ciberdelincuencia, es necesario repetir aquí la misma reflexión abordada para la prevención especial negativa, en el sentido en el que cabe preguntarse si, teniendo en cuenta el perfil habitual de los cibercriminales y su nivel de arraigo con la sociedad, es necesario observar las mismas exigencias de resocialización y reeducación que se deben cumplir con los delincuentes tradicionales.

En este sentido, Juanatey Dorado, en relación con los delincuentes de cuello blanco, apunta que generalmente este tipo de criminales no necesita que su período de estancia en el centro penitenciario esté dirigido a su reinserción social, ya que se trata de sujetos que ya están perfectamente integrados en la sociedad y es, incluso, poco probable que vuelvan a darse las circunstancias en las que tomó la decisión delictiva en el futuro. Así pues, aboga por la suspensión de la ejecución de las penas y por los beneficios penitenciarios por una serie de factores que diferencian a estos perfiles de los del delincuente clásico: su historial individual, familiar y social, su correcta conducta en prisión, la reducida gravedad del delito cometido y la falta de historial delictivo, la inexistencia de causas pendientes, el riesgo de desocialización que existe en su caso y la satisfacción de la responsabilidad civil y la reparación del daño (Juanatey Dorado, 2017: 135-145).

La mayoría de estos factores, vistos los perfiles de los ciberdelincuentes que hemos expuesto en el primer apartado del trabajo, también son extrapolables a los cibercriminales y, en consecuencia, también lo es, generalmente, la falta de necesidad de dirigir la pena hacia la prevención especial positiva.[29]

Conclusiones

Por todo lo expuesto hasta el momento, y tras analizar tanto el fenómeno de la ciberdelincuencia en profundidad como sus implicaciones en la teoría de los fines de la pena, es posible extraer cuatro conclusiones principales.

En primer lugar, en relación con las teorías absolutas o retributivas, es latente que, vista la superior capacidad lesiva que pueden presentar los ciberdelitos, la medida de la culpabilidad será, en ocasiones, superior y, en consecuencia, también deberá serlo la extensión del marco penal. Ahora bien, esta medida de la culpabilidad deberá limitarse también por el nivel de reprochabilidad del delito que, en el caso de los cibercrímenes, podrá verse reducido por la contribución de las víctimas en ellos.

---

si una pena de privación de libertad es la idónea para el programa de reeducación y si, en sentido contrario al que se persigue, no se trata de una medida desocializadora (Roxin, 1991: 47-48).

29. En el anexo del trabajo se recogen los perfiles más significativos de los ciberdelincuentes con el fin de tratar de llevar a cabo una caracterización lo más fiel posible de estos criminales. Así, de su estudio es posible identificar ciertas similitudes con los delincuentes de cuello blanco: antiguos trabajadores de empresas o delincuentes primarios, por ejemplo, son caracteres que encajan con ambas figuras.

Ahora bien, como hemos comprobado en el análisis de las restantes teorías, los fundamentos retributivos son los únicos basados en comprobaciones empíricas, algo que presenta aún más valor en la justificación del castigo penal de un fenómeno tan volátil y pendiente de explorar como la ciberdelincuencia. No es extraño comprobar, por tanto, cómo surgen corrientes doctrinales como las expuestas en este estudio, que abogan por devolver el protagonismo a esta teoría.

En segunda instancia, es posible afirmar que el fin preventivo-general negativo de la pena en los ciberdelitos tiene una relevancia menor que en el espacio físico tradicional. A pesar de que la decisión delictiva en el ciberespacio es menos visceral, el efecto conminatorio de la pena en los ciberdelitos de escasa entidad es poco relevante y las dificultades existentes en torno a su persecución e investigación, que derivan en una elevada cifra negra, rebajan la eficacia intimidatoria de las penas aparejadas a los cibercrímenes. Así, en términos disuasorios, es relevante abordar la cuestión desde una perspectiva interdisciplinar, que utilice herramientas no solo jurídicas y de técnica legislativa, sino también técnicas, sociológicas o político-criminales. Esto aumentaría la amenaza de la pena en el ciberespacio, no solo por su proporcionalidad con el desvalor causado, sino por la certeza de que los ciberdelitos no quedan impunes.

