LA PLURALIDAD DE VÍCTIMAS DERIVADA DE LA ELEVADA LESIVIDAD EN LOS CIBERDELITOS: UNA RESPUESTA PENAL PROPORCIONAL

Victim multiplicity derived from harm in cybercrime: A proportional criminal response

Jon López Gorostidi
Investigador predoctoral
Profesor de Derecho penal
Universidad de Deusto
jlgorostidi@deusto.es

http://dx.doi.org/10.18543/ed-68(1)-2020pp201-221

Recibido: 10.10.2019
Aceptado: 02.02.2020

Resumen

El siguiente trabajo aborda la cuestión del cibercrimen desde la perspectiva de la víctima y analiza este extremo con base en los principios penales fundamentales y la proporcionalidad.

Más concretamente, se centra en el hecho de que el cibercrimen presenta un nivel elevado de lesividad en comparación con los delitos tradicionales, cometidos por los medios comisivos habituales, y en consecuencia, el número de resultados lesivos por cada comportamiento humano penalmente relevante puede aumentar considerablemente.

Es por esto por lo que es necesario un examen que se cuestione si la respuesta penal actual a este tipo de delitos cibernéticos es adecuada en términos de proporcionalidad entre el daño causado y la pena aparejada a cada delito.

Así, el presente trabajo reflexiona sobre la respuesta penal otorgada por el Código Penal español, tanto por medio de preceptos de parte general (como la figura del delito continuado o los delitos cualificados), como por figuras penales específicas.

Palabras clave

cibercrimen, proporcionalidad, lesividad, Derecho penal, ciberdelincuencia.

Abstract

This paper approaches cybercrime from the victim perspective and analyses the matter regarding the fundamental criminal principles of harm and proportionality.

Precisely, it is since cybercrime presents an elevated level of harm compared to traditional criminality and, as a result, the number of victims in each criminal action can be easily increased.

Consequently, a conscious review of the principle of proportionality between the caused harm and the penal response in each case becomes compulsory, questioning if the current criminal legislation gives an adequate response.

For this aim, the paper analyses the way the Spanish Criminal Code manages the issue, with both general articles (such as the figure of continuous crimes or aggravations) or concrete criminal figures.

Keywords

cybercrime, proportionality, harm, Criminal Law, computer crime.

I. INTRODUCCIÓN: EL CIBERESPACIO COMO ESPACIO DELICTIVO SINGULAR

Es latente que existen diversas características distintivas en los ciberdelitos dignas de mención y análisis, que configuran el ciberespacio como un espacio delictivo novedoso el cual invita a la doctrina especializada a plantearse si son adecuadas para la ciberdelincuencia las respuestas penales creadas para cubrir el espacio físico tradicional. Son solo muestras de ello las novedosas características técnicas, lógicas y de uso de las TIC, la cuestión de la cifra negra en los ciberdelitos, la contribución de la víctima desde un plano victimológico, la reinterpretación de las reglas espaciotemporales, la superior capacidad lesiva de estos injustos o la pluralidad de potenciales víctimas existentes.

No obstante, son las dos últimas cuestiones mencionadas al inicio de esta introducción las que van a ser objeto de examen en este estudio, puesto que busca subrayar la frecuencia en la que la víctima no se trata de un individuo singular, sino que el titular del bien jurídico protegido en los cibercrímenes son, a menudo, una pluralidad de personas. Esto es debido, principalmente, a la capacidad multiplicadora que ofrecen las TIC, lo que lleva, en ocasiones, a enfrentarnos incluso a la indeterminación de la cuantía y la identidad de los afectados[1]. Cuestiones a las que se dedica un epígrafe específico con el apartado segundo del trabajo.

Ahora bien, tratamos de introducir en los subapartados que siguen unas líneas generales sobre el resto de los caracteres del ciberespacio como lugar de comisión de los ciberdelitos.

[1] Carlos María Romeo Casabona, «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* ed. por Carlos María Romeo Casabona (Granada: Editorial Comares, 2006)*,* 26-27.

1. *Características de uso, técnicas y lógicas de la red y de las TIC*

Resulta adecuado comenzar la enumeración de características del ciberespacio por la descripción de los factores que hacen que la propia red Internet y, en un plano general, las TIC sean el escenario ideal para la actividad criminal que nos ocupa.

Un primer distintivo de Internet es la capacidad de procesar, albergar y circular, de forma automática y a tiempo real, colosales cantidades de información en distintos (y cada vez más) soportes digitales[2]. Esto es posible gracias a los protocolos universales de transmisión y acceso y resultan en una herramienta de una potencialidad sin parangón para los ciberdelincuentes, puesto que permiten el envío bidireccional de texto, sonido, imagen o voz con los únicos límites que la velocidad de la propia red y la capacidad de procesamiento del sistema informático utilizado impongan[3].

Esto, unido a la extraordinaria capacidad de procesamiento, almacenamiento y envío de datos, se traduce, como comprobaremos más adelante, en la dificultad de supervisión y control que preside la red[4]. Internet, al contar con una estructura descentralizada y no jerarquizada, no permite la existencia natural de órganos o instituciones de control. En consecuencia, a pesar de que es posible aprobar protocolos de actuación en clave de seguridad, como el rastreo de direcciones IP o la censura sistemática, un control exhaustivo de tal ingente cantidad de información es absolutamente inviable[5].

Así pues, gracias a esta característica, el ciberespacio es un terreno especialmente proclive para facilitar conductas ilícitas en las que una transmisión clandestina de una gran cantidad de información resulta crucial. Por ende, injustos como el *phishing,* los daños informáticos vía virus, los delitos de piratería contra la propiedad intelectual o para la difusión de pornografía infantil, entre otros, son potenciados por las bondades técnicas de las nuevas tecnologías.

En la misma línea, es necesario subrayar también el inabarcable número de usuarios que utilizan la red y la frecuencia de acceso y de uso que estos hacen de esta tecnología[6]. Los sistemas informáticos con acceso a Internet han copado todas y cada una de nuestras actividades cotidianas y derivan

[2] *Ídem*, 3.

