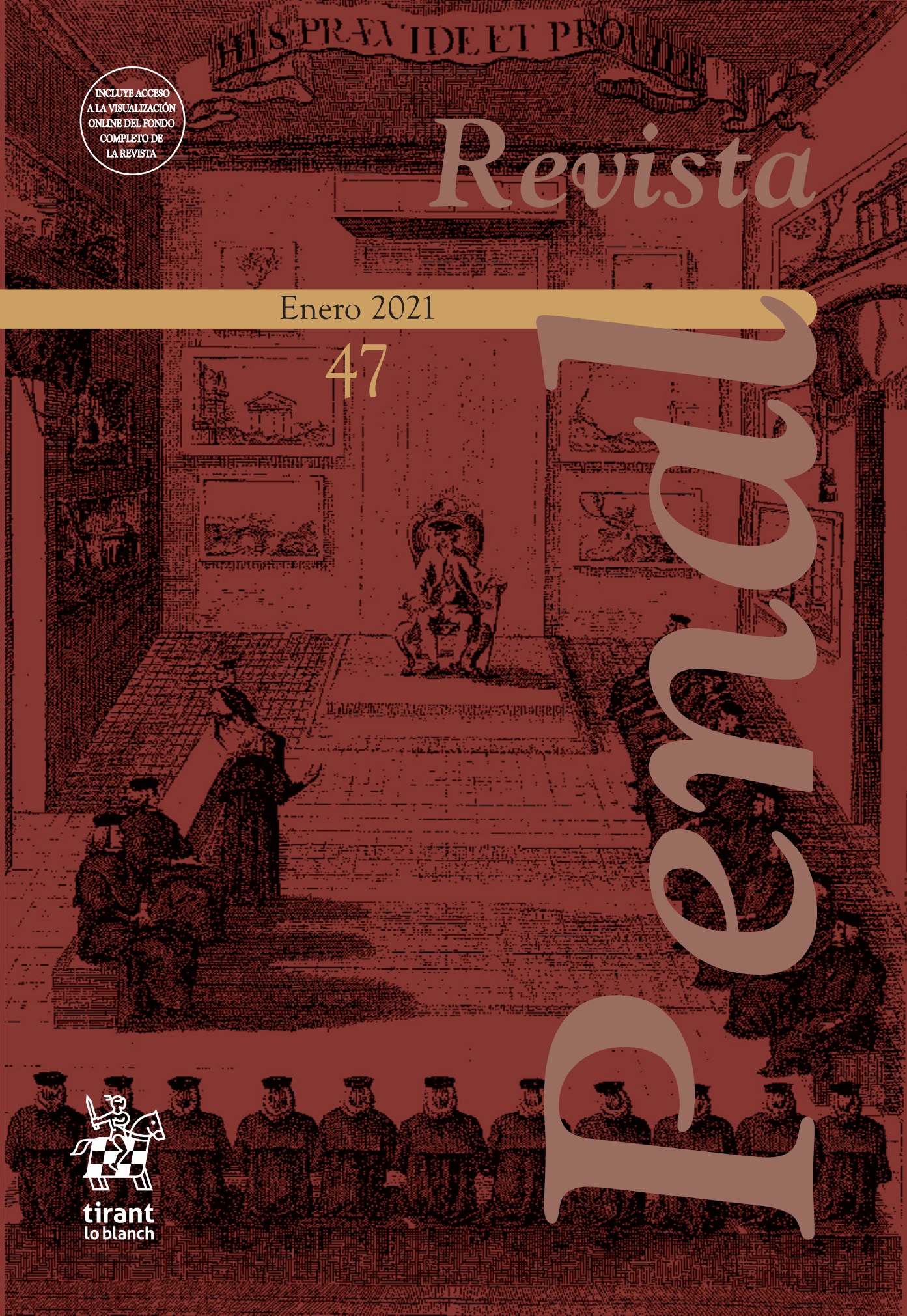
47

INCLUYE ACCESO A LA VISUALIZACIÓN ONLINE DEL FONDO COMPLETO DE LA REVISTA

Revista Penal

Enero 2021

47



tirant lo blanch

Revista Penal

47

Enero 2021

tirant lo blanch

Revista Penal

Número 47

Sumario

Doctrina:

* *Los primeros 25 números de la Revista Penal están recogidos en el repositorio institucional científico de la Universidad de Huelva Arias Montano:* http://rabida.uhu.es/dspace/handle/10272/11778

tirant lo blanch

Publicación semestral editada en colaboración con las Universidades de Huelva, Salamanca, Castilla-La Mancha, y Pablo Olavide de Sevilla

www.revistapenal.com

EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email:tlb@tirant.com
http://www.tirant.com
Librería virtual: http://www.tirant.es
DEPÓSITO LEGAL: B-28940-1997
ISSN.: 1138-9168
MAQUETA: Tink Factoría de Color

Los valores tradicionales como bienes jurídicos protegidos también en el ciberespacio: a propósito del confinamiento provocado por la crisis sanitaria del COVID-19

Jon López Gorostidi

Revista Penal, n.º 47. - Enero 2021

Ficha técnica

Autor: Jon López Gorostidi
Adscripción institucional: Universidad de Deusto (San Sebastián)
Title: Traditional values as legally protected goods also in cyberspace: about the confinement caused by the COVID-19 health crisis

Resumen: A falta de estudios criminológicos, informes de instituciones especializadas y el sector periodístico afirman que el confinamiento al que ha sido sometido la población mundial por la crisis del COVID-19, lejos de eliminar toda actividad criminal, ha resultado en un desplazamiento de la oportunidad delictiva a internet y ha llevado a los ciudadanos a introducir en el ciberespacio cada vez más valores básicos para su desarrollo personal y en sociedad. Dado este fenómeno, el presente trabajo lleva a cabo un análisis de los ciberdelitos más comunes y relevantes durante el confinamiento y se defiende que son los valores tradicionalmente protegidos por el derecho penal los bienes jurídicos protegidos por estos ilícitos, en contra de las voces que abogan por la protección de valores novedosos como los datos, la información o los sistemas de información.
Palabras clave: Ciberdelincuencia, ciberdelitos, bien jurídico, confinamiento, COVID-19.

Abstract: In the absence of criminological studies, reports from specialized institutions and the journalistic sector state that the confinement to which the world population has been subjected by the COVID-19 crisis, far from eliminating all criminal activity, has resulted in a shift of criminal opportunity to the Internet and has led citizens to introduce into cyberspace more and more basic values for their personal and social development. Given this phenomenon, this paper carries out an analysis of the most common and relevant cybercrimes during confinement and defends that the values traditionally protected by criminal law are the legally protected goods by these crimes, against the voices that advocate the protection of novel values such as data, information or information systems.
Key words: Cybercrime, cybercrimes, legally protected good, confinement, COVID-19.

Rec.: 15/11/2020 **Fav.:** 29/11/2020

1. Introducción: el confinamiento global derivado de la crisis sanitaria del COVID-19 como elemento de fomento de la actividad en la red y el consiguiente desplazamiento de los delitos al ciberespacio

La crisis sanitaria derivada del COVID-19 se ha visto traducida en medidas de confinamiento de la población a nivel mundial y, en consecuencia, la ciudadanía ha desplazado una buena parte de su actividad cotidiana a Internet. Ahora bien, este fenómeno se ha desarrollado en mayor o menor medida, dependiendo del territorio al que hacemos referencia y en función de la rigidez de las medidas de confinamiento adoptadas en cada estado.

Todos hemos sido testigos del aumento de las compras *online*[1], puesto que parte de las medidas acordadas para la lucha contra el virus se han centrado en la reducción de la vida en sociedad y en el cierre de los establecimientos que no comercializan bienes de primera necesidad, como los supermercados o las farmacias.

Del mismo modo, las comunicaciones por medio de la red han aumentado considerablemente, dado que el contacto entre individuos que no pertenecen a la misma unidad familiar se ha visto también reducido al mínimo. El uso de las redes sociales[2] y las plataformas de videollamada[3] han visto aumentada su popularidad y su frecuencia de uso de forma insospechada hasta la irrupción de la crisis sanitaria.