Como tercera conclusión, podemos traer a colación el hecho de que el fin preventivo-general positivo de las penas en la ciberdelincuencia está aún pendiente de un mayor desarrollo, dada la percepción que rodea a estos ilícitos de que la ley penal en el ciberespacio no rige con el mismo rigor que el mundo físico.

Por último, es muy relevante mencionar que el hecho de que el perfil del ciberdelincuente se trate, en su mayoría, de un sujeto con mucho más arraigo social que el criminal tradicional, se traduce en que no sean tan funcionales los fines preventivo-especiales a la hora de la ejecución de las penas. Todo esto, debería derivar en la facilitación de la suspensión de su ejecución y de los beneficios penitenciarios, siempre y cuando se cumplan los requisitos para ello.

Ahora bien, como hemos observado a lo largo de todo el trabajo, los perfiles de los ciberdelincuentes son muy diversos entre sí y, de hecho, lo más probable es que existan también diferencias entre los reos que aparentemente pueden encajar dentro de una misma descripción general. Por lo tanto, las implicaciones concretas de cada fin de la pena en cada caso deberán extraerse en el caso concreto. En definitiva, hacemos nuestro el planteamiento de Stratenwerth (1996: 25-38), quien, en un intento en convertir los postulados de la teoría de los fines de la pena en consecuencias concretas, llega a la conclusión de que no es posible obtener evidencia empírica sobre los fines penales y existen contradicciones e incompatibilidad entre los distintos fines. Por ende, lo más acertado es seguir las teorías de la unión que nos invitan a no aplicar ninguno de ellos con exclusividad, sino buscar el equilibrio adecuado en función del delito cometido y las circunstancias concretas del penado, ya que la teoría de los fines de la pena como tal solo debe limitarse a aportar un parámetro crítico desde el cual

medir la realidad y nunca podrá aportar una solución tanto general como definitiva. Esto, además, permite aplicar estos dogmas generales a los distintos fenómenos criminales que vayan surgiendo gracias a la evolución de la sociedad, como es, precisamente, el caso de la ciberdelincuencia.

No obstante, sigue siendo relevante ahondar en el análisis de la vigencia de los fines de la pena en estas nuevas formas de criminalidad, con el fin de dibujar, al menos, un marco para fundamentar la intervención penal. En particular, son tres las directrices a seguir en este sentido. La primera, la revisión de las teorías retributivas y su función de límite de la culpabilidad, como fundamento empírico del castigo penal. La segunda, el concepto de disuasión en el ciberespacio y la necesidad de trabajo coordinado entre las distintas disciplinas sociales para rebajar la cifra negra en los ciberdelitos y, en consecuencia, aumentar la amenaza penal y la confianza en el sistema. Por último, la revisión de la ejecución de las penas privativas de libertad en los cibercrímenes, en estrecha relación con un perfil de delincuente sin necesidad, en ocasiones, de procesos de reeducación y reinserción social.

Anexo: Perfiles más significativos de ciberdelincuentes

El primero de ellos describe a un trabajador desleal y resentido que, al abandonar la empresa y con finalidad vengativa, ataca sus sistemas de almacenamiento de datos valiéndose de sus accesos y de los conocimientos adquiridos en su puesto de trabajo. En la doctrina anglosajona este perfil es conocido como *insider.* En estos casos, podríamos estar hablando de un delito de daños informáticos o *cracking* del artículo 264 del Código Penal o de *denial of service* del artículo 264 bis, dependiendo de si el autor borre o altere algún dato de la empresa o, directamente, interrumpa el entero funcionamiento del sistema informático con el que solía trabajar (Velasco Núñez, 2010: 44).

El segundo perfil responde a un delincuente con desarrolladas capacidades informáticas, el cual boicotea de alguna manera los útiles informáticos de un ente ajeno y, tras conseguirlo, se ofrece de forma anónima o encubierta para restaurar el estado de las cosas tras la vulneración creada por él. El sujeto incurriría, en esta ocasión, en un delito de daños informáticos, como los expuestos en el párrafo anterior, por ejemplo. Un colectivo profesionalizado que se guía por estas pautas de comportamiento son los *viruckers,* quienes entran en un sistema informático para introducir un virus en él, con el objetivo de destruir, alterar o inutilizar la información alojada en este. Es posible diferenciar entre virus benignos (que molestan, pero no hacen daño) y malignos. Del mismo modo, este perfil se corresponde con los ciberestafadores, quienes pueden incurrir en conductas de *phishing, pharming,* falsas ventas o falsas subastas (Barrio Andrés, 2017: 129 o De la Cuesta y Pérez Machío, 2010: 107-108).