[3] Antonio Asencio Guillén, «El ciberespacio como sistema y entorno social: una propuesta teórica a partir de Niklas Luhmann», *Comunicación y Sociedad*, vol. 31, núm. 1 (2018): 23-36.

[4] Carlos María Romeo Casabona, «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», 3.

[5] Lawrence Lessig, «Las leyes del ciberespacio», *THEMIS: revista de Derecho*, núm. 1 (2002): 171-179.

[6] Carlos María Romeo Casabona, «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», 3.

irremediablemente al hecho de que son escasos los momentos en el día en el que no intercambiamos, al menos, un par de mensajes instantáneos o en los que no descargamos o subimos información a la red[7].

Como consecuencia, estos millones de usuarios diarios podemos ser tanto potenciales víctimas como los propios sujetos activos de hechos ilícitos, sin necesidad de una mayor preparación o tener acceso a ningún tipo de herramienta electrónica determinada[8]: el mero hecho de estar conectado a Internet y poder interactuar en el ciberespacio es condición suficiente para ser víctima o participar activamente en la comisión de un delito, gracias a la libre circulación y navegación que preside el sistema.

Asimismo, las posibilidades de anonimato y/o simulación de personalidad que la red permite facilitan la comisión delictiva y la decisión de perpetrar el injusto y, al mismo tiempo, dificultan la persecución del mismo[9]. Es posible que el rechazo y las inherentes represalias sociales lleven a un potencial delincuente a no cometer un injusto penal en el espacio tradicional, pero que el ciberespacio y la posible eliminación de estas consecuencias lo impulsen a tomar la decisión criminal. Además, siendo factible el seguimiento del rastro digital que una dirección concreta deja tras su navegación, pudiendo así identificar el terminal desde el cual se llevaron a cabo los actos que derivaron en la comisión de un delito, es siempre tarea complicada el identificar quién en concreto hizo uso de ese sistema informático en el momento de los hechos.

Por ello, estos caracteres de inimaginable número de usuarios y consultas diarias, junto con el anonimato y dificultad de persecución en la red, convierten el ciberespacio en un escenario adecuado para la perpetración de ilícitos como el *phishing,* el *pharming,* los delitos de espionaje informático, el blanqueo de capitales, los delitos de acoso sexual vía redes, el *stalking,* los delitos de injurias y calumnias, las amenazas, coacciones o extorsiones, la incitación al odio o a la violencia, los delitos de suplantación de personalidad o el ciberterrorismo.

Por último, las características lógicas de las TIC permiten que estas sean alteradas e intervenidas en cualquier momento por (casi) cualquier usuario, lo que se concreta en el permanente interrogante de si en realidad llegó a alterarse un dato o un fichero y desde qué terminal se llevó a cabo dicho movimiento[10].

[7] Francisco Javier Valiente García, «Comunidades virtuales en el ciberespacio», *Doxa comunicación: revista interdisciplinar de estudios de comunicación y ciencias sociales*, núm. 2 (2004): 137-150.

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

[9] Lawrence Lessig, «Las leyes del ciberespacio», 171-179.

[10] Carlos María Romeo Casabona, «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», 3.

Siendo esto así, son habituales los casos en los cuales se tiene acceso a información sin el consentimiento de sus responsables o creadores o se manipulan y alteran datos con propósitos presididos por la mala fe en entornos empresariales. Siempre desde la cómoda posición de anonimato que la red otorga y la dificultad de persecución que acabamos de subrayar[11].

Ejemplos de delitos que aprovechan estos factores son los de defraudación y hurto de tiempo por uso de sistemas de telecomunicaciones, los de daños informáticos, los delitos contra la propiedad intelectual e industrial, los de espionaje informático y secretos de empresa, los de falsedad de documentos y tarjetas, los delitos de pornografía infantil y los de descubrimiento y revelación de secretos.

2. *La cifra negra en los ciberdelitos*

También es necesario tratar la cuestión de la cifra negra existente[12] en la ciberdelincuencia.

Si bien los informes de la Fiscalía General del Estado apenas hacen mención de la cibercriminalidad, desde muchos ámbitos se sigue afirmando que su amenaza es creciente y nuestra propia experiencia de uso nos dicta que la frecuencia criminal en el ciberespacio no hace más que ir en aumento. Es más, se percibe un ambiente contradictorio en torno a esta cuestión, ya que se exageran ciertos aspectos, en un tono alarmista, sobre la ciberdelincuencia, a la vez que se banalizan otros, restándole importancia a la cuestión[13].

Esto es debido a la exageración de ciertos peligros en la red, con el exceso de publicidad que se les otorga a ciertas amenazas virtuales, junto con la desinformación y el desconocimiento que preside la cuestión para el público general. Lo cual deriva en una alarma inicial cuando, por ejemplo, llega a nuestros oídos un ataque de denegación de servicio contra un partido político y se convierte en incredulidad y minusvaloración si escuchamos la creciente posibilidad de un ciberataque terrorista[14]. Más aún, si la amenaza sobre los inminentes peligros de la red e Internet se lleva prolongando durante varios años y, sin embargo, la percepción es que nuestros tribunales siguen

[11] Francisco Javier Valiente García, «Comunidades virtuales en el ciberespacio», 139.

[12] Miguel Gómez Perals, «Los delitos informáticos en el derecho español, en Informática y Derecho», *Informática y Derecho: revista iberoamericana de Derecho informático*, nº 4 (1994): 483.

[13] Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* (Madrid: Editorial Marcial Pons, 2012), 289.

[14] Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* 289-291.

ocupándose de delitos contra la seguridad vial, de violencia de género y de tráfico de drogas, esencialmente.

A continuación, se enumeran los factores que dan pie al fenómeno de la cifra negra en los ciberdelitos.