En tercer lugar, es latente también el incremento de usuarios experimentado por los espacios web que ofrecen contenidos digitales. El principal exponente son las plataformas de visionado de películas y series por suscripción[4], pero no debemos desdeñar el aumento de consultas en los buscadores de Internet en busca de contenido o información relativa a recetas de cocina, manualidades, ejercicios y deporte en el hogar u otro tipo de actividad que permita ocupar el tiempo que los ciudadanos deben pasar en sus casas.

Por último, introducimos el fenómeno del teletrabajo, que ha constituido la opción predilecta para las empresas y autónomos en la medida de lo posible y siempre que no se tratara de una actividad esencial con necesidad de desarrollo fuera del hogar[5]. Como consecuencia, se ha disparado el uso que los trabajadores hacen de su correo electrónico y de las plataformas de videoconferencia, entre otros.

Sin embargo, estos cambios en los usos habituales del ciberespacio que han llevado a cabo los ciudadanos durante la duración de las medidas de confinamiento de la pandemia no se han producido en el escenario habitual, sino que existen más factores ambientales que convierten el desplazamiento de ciertas actividades del día a día de los individuos a la red en algo particular. El informe de la EUROPOL de marzo de 2020 sobre la afectación de la crisis del COVID-19 en la ciberdelincuencia[6] nos ilustra sobre este extremo.

Para empezar, se ha producido un aumento de la demanda de ciertos productos como, por ejemplo, equipamiento médico de protección y productos farmacéuticos, en lo que a los profesionales de salud se refiere, y geles desinfectantes o mascarillas higiénicas, si versamos sobre la ciudadanía en general. Este hecho conlleva que la compra de bienes por Internet no se lleve a cabo en las condiciones habituales de mercado, sino que exista una demanda superior a la normal sobre unos productos concretos. Si unimos a esto las limitaciones en la producción y el envío de bienes derivado de las estrictas medidas de lucha contra la crisis sanitaria, encontramos un mercado con una demanda superior sobre ciertos productos muy específicos y una oferta que, si ya encuentra dificultades para mantenerse en los niveles anteriores al virus, debe aumentar en la medida de lo posible para dar una respuesta completa a los consumidores[7].

Además, se ha desarrollado un sentimiento de inseguridad y ansiedad entre los ciudadanos, en relación

1 La razón, *El COVID-19 dispara las compras online en España y aumenta el pesimismo económico*, https://www.larazon.es/economia/20200330/topd6w7vjjddjkjzaccdc6wyjm.html (última consulta: 14 de mayo de 2020), 30 de marzo de 2020.

2 ABC, *El uso de redes sociales en España aumenta un 55% en la pandemia del coronavirus,* https://www.abc.es/tecnologia/redes/abci-redes-sociales-espana-aumenta-55-por-ciento-pandemia-coronavirus-202003241257_noticia.html?ref=https%3A%2F%2Fwww.google.com%2F (última consulta: 14 de mayo de 2020), 2 de abril de 2020.

3 Europa press, *Las videollamadas, los mensajes de voz y el consumo de noticias en directo crecen con las medidas de distancia social,* https://www.europapress.es/portaltic/internet/noticia-videollamadas-mensajes-voz-consumo-noticias-directo-crecen-medidas-distancia-social-20200407121838.html (última consulta: 14 de mayo de 2020), 7 de abril de 2020.

4 Expansión, *COVID-19: el confinamiento acelera la adopción de servicios como Netflix,* https://www.expansion.com/economiadigital/companias/2020/03/29/5e7b8fd8468aeb29108b45e9.html (última consulta: 14 de mayo de 2020), 29 de marzo de 2020.

5 Diario sur, *El teletrabajo se dispara para mantener el pulso de la actividad,* https://www.diariosur.es/andalucia/teletrabajo-dispara-mantener-20200403184055nt.html?ref=https:%2F%2Fwww.google.com%2F (última consulta: 14 de mayo de 2020), 3 de abril de 2020.

6 Europol, *Informe Pandemic profiteering: how criminals exploit the COVID-19 crisis,* marzo de 2020, https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic (última consulta: 14 de mayo de 2020), 27 de marzo de 2020, p. 3.