También es común, en tercer término, la vocación delictiva en un delincuente primario, ocasional y solitario que, con reducidos conocimientos informáticos, pero

aprovechando las posibilidades en forma de herramientas y de accesible formación, se vale de internet para inmiscuirse en las intimidades, secretos que tanto sus allegados (exparejas sentimentales, compañeros de trabajo, competidores laborales, compañeros de estudios, etcétera) como personajes con cierta proyección pública puedan tener con el fin de sacarlos a la luz por vías telemáticas accesibles a la generalidad. Incurriendo, claro está, en delitos de descubrimiento y revelación de secretos de los artículos 197 y siguientes del Código Penal, con clara afectación a la intimidad de las víctimas (Velasco Núñez, 2010: 45).

Los más jóvenes también pueden ejercer el papel de sujeto activo en ciertas conductas delictivas en un mundo virtual, donde ellos han desarrollado sus habilidades desde la infancia de forma natural. Así pues, son habituales hoy en día los casos de *cyberbulling* o *mobbing* o *stalking* por la facilidad de captación instantánea de imágenes y sonido que poseen gracias a sus teléfonos móviles, y al habitual uso que dan a estas edades de herramientas de comunicación virtual como chats, redes sociales, correos electrónicos o, incluso, chats de videojuegos. La normalización de estas conductas entre sus pares y la minimización de los riesgos aparejados a estos comportamientos no hacen más que fomentar nuevas modalidades delictivas, a medida que surgen novedosos sistemas de intercambio de información en la red (Hyland y otros, 2018: 47-50; Villacampa Estiarte y Pujols Pérez, 2018: 183-185).

Asimismo, es también conocido el caso del *child grooming*, en el que sujetos de mediana o avanzada edad, generalmente varones, simulan su edad gracias a las posibilidades de anonimato y simulación de identidad que permite la red para llevar a cabo un acercamiento con intenciones sexuales hacia menores que, en la red, se encuentran vulnerable ante este tipo de amenazas. Esta modalidad delictiva encaja en el artículo 183, ter. 1, del Código Penal. También es habitual el caso del *sexting*, que se concreta en el embaucamiento de un menor por medio de las tecnologías de la información y la comunicación para obtener o conseguir la exhibición de material pornográfico, y está castigado en el apartado segundo de este mismo precepto (Górriz Royo, 2016: 16-17).

El discurso de odio o, en su denominación inglesa, *hate speech*, ha alcanzado una nueva significación en los últimos años, sobre todo gracias al auge y el creciente uso de las redes sociales. Ahora bien, este delito no cuenta con un perfil de ciberdelincuente muy marcado, sino que cualquiera puede verter en internet contenidos susceptibles de constituir un delito siempre que encaje en uno de los dos grupos de discursos del odio penalmente relevantes: los que incitan a un peligro de actuación real e inminente y los que, en un nivel de gravedad menor, contribuyen eficazmente a denostar al colectivo vulnerable de referencia. El legislador, además, distingue dos elementos comunes para todas las conductas subsumibles en esta modalidad delictiva: que la acción se dirija contra un colectivo vulnerable y que exista un elemento subjetivo motivacional basado en la voluntad de crear odio, violencia o discriminación (Landa Gorostiza, 2018: 222-223).

Tampoco es posible definir de forma nítida el perfil del sujeto que lleva a cabo actos de ciberterrorismo. Ahora bien, es relevante apuntar que existen tres conductas principales al respecto. La primera de ellas es el tipo descrito en el artículo 573.2 del código penal, el cual recoge los mismos fines de la conducta del tipo básico del delito de terrorismo cuando estos objetivos se buscan con uno de los delitos informáticos de los artículos 197 bis y ter (allanamiento informático, producción y facilitación, entre otros, de programas informáticos o claves de acceso para ello) y de daños informáticos tipificados entre los artículos 264 y 264 quáter (explicados antes en este mismo apartado) (Llobet Anglí, 2015: 433-435; Cancio Meliá, 2010: 259).