Un primer factor relevante, a día de hoy, para la justificación del fenómeno es sin duda el elevado nivel de tecnicidad que ha alcanzado la tecnología en su parcela informática, lo que dificulta enormemente las tareas de persecución de los delitos[15]. La autoridad policial y judicial se encuentran, en ocasiones, faltos de medios a la hora de investigar e instruir ciertas causas cibercriminales por lo complejo de su desarrollo y la alta cualificación de los delincuentes en la red[16].

Es más, la tarea más complicada a la hora de instruir un cibercrimen suele ser la inicial de identificar al presunto criminal, puesto que las denuncias en muchas ocasiones no van dirigidas a un usuario determinado, sino que las casuística es muy variada, pero con la característica común de la falta de identificación inicial del denunciado[17]: desplazamientos patrimoniales por una estafa informática, daños en sistemas informáticos vía virus o calumnias en redes sociales por medio de un perfil falso, son ejemplos de esto.

Con todo, el anonimato que aporta el ciberespacio, el carácter transnacional del delito y las novedosas reglas espaciotemporales fomentan la cifra negra de la ciberdelincuencia por su dificultad de persecución.

No es desdeñable tampoco la cuestión de que, en ocasiones, las propias víctimas desconocen su condición de sujetos pasivos del delito[18], de nuevo por las características de naturaleza técnica que presiden estos supuestos[19]. Son habituales las intromisiones en sistemas informáticos ajenos por vías telemáticas a tiempo real, sin que el perjudicado logre tomar conciencia del potencial delito, o los ataques, copias y transmisiones de estos bienes informáticos sin dejar rastro[20], lo que deriva en que el sujeto pasivo no tome conciencia de la lesión que ha sufrido o lo haga una vez transcurrido un periodo

[15] Luis Miguel Reyna Alfaro, «Aproximaciones criminológicas al delito informático», *Capítulo Criminológico*, vol. 31, núm. 4 (2003), 99.

[16] José Luis de la Cuesta Arzamendi y Ana Isabel Pérez Machío, «Ciberdelincuentes y cibervíctimas», *Derecho penal informático*, ed. por De la Cuesta Arzamendi, José Luis (Pamplona, Editorial Civitas - Thomson Reuters, 2010), 116.

[17] Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* 295.

[18] M. Carmen Alastuey Dobón, «Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial», *Informática y Derecho: revista iberoamericana de Derecho informático*, nº 4 (1994): 457.

[19] José Luis de la Cuesta Arzamendi y Ana Isabel Pérez Machío, «Ciberdelincuentes y cibervíctimas», 116.

[20] Esther Morón Lerma, *Internet y Derecho penal: hacking y otras conductas ilícitas en la red,* (Pamplona: Editorial Aranzadi, 2002), 27.

de tiempo[21]. Otro ejemplo de esta situación lo puede constituir el caso en el que un usuario de una red social injurie o calumnie a otro, sin que este último se percate, lo que no impida que el resto de los usuarios del servicio consuman dichas información, potencialmente delictiva que, generalmente, nunca será denunciada. Esto es, existe una *macro-victimización*[22] muy difícil de determinar y cuantificar, que a menudo es percibida por la víctima cuando ya es absurdo ejercer acciones legales por los costes que estas acarrearían o por haber prescrito o, incluso, que nunca es percibida por esta[23].

También es habitual el supuesto en el cual la víctima sí es consciente del ciberataque en un primer momento, pero no considera que este pueda ser constitutivo de delito: este es generalmente el caso de las infecciones por virus, los envíos de *spam,* los casos de *phishing* o *pharming,* el acceso informático ilícito por *hacking,* a pesar de que en algunos supuestos, en especial los patrimoniales, se trate de ilícitos en grado de tentativa, si aún no se ha llevado a cabo el pertinente desplazamiento patrimonial[24].

En el ámbito empresarial, además, se debe tomar en consideración la cuestión de la publicidad negativa que puede influir sobre una corporación que ve vulnerado su sistema informático[25]. Aquí debemos tener en cuenta es desprestigio que esto supone para la seguridad del sistema informático de la empresa y para la seguridad de esta en general, lo que puede derivar en una pérdida de confianza de inversores y clientes en su gestión. Como añadidura, es más que probable que estos últimos también vean la posibilidad de que sus datos personales o sociales se vuelvan accesibles a los delincuentes que han burlado los sistemas informáticos de la empresa en cuestión[26]. Todo esto deriva, como es lógico, en la no denuncia por parte de los responsables de la mercantil y la contribución así a la cifra negra de la ciberdelincuencia[27].

---

[21] Carlos María Romeo Casabona y José Antonio Martín Pallín, *Poder informático y seguridad jurídica: la función tutelar del Derecho penal ante las nuevas tecnologías de la información,* (Madrid: Editorial Fundesco, 1988), 38.

[22] Moisés Barrio Andrés, *Ciberdelitos: amenazas criminales del ciberespacio,* (Madrid: Editorial Reus, 2017), 49.

[23] Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* 296.

[24] Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* 297.

[25] José Luis de la Cuesta Arzamendi y Ana Isabel Pérez Machío, «Ciberdelincuentes y cibervíctimas», 117.

[26] Carlos María Romeo Casabona y José Antonio Martín Pallín, *Poder informático y seguridad jurídica: la función tutelar del Derecho penal ante las nuevas tecnologías de la información,* 39.

[27] Esther Morón Lerma, *Internet y Derecho penal: hacking y otras conductas ilícitas en la red,* 37.

Es muy relevante también el papel de los menores, tanto como sujetos activos de los ciberdelitos, como en el perfil de víctimas, y su contribución al fenómeno de cifra negra. Puesto que, a pesar de constituir el colectivo más victimizado y digitalizado[28], tiene un escaso impacto en la estadística de cibercriminalidad y en los tribunales de justicia. Montiel Juan[29], en su estudio criminológico en torno a esta concreta cuestión, apunta como posibles explicaciones, además de que ciertas conductas no revistan la gravedad suficiente para ser catalogadas como delito, la transversalidad de las formas de delincuencia que pueden así manifestarse en ilícitos de muy diversa naturaleza, la ausencia de pruebas impidiendo su imputación y esclarecimiento, las dificultades técnicas de registrar el componente cibernético o la propia reticencia a denunciar los hechos por parte de los menores.