7 El Confidencial, *La crisis del COVID-19 que nadie previó: el "e-commerce" colapsa al enviar sus pedidos,* https://www.elconfidencial.com/tecnologia/2020-03-30/coronavirus-ecommerce-pedidos-stock-covid19_2521043/(última consulta: 14 de mayo de 2020), 30 de marzo de 2020.

con varias esferas de las que acabamos de introducir en el inicio de este apartado. Los medios de comunicación se han hecho eco de la aparentemente excesiva demanda de bienes de primera necesidad que ha derivado en aglomeraciones en los supermercados durante las primeras semanas de confinamiento[8], de la dificultad de compaginar vida familiar y obligaciones laborales en el mismo espacio y al mismo tiempo y la necesidad de los individuos de mantenerse en constante interacción con sus pares por medio de, en su mayoría, las redes sociales, que han visto su uso también disparado gracias a la crisis del COVID-19.

En definitiva, el confinamiento ha derivado en que los ciudadanos hayamos trasladado la mayoría de los aspectos más esenciales de nuestro día a día a la red por nuestra necesidad de conexión ininterrumpida, bien sea hacia nuestros seres queridos y amigos, respecto del mercado y los bienes de los que este nos provee, en relación con el entretenimiento que nos proporcionan las plataformas digitales o por obligaciones laborales.

Como consecuencia, la aproximaciones criminológicas llevadas a cabo hasta el momento, a la espera de la publicación de artículos científicos sobre el fenómeno indican que, a pesar de que los primeros estudios apuntaban a una reducción de la delincuencia durante el confinamiento de la población[9], se ha producido un desplazamiento de los delitos al ciberespacio[10]. Esto es así por dos razones principales: la primera, el hecho de que, como acabamos de relatar, los usos diarios de los ciudadanos han sido igualmente desplazados a Internet y es donde, en consecuencia, se encuentra la oportunidad delictiva; la segunda, se trata de que los potenciales cibercriminales pasan también, en época de confinamiento, más tiempo en el ciberespacio, lo que fomenta las opciones de que tomen una decisión delictiva.

Así las cosas, a falta de estadísticas oficiales por el momento, los medios de comunicación y diferentes contenidos publicados en Internet se han hecho eco de los ciberdelitos más comunes.

En primer lugar, el fraude o la estafa informática ha sido sin duda una de las infracciones más cometidas en el ciberespacio en las últimas semanas, siendo las víctimas de estos ilícitos tanto particulares como empresas y administraciones públicas[11].

Uno de los *modus operandi* más comunes lo está constituyendo la venta de bienes de primera necesidad en esta pandemia, como mascarillas higiénicas, geles desinfectantes o material de protección para los profesionales del ámbito sanitario, por medio de Internet que, tras efectuar el pago por medios telemáticos, nunca se completa con la recepción de lo acordado. Como la venta por valor de 6,6 millones de euros entre dos compañías en Singapur de geles desinfectantes y mascarillas FFP2 y FFP3[12] que nunca llegaron a ser

8 Voz Libre, *Colapso en supermercados, escasez y colas interminables ante el cierre escolar por el Coronavirus,* https://vozlibre.com/nacional/colapso-supermercados-escasez-colas-interminables-ante-cierre-escolar-coronavirus-27849/(última consulta: 14 de mayo de 2020), 10 de marzo de 2020.

9 Ara, *El COVID-19 desploma els delictes presencials,* https://www.ara.cat/societat/coronavirus-covid-19-delictes-presencials_0_2425557497.html?utm_medium=social&utm_source=twitter&utm_campaign=ara (última consulta: 14 de mayo de 2020), 29 de marzo de 2020, Deia, *El confinamiento por el Coronavirus reduce los delitos en Bilbao casi un 90%,* https://www.deia.eus/actualidad/sociedad/2020/04/07/confinamiento-reduce-delitos-bilbao-90/1030007.html (última consulta: 14 de mayo de 2020), 7 de abril de 2020 o Heraldo, *La Guardia Civil destaca que los delitos bajan a la mitad, pero alerta sobre el cibercrimen,* https://www.heraldo.es/noticias/nacional/2020/03/20/coronavirus-pandemia-guardia-civil-destaca-que-delitos-bajan-a-mitad-pero-alerta-sobre-cibercrimen-1365010.html (última consulta: 14 de mayo de 2020), 20 de marzo de 2020, entre muchos otros.