La segunda conducta digna de subrayar es el autoadoctrinamiento o autoadiestramiento para la comisión de un delito terrorista, recogido en el 575.2, del Código Penal. Esta se centra en quien accede de manera habitual a servicios de comunicación accesibles al público a través de internet o de otro medio de comunicación electrónico de forma idónea para incitar a colaborar o incorporarse a una organización terrorista. En consecuencia, este delito, en concreto, se trataría de un ciberdelito en sentido estricto.

El artículo 578 del Código Penal, por su lado, recoge el delito de enaltecimiento del terrorismo, el cual, desde la concepción amplia de los ciberdelitos, puede considerarse un cibercrimen. Así, en primer lugar, el artículo 578.1, recoge dos conductas diferenciadas: la primera, la de enaltecer o justificar públicamente los delitos de los artículos 572 a 577 (delitos de terrorismo) o de sus autores y/o partícipes; y la segunda, la consistente en llevar a cabo actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares.

Referencias

Alcácer Guirao, Rafael (2001). *Los fines del derecho penal*. Buenos Aires: Ad hoc.

Almenar Pineda, Francisco (2018). *Ciberdelincuencia*. Oporto: Juruá.

Antón Oneca, José (1965). *Los fines de la pena según los penalistas de la Ilustración*. Madrid: Instituto de Ciencias Jurídicas.

Barrio Andrés, Moisés (2017). *Ciberdelitos: Amenazas criminales del ciberespacio*. Madrid: Reus.

—. (2018). *Delitos 2.0: Aspectos penales, procesales y de seguridad de los ciberdelitos*. Madrid: Wolters Kluwer.

Bequai, August (1978). *Computer crime*. Massachusetts: Lexington Books.

Bustos Ramírez, Juan J. y Hernán Hormazabal Malarée (1997). *Lecciones de derecho penal*. Tomo I. Madrid: Trotta.

Cancio Meliá, Manuel (2010). *Los delitos de terrorismo: Estructura típica e injusto*. Madrid: Reus.

Castro Moreno, Abraham (2008). *El por qué y el para qué de las penas*. Madrid: Dykinson.

Clough, Jonathan (2010). *Principles of cybercrime*. Nueva York: Cambridge University Press.

Corcoy Bidasolo, Mirentxu (2007). «Problemática de la persecución penal de los denominados delitos informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos». *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, 21: 7-32.

Cutiño Raya, Salvador (2017). *Fines de la pena, sistema penitenciario y política criminal.* Valencia: Tirant lo Blanch.

Davara Rodríguez, Miguel Ángel (2015). *Manual de derecho informático*. Pamplona: Aranzadi Thomson Reuters.

—. (2017). «Un primer acercamiento a la ciberdelincuencia». *Consultor de los ayuntamientos y de los juzgados*, 9: 1240-1246.

De la Cuesta Arzamendi, José Luis y Ana Isabel Pérez Machío (2010). «Ciberdelincuentes y cibervíctimas». En José Luis de la Cuesta Arzamendi (director), *Derecho penal informático*. Pamplona: Civitas y Thomson Reuters.

De la Cuesta Arzamendi, José Luis, Ana Isabel Pérez Machío y César San Juan Guillén (2010). «Aproximaciones criminológicas a la realidad de los ciberdelitos». En José Luis de la Cuesta Arzamendi (director), *Derecho penal informático*. Pamplona: Civitas y Thomson Reuters.

Demetrio Crespo, Eduardo (1999). *Prevención general e individualización judicial de la pena*. Salamanca: Universidad de Salamanca.

Diamond, Brie y Michael Bachmann (2015). «Out of the beta phase: obstacles, challenges and promising paths in the study of cyber criminology». *International Journal of Cyber Criminology*, 1 (9): 24-34.

Eser, Albin (2002). «Internet und internationales Strafrecht». En Dieter Leipold (compilador), *Rechtsfragen des Internet und der Informationsgesellschaft*. Heidelberg: C. F. Müller.

Fernández Teruelo, Javier Gustavo (2007). *Cibercrimen: Los delitos cometidos a través de internet*. Madrid: Constitutio Criminalis Carolina.