Por último, existen también cibervíctimas que deciden no denunciar los hechos por la falta de confianza en el sistema judicial, dadas las dificultades de averiguación que acabamos de exponer. Esto es bastante común en el caso de los delitos patrimoniales en los que la pérdida económica no es demasiado elevada, en los cuales el sujeto pasivo opta por asumir el perjuicio económico causado por el ciberdelito, en lugar de afrontar los costes económicos y morales que acarrea un proceso judicial sin garantía de éxito[30].

Así pues, la doctrina introduce el término *invisibilidad del delito informático*[31] relativa a la sensación que produce en la opinión pública este fenómeno delictivo derivado, en suma, por las características de diversa índole que están siendo analizadas en el presente apartado: las características técnicas, lógicas y de uso de las TIC, la reinvención de las reglas de espacio y tiempo y las dificultades de investigación y persecución aparejadas a estos delitos, principalmente.

Por todo ello, De la Cuesta[32] propone centrar la discusión doctrinal en un plano victimológico, con el objetivo de acabar con la impunidad de este tipo de conductas y visibilizar los casos de delitos cibernéticos. Afirma que el camino a seguir es, a su juicio, la adopción de estrategias preventivas de incremento del riesgo y del esfuerzo a la hora de la comisión del delito y la presentación de denuncias por parte de los afectados. Lo cual contribuirá,

[28] Irene Montiel Juan, «Cibercriminalidad social juvenil: la cifra negra», *IDP: revista de Internet, derecho y política*, núm. 22 (2016), 119-131.

[29] *Ídem*.

[30] Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* 297.

[31] Luis Miguel Reyna Alfaro, «Aproximaciones criminológicas al delito informático», 100 o Myriam Herrera Moreno, «El fraude informático en el Derecho penal español», *Actualidad penal*, nº 39 (2001), 925.

[32] José Luis de la Cuesta Arzamendi y Ana Isabel Pérez Machío, «Ciberdelincuentes y cibervíctimas», 118.

como consecuencia directa, en un mayor conocimiento de estos ilícitos tanto por parte de la generalidad y potenciales víctimas, como por parte de la Administración de Justicia.

Acurio del Pino[33] apostilla que con el fin de conseguir una prevención efectiva de la criminalidad informática es necesario un análisis de las necesidades de protección y las fuentes de peligro, con el fin de que las potenciales víctimas conozcan las técnicas de manipulación y las formas de prevención y encubrimiento.

En definitiva, resulta obvio que la cuestión de la cifra negra está haciendo un flaco favor a una futura reducción de la tasa de ciberdelincuencia a nivel global y que la política-criminal de los estados debe centrar sus esfuerzos en la visibilidad del problema y de los riesgos que el ciberespacio alberga para sus usuarios, en la minimización de los riesgos para las víctimas (con especial hincapié en el ámbito empresarial) y en la formación en materia de ciberseguridad para los ciudadanos como mejor herramienta de prevención ante este tipo de delitos en constante aumento.

3. *La contribución de la víctima en el ciberdelito*

Un tercer punto que subrayar, esta vez desde el plano victimológico[34], es la contribución de la víctima a la comisión de ciertos delitos, partiendo de la base de que el sujeto pasivo no suele ser un elemento neutro en los casos de ciberdelitos.

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[35]. 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[36].

---

[33] Santiago Martín Acurio del Pino, «La delincuencia informática transnacional y la UDIMP», *AR: Revista de Derecho informático*, nº 95 (2006), 17.

[34] En Fernando Miró Llinares, «La victimización por cibercriminalidad social: un estudio a partir de las teorías de las actividades cotidianas en el ciberespacio», *Revista española de investigación criminológica REIC*, núm. 11 (2013) se lleva a cabo un estudio estrictamente criminológico, que escapa del objeto de estudio del presente trabajo, que busca medir los niveles de cibervictimización social y, además, plantear estrategias de prevención en este sentido.

[35] Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* 191.

[36] Fernando Miró Llinares, «La oportunidad criminal en el ciberespacio», *Revista electrónica de ciencia penal y criminología*, nº 13 (2011), 47.

Miró Llinares[37] 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 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).

Además, sobre la teoría delimitación de los riegos a los que se expone la víctima de un ciberdelito, por las particularidades de los entornos virtuales, es relevante que el usuario se enfrenta a menudo a dificultades para controlar la información, para limitar su permanencia en el tiempo y la huella de su actividad digital y para controlar la proyección expansiva al abrirse a un grupo de ofensores más amplio y diverso, en comparación con el espacio delictivo tradicional[38].

Asimismo, podemos exponer dos factores que ayudan a comprender mejor la posición de la víctima en el cibercrimen.

El primero de ellos es el efecto desinhibidor u *online disinhibition effect*[39] que se analiza el comportamiento de las víctimas en la red y se traduce en que existen usuarios habituales de Internet que dicen y hacen cosas en el ciberespacio que no dirían ni harían en el espacio físico tradicional. En el sentido en el cual estos usuarios son más directos, menos constreñidos y se expresan de una forma mucho más abierta en sus relaciones virtuales. Esto puede resultar en oportunidades delictivas para los ciberdelincuentes, puesto que los usuarios de Internet que actúan bajo el efecto desinhibidor son más proclives a revelar información personal en Internet, a mantener relaciones más íntimas

[37] Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* 191-193.

[38] José Ramón Agustina Sanllehí, «Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización», *Cuadernos de Política Criminal*, núm. 114 (2014): 156-157.

[39] Concepto introducido en John Suler, «The online disinhibition effect», *Cyberpsychology and Behavior*, vol. 7, núm. 3 (2004), el cual enumera los siguientes elementos y oportunidades del ciberespacio para explicar el fenómeno: anonimidad disociativa, invisibilidad, asincronicidad, introyección solipsística o que la persona imagine datos sobre la persona con la que interactúa en la red, imaginación disociativa y minimización del status y autoridad.

que las que tienen en el espacio tradicional o a ser parte de enfrentamientos *online*[40].