10 En BUIL-GIL, David, LORD, Nicholas, BARRETT, Emma, DRESNER, Daniel y HIGGINS, Brian, "Profiting from pandemics: COVID-19, changing routines and cyber crimes", en Blog Digital Futures, Universidad de Manchester, http://blog.policy.manchester.ac.uk/digital-futures/2020/03/profiting-from-pandemics-covid-19-changing-routines-and-cyber-crimes/(última consulta: 14 de mayo de 2020), 19 de marzo de 2020 se expone cómo el fenómeno causado por el COVID-19 no se trata tanto de una reducción de la delincuencia en general, sino que esa delincuencia se desplaza al ciberespacio. En concreto, en el artículo de estos autores se relata cómo el teletrabajo afecta a este punto e invita a los ciudadanos y a las empresas a adoptar medidas preventivas en este sentido. Como ejemplos de los delitos que podrían cometerse en el ciberespacio nombras los fraudes o estafas en las compras por Internet, en las que el usuario puede pagar por un producto como una mascarillas o gel desinfectante y nunca recibirlo, o las conductas de *phishing,* donde los cibercriminales se valen de suplantaciones de identidad (por medio de la simulación de una comprobación rutinaria de claves bancarias, por ejemplo) para obtener información idónea para crear un perjuicio en el patrimonio de la víctima. En la misma línea: Públic, *La delinqüència canvia d'escenari i es desplaça durant l'epidèmia,* https://www.publico.es/public/delinqueencia-canvia-d-escenari-i-desplaca-durant-l-epidemia.html (última consulta: 14 de mayo de 2020), 15 de abril de 2020 o CAMPOY TORRENTE, Pedro, "¿Flu-ctuaciones delictivas? Los posibles efectos del COVID-19 en la criminalidad", en Blog de la REIC: revista española de investigación criminológica, SEIC: sociedad española de investigación criminológica, https://criminologia.net/2020/03/23/flu-ctuaciones-delictivas-los-posibles-efectos-del-covid-19-en-la-criminalidad/ (última consulta: 14 de mayo de 2020), 23 de marzo de 2020.

11 Europol, *Informe Pandemic profiteering: how criminals exploit the COVID-19 crisis… op. cit.,* p. 6.

12 Esta clase de mascarillas higiénicas son aptas para formar parte de un Equipo de Protección Individual (EPI) en los términos concretados en: Unión Europea, *Reglamento 2016/425/UE del Parlamento Europeo y del Consejo, relativo a los equipos de protección individual*, de 9 de marzo de 2016, DOUE núm. 81, de 31 de marzo de 2016, pp. 51-98.

enviadas[13], los casos registrados en España en los que se pagaron hasta 600 € por una caja de mascarillas que nunca llegó a su destinatario o las donaciones a falsos fondos destinados a la lucha contra el virus[14].

También son numerosos los casos en los que el producto adquirido por la víctima del ciberdelito sí llega a sus manos, pero se trata de un producto falsificado o que no cumple con las especificidades acordadas[15]. Conducta que se ve agravada por el hecho de que los productos comprados por Internet se traten de equipamiento de protección contra el virus (como mascarillas, guantes, productos de limpieza o artículos farmacéuticos) y test de infección, dado el riesgo para la salud que su uso conlleva.