Fischer, Thomas (1979). *Computer-Kriminalität*. Berna: Paul Haupt.

Flor, Roberto (2019). «La legge penale nello spazio, fra evoluzione tecnológica e difficoltà applicative». En Alberto Cadoppi (compilador), Cybercrime. Milán: Utet Giuridica.

Gercke, Marco y Phillip W. Brunst (2009). *Praxishandbuch Internetstrafrecht*. Stuttgart: W. Kohlhammer.

Gómez Benítez, José Manuel (1980). «Racionalidad e irracionalidad en la medición de la pena». *Revista de la Facultad de Derecho de la Universidad Complutense de Madrid*, 3: 129-194.

Górriz Royo, Elena (2016). «*Online child grooming* en Derecho penal español». *InDret:Rrevista para el análisis del Derecho*, 3: 1-47.

Gutiérrez Francés, María Luz (2005). «Reflexiones sobre la ciberdelincuencia hoy (en torno a la ley penal en el espacio virtual)». *Revista Electrónica del Departamento de Derecho de la Universidad de La Rioja*, 3: 69-92.

Hassemer, Winfried (1984). *Fundamentos del derecho penal.* Barcelona: Bosch.

Hayward, Keith J. (2012). «Five spaces of cultural criminology». *The British Journal of Criminology*, 52: 441-462.

Hernández Moreno, Alberto (2017). «Ciberseguridad y confianza en el ámbito digital». *Información Comercial Española, ICE: revista de economía*, 897: 55-66.

Hilgendorf, Eric y Brian Valerius (2012). *Computer-und Internetstrafrecht*. Berlín: Springer.

Huber, Edith (2019). *Cybercrime*. Wiesbaden: Springer.

Hyland, John M., Pauline K. Hyland y Lucie Corcoran (2018). «Cyber aggression and cyberbullying: widening the net». En Hamid Jahankhani (compilador), *Cyber Criminology* (pp. 47-50). Londres: Springer.

Jewkes, Yvonne y Majid Yar (2013). *Handbook of Internet crime*. Nueva York: Routledge.

Juanatey Dorado, Carmen (2017). «Función y fines de la pena: La ejecución de penas privativas de libertad en el caso de los delincuentes de cuello blanco». *Revista Penal*, 40: 126-145.

Landa Gorostiza, Jon Mirena (2018). «El discurso de odio criminalizado: propuesta interpretativa del artículo 510 Código Penal». En Jon Mirena Landa Gorostiza y Enara Garro Carrera (compiladores), *Delitos de odio: Derecho comparado y regulación española* (pp. 222-223). Valencia: Tirant lo Blanch.

Lardizábal y Uribe, Manuel de (1997). *Discurso sobre las penas.* Granada: Comares.

Lessig, Lawrence (2002). «*Las leyes del ciberespacio». Themis: Revista de Derecho*, 44: 171-179.

Leukfeldt, Rutger, Sander Veenstra y Wouter Stol (2013). «High volume cybercrime and the organization of the police: The results of two empirical studies in the Netherlands». *International Journal of Cyber Criminology*, 1 (7): 1-7.

Llobet Anglí, Mariona (2015). «Delitos contra el orden público». En Jesús-María Silva Sánchez (compilador), *Lecciones de derecho penal: Parte especial* (pp. 433-435). Barcelona: Atelier.

Luzón Peña, Diego Manuel (1979). *Medición de la pena y sustitutivos penales.* Madrid: Instituto de Criminología de la Universidad Complutense de Madrid.

Maimon, David (2020). «Deterrence in Cyberspace: an interdisciplinary review of the empirical literature». En T. Holt y A. Bossler (compiladores), *The palgrave handbook of cybercrime and cyberdeviance*. Londres: Palgrave Macmillan.

Mañalich Raffo, Juan Pablo (2007). «La pena como retribución. Primera parte: La retribución como teoría de la pena». *Derecho Penal y Criminología*, 83: 37-74.

—. (2007). «La pena como retribución. Segunda parte: La retribución como teoría

del Derecho penal». *Derecho Penal y Criminología*, 83: 75-120.

Marqués de Beccaria (1993). *De los delitos y las penas.* Madrid: Biblioteca Nacional.