El segundo factor, mucho más obvio, es la ingenuidad y la irreflexión que preside en ocasiones nuestra actividad en la red y que deja vía libre a quien desee cometer un delito en el ciberespacio[41]. Esta característica es bastante común, sobre todo, en el segmento de edad de los más jóvenes quienes, movidos por la necesidad social de compartir contenido de forma constante y maravillados por la inmediatez que les proporciona Internet, ni tan siquiera reflexionan antes de subir y descargar información de la red, en forma de sonido, texto o imagen.

4. *La relatividad temporal de los ciberdelitos*

Es muy relevante mencionar también que la contracción de las distancias que caracteriza al ciberespacio tiene dos consecuencias sencillas y directas en la percepción temporal en este lugar de comisión de delitos. Por un lado, la importancia del factor tiempo se multiplica por el simple hecho de que el espacio no sea ya un obstáculo para las interacciones virtuales; por otro, al eliminar las distancias, el factor tiempo también se contrae en el mundo virtual[42].

Las leyes temporales que rigen nuestro sistema penal tradicional se ven, así, alteradas por el ciberespacio. Las características técnicas y lógicas que hemos analizado y las facilidades de tratamiento y procesamiento de la información ofrecen a los usuarios de Internet la posibilidad de actuar en la red de forma instantánea o por medio de programas con actuación retardada o controlada en el tiempo. Asimismo, estas comunicaciones telemáticas permiten a un potencial criminal actuar en tiempo real en espacios distantes[43].

Todo ello, multiplica la posibilidades de comisión delictiva, rompiendo con los límites que la necesidad de encontrarse en un momento determinado en un lugar concreto de la delincuencia tradicional impone y, a su vez, dificulta también la investigación, persecución y enjuiciamiento de los cibercrímenes.

Pues es latente la posibilidad que dan las redes de contar con un alto grado de separación temporal entre la comisión del hecho ilícito y la materialización

[40] José Ramón Agustina Sanllehí, «Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización», 162-164.

[41] *Ídem*, 165-167.

[42] Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* 148.

[43] Elena Davara Fernández de Marcos y Laura Davara Fernández de Marcos, *Delitos informáticos,* (Pamplona: Editorial Thomson Reuters Aranzadi, 2017), 38.

final del mismo en un posible resultado lesivo, si bien la doctrina lo ha catalogado en la figura del delito continuado. Lo cual deriva, en más de una ocasión, a la imposibilidad material de determinar de forma exacta el momento concreto de consumación del delito ya que, a pesar de que el sujeto activo haya podido llevar a cabo todos los actos que objetivamente darían lugar a la lesión o puesta en peligro de un bien jurídico en el espacio delictivo tradicional, puede que no exista aún afectación alguna en el valor protegido[44].

Una cuestión concreta en relación a la reglas temporales en el ciberespacio es la de la caducidad de los *logs*[45]. Resulta que el tamaño de los discos duros es limitado y, por ende, cuando transcurre un periodo de tiempo (variable dependiendo de la capacidad de almacenamiento de cada terminal) la información relativa al programa o sistema concreto se sobrescribe, borrando el rastro electrónico de una actuación delictiva en la red, en su caso. Es por esto por lo que la investigación en cuestiones de ciberdelincuencia tiene cierta premura, a no ser que el programa no presente actividad, ya que en ese caso el *log* dejaría de almacenar información nueva, pudiendo estar tanto en el ordenador del autor, como en el de la víctima e, incluso, en algún sistema intermediario[46].

Además del carácter instantáneo y programable de las comunicaciones en el ciberespacio, es posible que estas adquieran, si así lo desea el usuario, un carácter perenne en la red, a pesar de que el esfuerzo comunicativo solo dure un instante. Este es el caso de los virus, por medio de los cuales somos capaces de alojar una comunicación en la red que se perpetúa en el tiempo, lo que deriva a que el resto de los usuarios de Internet puedan ser infectados por nuestra interacción en cualquier momento, siempre que sea posterior al de la acción inicial. Lo que va en clara contradicción a las reglas del espacio delictivo tradicional, puesto que las acciones producen un efecto en un momento determinado y, si sus efectos son duraderos en el tiempo, sus consecuencias son mucho más controlables que las de un envío de información en el ciberespacio[47].

---

[44] Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos* (Granada: Editorial Comares, 2002), 96-97.

[45] En Manuel Viota Maestre, «Problemas relacionados con la investigación de los denominados delitos informáticos (ámbito espacial y temporal, participación criminal y otros)», *Cuadernos penales José María Lidón*, núm. 4 (2007), 243 se habla de los *logs* que se tratan de unos ficheros donde se almacenan todos los datos de un programa o sistema creado, con el fin de comprobar en todo momento la coherencia entre el funcionamiento del sistema y su diseño.

[46] Manuel Viota Maestre, «Problemas relacionados con la investigación de los denominados delitos informáticos (ámbito espacial y temporal, participación criminal y otros)», 247-248.

[47] Fernando Miró Llinares, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* 150-151.

II. LA PLURALIDAD DE VÍCTIMAS Y LA ELEVADA LESIVIDAD DE LOS CIBERDELITOS

En este segundo apartado, por ende, tratamos de desarrollar los caracteres que traen como consecuencia la existencia de una pluralidad de sujetos pasivos en los delitos cibernéticos y su consiguiente lesividad elevada.

Rovira del Canto[48] entiende que dichos fenómenos que presentan los cibercrímenes son consecuencia de la *permanencia del hecho,* la cual tiene su base en la repetición y el automatismo[49] que la red permite respecto de la conductas delictivas. Suceso que se repite cada vez que el delincuente es capaz de encontrar una laguna en el sistema informático por medio de la cual puede perpetrar un cibercrimen, dada la rígida organización que caracteriza a un equipo de procesamiento de datos. También Sieber[50], unos años antes, advertía de la *permanencia y automatismo del hecho* respecto de los ilícitos patrimoniales cometidos por fenómenos de delincuencia informática, característica trasladable a la ciberdelincuencia, al ser esta última una concreción de la primera.