Del mismo modo, son habituales los casos de *phishing* en los que se lleva a cabo una suplantación de identidad, generalmente por medio del envío de un correo electrónico masivo con apariencia de ser una entidad que genere confianza en la víctima para, más tarde, solicitar datos personales o bancarios que llevan a la obtención de un beneficio patrimonial a los ciberciminales. Uno de los casos más sonados en la últimas semanas ha sido el de los correos electrónicos que han recibido millones de usuarios desde, en apariencia, la Organización Mundial de la Salud (OMS, en adelante) con los que un grupo de ciberdelincuentes buscaba hacerse con los datos bancarios de usuarios de Internet que quisieran hacer donaciones para la lucha contra el virus o, simplemente, querían consultar información sanitaria relacionada con el COVID-19. Algo que llevó a la propia OMS a alertar a la población de los mensajes, indicando que nunca exigen un usuario y contraseña para acceder a sus recomendaciones, que nunca envían archivos adjuntos que no han sido previamente solicitados por los destinatarios, que nunca te invitan a visitar páginas web fuera de su dominio, que nunca piden dinero para acceder a sus servicios y que nunca llevan a cabo sorteos o concursos para financiación por medio del correo electrónico[16].

En segundo término, también hemos sido testigos de casos de ciberataques, sin afectación directa a particulares, sino que han sido capaces de acceder a sistemas informáticos de personas jurídicas, incurriendo en las conductas delictivas de intrusismo informático o interrupción de servicio, según el caso.

En concreto, el caso más sonado lo ha constituido el ataque sufrido por el Hospital Universitario de Brno, en la República Checa el pasado 12 de marzo[17]. Como consecuencia, tuvieron que posponer diversas intervenciones médicas y trasladar a pacientes a hospitales cercanos, dado que se vieron obligados a dejar sin funcionamiento durante horas a su sistema informático, hasta que la situación pudo volver a la normalidad.

Tampoco podemos olvidarnos de la proliferación de los delitos contra la libertad sexual durante el confinamiento derivado de la crisis sanitaria, entre otras razones, porque nuestros menores pasan más tiempo delante de sus pantallas de ordenador, lo que los lleva a estar más expuestos a estas amenazas.

De hecho, la National Crime Agency (NCA) de Reino Unido ha alertado a la población de este peligro[18] afirmando que existen 300.000 personas en todo su territorio que pueden constituir una amenaza real para la indemnidad sexual de los menores por su actividad en la red. Asimismo, anima a las familias y a los profesores de los alumnos de edades tempranas a implementar medidas de prevención y a establecer controles sobre el uso que los menores hacen de Internet.

Por último, no podemos dejar sin mencionar el fenómeno de aumento de la violencia intrafamiliar que deri-

13 Europol, *Informe Pandemic profiteering: how criminals exploit the COVID-19 crisis… op. cit.,* p. 7.

14 20 Minutos, *Compras por teléfono, pruebas gratis del COVID-19… Las estafas perpetradas aprovechando la crisis del Coronavirus,* https://www.20minutos.es/noticia/4206878/0/enganos-estafas-perpetradas-crisis-coronavirus/(última consulta: 14 de mayo de 2020), 27 de marzo de 2020.

15 Europol, *Informe Pandemic profiteering: how criminals exploit the COVID-19 crisis… op. cit.,* pp. 8-9. En este informe se relata como la Operación Pangea dedicada a la interceptación de productos para la prevención y tratamiento del COVID-19 falsificados o de calidad inferior a la permitida está presente en 90 países y ha interceptado ya 34.000 mascarillas quirúrgicas preparadas para su venta en la red, a través de más de 2.000 links. Entre el 3 y el 10 de marzo de 2020, se llevaron a cabo 121 detenciones, fueron interceptados 48.000 paquetes en total, se eliminaron unos 2.500 links de Internet con contenido fraudulento y fueron desmantelados 37 organizaciones que se dedicaban a esta actividad ilícita.

16 Organización Mundial de la Salud (OMS), *Beware of criminals pretending to be WHO,* https://www.who.int/about/communications/cyber-security (última consulta: 14 de mayo de 2020).

17 Europol, *Informe Pandemic profiteering: how criminals exploit the COVID-19 crisis… op. cit.,* p. 5, ZD Net, *Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak,* https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/(última consulta: 14 de mayo de 2020), 13 de marzo de 2020 o ABC, *Un ciberataque bloquea la actividad en un hospital checo en plena pandemia del Coronavirus,* https://www.abc.es/tecnologia/redes/abci-ciberataque-bloquea-actividad-hospital-checo-plena-pandemia-coronavirus-202003141652_noticia.html (última consulta: 14 de mayo de 2020), 14 de marzo de 2020.