Mata y Martín, Ricardo M. (2001). *Delincuencia informática y derecho penal*. Madrid: Edisofer.

Mir Puig, Santiago (1994). *El derecho penal en el Estado social y democrático de derecho*. Barcelona: Ariel.

—. (1998). *Derecho penal: Parte general*. Barcelona: PPU.

Miró Llinares, Fernando (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Moore, Robert (2011). *Cybercrime.* Oxford: Elsevier.

Morón Lerma, Esther (2002). *Internet y derecho penal: Hacking y otras conductas ilícitas en la red*. Pamplona: Aranzadi.

Owen, Tim (2017). «The problems of virtual criminology». En Tim Owen, Wayne Noble y Christabel Faye (compiladores), *New perspectives on cybercrime*. Preston: Palgrave MacMillan.

Robinson, Paul H., Manuel Cancio Meliá e Íñigo Ortiz de Urbina Gimeno (2012). *Principios distributivos del Derecho penal: a quién debe sancionarse y en qué medida*. Madrid: Marcial Pons.

Röder, Carlos David Augusto (1876). *Las doctrinas fundamentales reinantes sobre el delito y la pena en sus interiores contradicciones*. Madrid: Librería de Victoriano Suárez.

Romeo Casabona, Carlos María (2006). «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal». En Carlos María Romeo Casabona (compilador), *El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales* (pp. 8-27). Granada: Comares.

—. (2007). «De los delitos informáticos al cibercrimen». En Fernando Pérez Álvarez, Miguel Ángel Núñez Paz y Isabel García Alfaraz (compiladores), *Universitas vitae: homenaje a Ruperto Núñez Barbero*. Salamanca: Universidad de Salamanca.

Rovira del Canto, Enrique (2002). *Delincuencia informática y fraudes informáticos*. Granada: Comares.

Roxin, Claus (1991). *Culpabilidad y prevención en derecho penal*. Madrid: Reus.

Sieber, Ulrich (1980). *Computerkriminalität und Strafrecht*. Colonia: Carl Heymanns.

—. (1992). «Criminalidad informática: peligro y prevención». En Santiago Mir Puig (compilador), *Delincuencia informática* (pp. 29-30). Barcelona: PPU.

Stratenwerth, Günther (1996). «¿Qué aporta la teoría de los fines de la pena?», *Cuadernos de conferencias y artículos de la Universidad Externado de Colombia*, 8.

Valiente García, Francisco Javier (2004). «Comunidades virtuales en el ciberespacio». *Doxa comunicación: Revista Interdisciplinar de Estudios de Comunicación y Ciencias Sociales*, 2: 137-150.

Velasco Núñez, Eloy (2010). *Delitos cometidos a través de Internet: Cuestiones procesales*. Madrid: La Ley.

Villacampa Estiarte, Carolina y Alejandra Pujols Pérez (2018). «El delito de *stalking* en el Código Penal español». En Carolina Villacampa Estiarte (compiladora), *Stalking: Análisis jurídico, fenomenológico y victimológico* (pp. 183-185). Pamplona: Thomson Reuters Aranzadi: 183-185.

Viota Maestre, Manuel (2007). «Problemas relacionados con la investigación de los denominados delitos informáticos (ámbito espacial y temporal, participación criminal y otros)». *Cuadernos Penales José María Lidón*, 4: 237-257.

Vivó Cabo, Silvia (2018). «La globalización del delito: ciberdelincuencia». *La Ley penal: Revista de Derecho Penal, Procesal y Penitenciario*, 132.

Wernert, Manfred (2017). *Internetkriminalität.* Stuttgart: Boorberg.

Sobre el autor

Jon López Gorostidi es profesor de Derecho Penal en la Universidad de Deusto, España. Además, es doctor en Derecho Económico y de la Empresa por la Universidad de Deusto, España. Doble graduado en ADE + Derecho por la Universidad de Deusto, España. Máster en Sistema de Justicia Penal por la Universidad de Lleida, España, y máster en Acceso a la Abogacía por la UNED. Su correo electrónico es jlgorostidi@deusto.es https://orcid.org/0000-0001-5532-9354.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

DIRECTOR

Daniel Álvarez Valenzuela

(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).