Tradicionalmente, se ha relacionado la comisión de ilícitos patrimoniales por medio de sistemas informáticos con un perjuicio económico superior a los cometidos por otros medios[51], jugando un papel clave en este aspecto la interconexión de las actividades económicas y el efecto cascada que estas pueden producir, al poder extender su afectación a un número importante de entidades del sector[52]. Actualizando a las formas criminales actuales, por tanto, los delitos ciber-económicos procuran a quienes los cometen, con carácter general, elevadas ganancias[53].

En concreto, Gómez Perals[54] apunta que la rentabilidad de estos delitos es una tercera parte superior al resto, o bien por la sustracción en contadas ocasiones de grandes cantidades, o bien por la recurrente apropiación de importes

[48] Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos,* 77-79, donde se refiere a la delincuencia informática, pero es una característica aplicable a la ciberdelincuencia, al ser esta última una concreción de la primera.

[49] M. Carmen Alastuey Dobón, «Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial», 459.

[50] Ulrich Sieber, «Criminalidad informática: peligro y prevención», en *Delincuencia informática,* ed. por Santiago Mir Puig (Barcelona: Editorial PPU, 1992), 29-30.

[51] Rovira del Canto, *Delincuencia informática…,* 79.

[52] De la Cuesta Arzamendi, Pérez Machío y San Juan Guillén, «Aproximaciones criminológicas a la realidad de los ciberdelitos», 86-87.

[53] Alastuey Dobón, «Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial», 459.

[54] Miguel Gómez Perals, «Los delitos informáticos en el derecho español, en Informática y Derecho», 483-484.

más pequeños. También Álvarez Vizcaya[55] alerta sobre esta cuestión cuando afirma que el perjuicio económico que causan estos delitos difícilmente puede compararse con los perjuicios derivados de la delincuencia tradicional.

Debemos sumar a esto algo que pone de relieve Rovira del Canto[56] cuando argumenta que existe, además, otra causa que convierte a los delitos cibernéticos de contenido patrimonial en especialmente lesivos para el bien jurídico que protegen: que el objeto del delito es el llamado *dinero contable.* Dicho de otra forma, que la cantidad máxima de sustracción en un delito informático no se limita al dinero que en el momento preciso de la comisión del delito el sujeto pasivo posee o tiene en caja, sino que se extiende a todo lo disponible en un soporte informático, cantidad habitualmente superior.

Este carácter de capacidad lesiva potenciada lo mantienen, no obstante, los ilícitos cibernéticos de nueva creación que no afectan tan solo al patrimonio de las víctimas, sino que extienden su capacidad de afectación a bienes jurídicos de todas las esferas de la vida de los ciudadanos (intimidad, honor, libertad, libertad sexual, moral, seguridad del estado, etc.)[57]. Así pues, a pesar de que ya no es siempre reflejo del perjuicio económico creado por el delito, la lesividad extensa y elevada sigue siendo un elemento de estos crímenes desde un punto de vista material del concepto y se traduce tanto en un mayor desvalor de resultado en cada acción delictiva virtual, como en la posibilidad de afectación a un mayor número de usuarios de Internet.

Algo que, desafortunadamente, dificulta enormemente la detección e investigación de los cibercrímenes[58] ya que, en ocasiones, las conductas que conforman todo el proceso criminal consideradas individual y aisladamente, no son de suficiente gravedad como para constituir un hecho delictivo, lo que deriva en la imposibilidad de analizar la lesividad global del conjunto de conductas concretas, a pesar de que estas causen una extensa afectación y un elevado resultado perjudicial total[59].

Ahora bien, es cierto que este dato no constituye una novedad atribuible de forma exclusiva y originaria a Internet, ni siquiera a los sistemas informáticos, sino que este efecto de superior capacidad lesiva ha sido tratado y resuelto ya doctrinalmente en otros ámbitos de carácter tradicional[60].

---

[55] Maite Álvarez Vizcaya, «Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red», *Cuadernos de Derecho judicial*, nº 10 (2001): 264-265.

[56] Rovira del Canto, *Delincuencia informática…,* 81.

[57] De la Cuesta Arzamendi, Pérez Machío y San Juan Guillén, «Aproximaciones criminológicas a la realidad de los ciberdelitos», 87.

[58] Ídem, 88.

[59] Rovira del Canto, *Delincuencia informática…,* 81.

[60] Juan José González Rus, «Precisiones conceptuales y político-criminales sobre la intervención penal en Internet», *Cuadernos penales José María Lidón*, nº 4 (2007): 33.

Un ejemplo de este fenómeno lo constituyen los atentados al honor perpetrados vía medios de comunicación, como la televisión, los periódicos, la radio, las publicaciones periódicas o revistas. Los cuales ya aportan el efecto multiplicador que la red y los sistemas informáticos pueden añadir a ciertos delitos de injurias, calumnias, entre otros. No es desdeñable, sin embargo, el hecho de que la red no solo facilita la difusión, sino que también abarata considerablemente los costes y favorece la comunicación y el intercambio instantáneo de información con personas afines, a diferencia de los medios de comunicación tradicionales[61].

En otro plano, los delitos tradicionales contra los consumidores presentan una fundamentación paralela, por ejemplo, a los delitos de daños informáticos llevados a cabo por medio de virus, en el sentido en el cual su característica distintiva está basada en la capacidad que presentan de afectación a un número de sujetos muy elevado.

Esto es, tanto en el caso de Internet, como en los supuestos en los que entran en juego las plataformas comunicativas tradicionales, el soporte empleado permite obtener un mayor desvalor de acción o de resultado, o la ampliación y multiplicación del peligro o de la lesión propia del delito, hasta alcanzar un número de sujetos superior al habitual y unas dimensiones de gran envergadura[62].