18 National Crime Agency, "Law enforcement in coronavirus online safety push as National Crime Agency reveals 300,000 in UK pose sexual threat to children", en Página web de la National Crime Agency, Reino Unido, https://www.nationalcrimeagency.gov.uk/news/onlinesafetyathome (última consulta: 14 de mayo de 2020), 4 de abril de 2020.

va del confinamiento por el COVID-19, a pesar de que en este caso no se trate de un caso de ciberdelincuencia, sino de delincuencia en el espacio delictivo tradicional. Baste como ejemplo la estadística facilitada por la Fundación ANAR, dedicada a la ayuda de los niños y los adolescentes en riesgo, que arrojaba el dato de que del 23 al 30 de marzo fueron identificados por sus trabajadores 173 casos graves en los cuales menores de edad estaban sufriendo algún tipo de violencia dentro de su propio hogar[19].

En definitiva, es latente que el confinamiento ha traído consigo el hecho de que pasemos más tiempo que antes en Internet, que llevemos a cabo más actividades en la red y que, en consecuencia, introduzcamos más intereses y valores personales en el ciberespacio. Algo que no deja de constituir un aumento de la velocidad de un fenómeno que ya llevamos años experimentando en la medida en la que las Tecnologías de la Información y de la Comunicación (TIC, en adelante) y, en concreto, Internet van teniendo cada vez más protagonismo en nuestra vida diaria[20]. Lo que queda fuera de toda duda es que el confinamiento ha derivado en un desplazamiento de la delincuencia al ciberespacio, donde los ciberdelincuentes pueden amenazar estos valores bajo las condiciones e implicaciones que analizamos en el apartado que sigue.

2. Los caracteres del ciberespacio y sus implicaciones en la dogmática penal

En efecto, cuando afirmamos que la delincuencia se ha visto desplazada al ciberespacio no se trata de una afirmación vacía de contenido y que tan solo hace referencia al espacio de perpetración de la actividad delictiva durante el confinamiento, sino que el mundo virtual presenta ciertas características de corte criminológico, muy diferenciadas de las que rigen el espacio delictivo tradicional, y que tiene influencia directa en los aspectos penales de los ilícitos.

Comenzando por los aspectos técnicos, es posible apuntar que el ciberespacio, presidido por Internet y, en general, las TIC atesoran una gran capacidad de albergar, procesar y distribuir ingentes volúmenes de datos y llevan a cabo este cometido a una velocidad sin parangón[21].

Este carácter resulta idóneo para la comisión de ciertos delitos contra la propiedad intelectual[22], donde es necesario el almacenamiento y descarga de obras en alta calidad y a una velocidad competitiva. El espionaje industrial o el descubrimiento de secretos[23], por su parte, pueden verse también fomentados en la red, en el momento en el que el material susceptible de lesionar la intimidad o el patrimonio empresarial se trata de archivos de tamaño considerable. También los delitos de pornografía infantil[24], en lo que a su distribución se refiere, son idóneos para ser cometidos por Internet gracias, entre otras, a esta característica.

19 En Fundación ANAR, "Informe sobre violencia intrafamiliar durante el confinamiento por Coronavirus", en Página web de la Fundación ANAR, Fundación ANAR, https://www.anar.org/fundacion-anar-refuerza-chat-ayuda-ninos-adolescentes-durante-confinamiento-y-alerta-de-la-gravedad-de-los-casos-detectados/(última consulta 14 de mayo de 2020) se detalla como la violencia física constituye el 12,7% de los casos detectados, la psicológica un 6,9% y el abuso sexual un 3,5%.

20 Por todos, BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos,* Editorial Wolters Kluwer, Madrid, 2018, pp. 27-30.