III. ENCAJE Y TRATAMIENTO EN NUESTRA LEGISLACIÓN PENAL ACTUAL: EL DELITO CONTINUADO Y EL DELITO MASA

El apartado que sigue trata, así, de arrojar luz sobre la cuestión de cómo trata el Código Penal español las peculiaridades de los ciberdelitos analizadas hasta el momento.

Lo cierto es que dichas características del cibercrimen nos llevan irremediablemente a la construcción dogmática prevista en el art. 74 CP de delito continuado, ya que el sujeto activo afecta a una pluralidad de personas «en ejecución de un plan preconcebido o aprovechando idéntica ocasión», tal y como describe el propio precepto. Tanto que, en ocasiones, una sola ocasión es suficiente para afectar a varios sujetos pasivos, infringiendo el mismo tipo penal[63].

[61] Carlos María Romeo Casabona, «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», 4.

[62] Juan José González Rus, «Precisiones conceptuales y político-criminales sobre la intervención penal en Internet», 33.

[63] De la Cuesta Arzamendi, Pérez Machío y San Juan Guillén, «Aproximaciones criminológicas a la realidad de los ciberdelitos», 85.

Según Romeo Casabona, además, 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, puesto que, en su ejecución, el sujeto es plenamente consciente y quiere aprovecharse del recurso al procedimiento repetitivo[64].

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 *click,* consistente en el envío de cientos de mensajes con idéntico contenido, logra estafar electrónicamente (art. 248. 2 a) del CP) a una pluralidad de víctimas en el momento en el cual se lleva a cabo el acto de disposición patrimonial en su beneficio.

No obstante, no deben pasarse por alto las conductas que no afectan al patrimonio y presentan, de igual manera, el carácter de continuidad delictual, puesto que estas centran su afectación en bienes jurídicos personalísimos, como la integridad moral, el honor o la libertad, lo que las lleva a estar excluidas de la aplicación de la norma del delito continuado en virtud de lo expuesto en el art. 74. 3 CP[65] (cuando afectan a distintos sujetos).

La cuestión controvertida aquí, sin embargo, se trata de si la respuesta penal que el legislador ofrece a las figuras de delito continuado y, sobre todo, de delito masa (pena superior en uno o dos grados) es suficiente a la vista de la enorme capacidad lesiva de estas conductas que llevan a cabo los ciberdelincuentes, con un desvalor de resultado descomunal[66], en comparación con lo que requiere la comisión de un delito continuado en el espacio delictivo tradicional. Y, no solo eso, sino si el carácter de anonimato, riesgo reducido y dificultad de persecución que los ciberdelitos ofrecen deben ser tenidos de alguna manera en cuenta en estos supuestos, a la hora de determinar la respuesta penal.

[64] Romeo Casabona, «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», 27.

[65] De la Cuesta Arzamendi, Pérez Machío y San Juan Guillén, «Aproximaciones criminológicas a la realidad de los ciberdelitos», 85-86.

[66] Romeo Casabona, «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», 27.

González Rus[67] no considera, por ende que, desde un punto de vista de técnica penal, la superior capacidad lesiva de los ciberdelitos constituya una novedad de suficiente relevancia como para justificar la creación de bienes jurídicos nuevos o de específicas figuras delictivas. Ahora bien, aboga por la justificación e inclusión de tipos agravados en la redacción de los delitos afectados, en la medida en la que la elevada capacidad lesiva que aporte la comisión delictual por medio de la red configure la conducta como merecedora de respuesta penal de mayor gravedad. Dependiendo del valor de lo defraudado, la entidad del perjuicio o el número de sujetos pasivos, por ejemplo.

En idéntico sentido se pronuncia Rovira del Canto[68] cuando apunta que en los ciberdelitos la cuantía del perjuicio económico, potenciada por la extensa lesividad, no debe afectar a la consumación del delito ni a la existencia del delito en sí, sino que solución legal adecuada es tenerlo únicamente en cuenta para la formulación de tipos agravados y cualificados y para la depuración de la responsabilidad civil correspondiente.

IV. CONCLUSIONES: REFLEXIONES DOGMÁTICAS Y DE POLÍTICA LEGISLATIVA

Así las cosas, son cuatro los principales aspectos distintivos de un posible delito continuado o masa en el ciberespacio respecto a esta figura en el caso de que sea cometida en el espacio delictivo tradicional: la elevada lesividad que presenta, la capacidad de afectación a una pluralidad de víctimas, la facilidad con la que el ciberdelincuente consigue llevar a cabo esta pluralidad de acciones y el carácter anónimo y distanciado de los ilícitos virtuales que derivan en el fácil encubrimiento del delito y la consiguiente dificultad de persecución de este.

Sobre la primera cuestión, en un plano general y a sabiendas de que se trata de un punto digno de largo análisis, es necesario plantearse si son suficientes las penas previstas para algunos de los delitos tradicionales que pueden también cometerse por Internet.

No existen dudas, en los casos en los cuales manipulación está prevista ya en el tipo, como es el caso de la estafa informática del artículo 248. 2 a) del CP o los delitos de daños informáticos.

No es tan claro, por ejemplo, en el caso de un delito de calumnias cabe preguntarse si es proporcional una pena de 6 meses a dos años de prisión por calumniar con publicidad, si tenemos en cuenta que dicha publicidad se definió en su momento como propagar «por medio de la imprenta, la

[67] Juan José González Rus, «Precisiones conceptuales y político-criminales sobre la intervención penal en Internet», 33.

[68] Rovira del Canto, *Delincuencia informática…,* 82.

radiodifusión o por cualquier otro medio de eficacia semejante». La cuestión reside en si Internet en un medio de eficacia semejante hoy en día o su eficacia es brutalmente mayor.

Así pues, se presentan las posibilidades de confiar en que el marco penal propuesto en estos casos es suficientemente amplio para dar respuesta a estos casos de elevada lesividad, escogiendo el juzgador una pena cercana al límite penal máximo o la opción de incluir apartados específicos previendo modalidades agravadas de comisión por medios cibernéticos.

En relación con la afectación a varias víctimas, la legislación penal actual da una respuesta completa y proporcional a los distintos niveles que el ciberdelito que afecte al patrimonio (delito masa) pueda alcanzar vía el artículo 74. 2 CP, puesto que, en estos casos, el precepto prevé que el juzgador tenga en cuenta el perjuicio total causado a la hora de la imposición de la pena, permitiendo agravar el castigo hasta dos grados, sean uno o varios los sujetos afectados.

No obstante, como hemos avanzado, la ciberdelincuencia no afecta hoy en día tan solo al patrimonio de los usuarios de la red, sino que lo económico constituye tan solo una pequeña parte de todos los intereses y valores que cada día están en juego en el mundo *online.* Así pues, resulta aún una incógnita la adecuación de lo que expone el 74. 3 CP a los ilícitos cibernéticos actuales, ya que la excepción sobre los delitos que afectan al honor y la indemnidad sexual no sería aplicable aquí al tener que darse sobre el mismo sujeto pasivo. Por tanto, el juez deberá atenerse a «la naturaleza del hecho y del precepto infringido» para dilucidar el castigo penal adecuado en los casos de pluralidad de víctimas.

Por último, sobre las dos últimas cuestiones relativas a la facilidad de afectación a varias víctimas y el sencillo encubrimiento del hecho, es posible plantearse que sean tenidas en cuenta por medio de las circunstancias agravantes previstas en los artículos 22. 1 y 22. 2 del CP, relativas a la alevosía y el aprovechamiento del lugar para facilitar la impunidad del delincuente que, en este caso, sería Internet.

FUENTES BIBLIOGRÁFICAS

a. Libros

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

Davara Fernández de Marcos, Elena y Davara Fernández de Marcos, Laura, *Delitos informáticos,* (Pamplona: Editorial Thomson Reuters Aranzadi, 2017).

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

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

Romeo Casabona, Carlos María y Martín Pallín, José Antonio, *Poder informático y seguridad jurídica: la función tutelar del Derecho penal ante las nuevas tecnologías de la información,* (Madrid: Editorial Fundesco, 1988).

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

b. Capítulos de libro

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

De la Cuesta Arzamendi, José Luis y Pérez Machío, Ana Isabel, «Ciberdelincuentes y cibervíctimas», *Derecho penal informático*, ed. por De la Cuesta Arzamendi, José Luis (Pamplona, Editorial Civitas - Thomson Reuters, 2010).

Romeo Casabona, Carlos María, «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* ed. por Romeo Casabona, Carlos María (Granada, Editorial Comares, 2006).

Sieber, Ulrich, «Criminalidad informática: peligro y prevención», *Delincuencia informática,* ed. por Mir Puig, Santiago (Barcelona, Editorial PPU, 1992).

Sieber, Ulrich, «Las medidas de seguridad de los usuarios de ordenadores», *Delincuencia informática,* ed. por Mir Puig, Santiago (Barcelona, Editorial PPU, 1992).

c. Artículos de revista

Acurio del Pino, Santiago Martín, «La delincuencia informática transnacional y la UDIMP», *AR: Revista de Derecho informático*, nº 95 (2006).

Agustina Sanllehí, José Ramón, «Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización», *Cuadernos de Política Criminal*, núm. 114 (2014).

Alastuey Dobón, M. Carmen, «Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial», *Informática y Derecho: revista iberoamericana de Derecho informático*, nº 4 (1994).

Álvarez Vizcaya, Maite, «Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red», *Cuadernos de Derecho judicial*, nº 10 (2001).

Asencio Guillén, Antonio, «El ciberespacio como sistema y entorno social: una propuesta teórica a partir de Niklas Luhmann», *Comunicación y Sociedad*, vol. 31, núm. 1 (2018).

Gómez Perals, Miguel, «Los delitos informáticos en el derecho español», *Informática y Derecho*, nº 4 (1994).

González Rus, Juan José, «Precisiones conceptuales y político-criminales sobre la intervención penal en Internet», *Cuadernos penales José María Lidón*, nº 4 (2007).

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

Herrera Moreno, Myriam, «El fraude informático en el Derecho penal español», *Actualidad penal*, nº 39 (2001).

Lessig, Lawrence, «Las leyes del ciberespacio», *THEMIS: revista de Derecho*, núm. 1 (2002).

Miró Llinares, Fernando, «La oportunidad criminal en el ciberespacio», *Revista electrónica de ciencia penal y criminología*, nº 13 (2011).

Miró Llinares, Fernando, «La victimización por cibercriminalidad social: un estudio a partir de las teorías de las actividades cotidianas en el ciberespacio», *Revista española de investigación criminológica REIC*, núm. 11 (2013).

Montiel Juan, Irene, «Cibercriminalidad social juvenil: la cifra negra», *IDP: revista de Internet, derecho y política*, núm. 22 (2016).

Reyna Alfaro, Luis Miguel, «Aproximaciones criminológicas al delito informático», *Capítulo Criminológico*, vol. 31, nº 4 (2003).

Suler, John, «The online disinhibition effect», *Cyberpsychology and Behavior*, vol. 7, núm. 3 (2004).

Valiente García, Francisco Javier, «Comunidades virtuales en el ciberespacio», *Doxa comunicación: revista interdisciplinar de estudios de comunicación y ciencias sociales*, núm. 2 (2004).

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

LA PLURALIDAD DE VÍCTIMAS DERIVADA DE LA ELEVADA LESIVIDAD EN LOS CIBERDELITOS: UNA RESPUESTA PENAL PROPORCIONAL

Victim multiplicity derived from harm in cybercrime: A proportional criminal response

Jon López Gorostidi
Investigador predoctoral
Profesor de Derecho penal
Universidad de Deusto
jlgorostidi@deusto.es

http://dx.doi.org/10.18543/ed-68(1)-2020pp201-221