21 La doctrina se ha hecho eco durante los años de esta peculiaridad de las TIC, la cual ha sido definitoria en todas las etapas de su evolución y lo es, si cabe, a día de hoy en mayor medida: GERCKE, Marco y BRUNST, Phillip W., *Praxishandbuch Internetstrafrecht,* Editorial W. Kohlhammer, Stuttgart, 2009, pp. 14-16, ASENCIO GUILLÉN, Antonio, "El ciberespacio como sistema y entorno social: una propuesta teórica a partir de Niklas Luhmann", en Comunicación y Sociedad, vol. 31, núm. 1, Universidad de Navarra, Pamplona, 2018, pp. 23-36, ROMEO CASABONA, Carlos María, "De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* ROMEO CASABONA, Carlos María (coord.), Editorial Comares, Granada, 2006, p. 3, HILGENDORF, Eric, "Die strafrechtliche Regulierung des Internet als Aufgabe eines modernen Technikrechts", en Juristen Zeitung, núm. 17, Mohr Siebeck, Tubinga, 2012, pp. 829 o LESSIG, Lawrence, "Las leyes del ciberespacio", en THEMIS: revista de Derecho, Asociación civil THEMIS, Perú, 2002, pp. 171-179.

22 Una monografía centrada en este ciberdelito y, en concreto, en la posibilidad de difusión de los contenidos que otorga la red en: BARRIO ANDRÉS, Moisés, *Derecho público y propiedad intelectual: su protección en Internet,* Editorial Reus, Madrid, 2017.

23 Este delito se centra, tal y como se explica en FERNÁNDEZ DÍAZ, Carmen Rocío, *El Derecho penal frente al espionaje empresarial,* Editorial Tirant lo Blanch, Valencia, 2018, pp. 45-47, el descubrimiento o difusión tras descubrimiento de un secreto de empresa que constituye una expectativa idónea para traducirse a una ventaja competitiva del propietario del secreto en el mercado.

24 Un análisis de este delito y de la problemática con el debido control de los prestadores de servicios de Internet en GARCÍA ALBERO, Ramón, "Pornografía infantil y reforma penal", en *Delitos contra la libertad e indemnidad sexual de los menores,* VILLACAMPA ESTIARTE, Carolina (coord.), Editorial Thomson Reuters Aranzadi, Pamplona, 2015, pp. 284-292. Del mismo modo, se trata de un ciberdelito que ha alcanzado una nueva significación gracias a Internet, ya que la difusión de sus contenidos y el acceso global a los mismos por parte de los consumidores finales se ha disparado.

Poniendo el foco en los delitos que están proliferando en esta época de confinamiento de la población, la gran capacidad y velocidad de almacenamiento y procesamiento de datos que presentan las TIC resulta aparentemente adecuada también para vulnerar sistemas de información, como el del anteriormente mencionado Hospital Universitario de Brno, dada la velocidad con la que los cibercriminales son capaces de desplazarse y descargar datos en la red.

En segundo término, como principal característica del moderno 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[25]. Algo que, sin lugar a dudas, se ha visto potenciado por la obligación de permanecer en sus hogares bajo la que se encuentra gran parte de la ciudadanía.

Tal y como hemos comprobado en el apartado anterior, son dos los principales ciberdelitos cuya comisión se ha visto potenciada por este aspecto: las estafas informáticas y los delitos contra la libertad e indemnidad sexual de los menores.

En lo que se refiere a las estafas, estas se ven fomentadas en el momento en el que llevamos a cabo en el mundo virtual acciones imprudentes con respecto de nuestro patrimonio que, de ninguna manera, haríamos en el mundo real[26]. Por su lado, los delitos contra la indemnidad sexual son más comunes gracias a que el acceso al ciberespacio se ha democratizado sin entender de clases sociales ni de edades y un mayor tiempo de uso de Internet por parte de nuestros menores se traduce en una mayor amenaza para ellos, en los casos en los que su actividad *online* no sea tutelada[27].

Asimismo, los delitos contra el honor[28] o contra la paz pública (delitos de terrorismo)[29] han sido facilitados por el aumento en el número de usuarios de Internet, puesto que los contenidos calumniosos, injuriosos o de enaltecimiento terrorista, por ejemplo, son accesibles por un mayor número de personas en la actualidad.

En la línea de los usos de Internet, no debemos desdeñar la irrupción del *Internet of Things (IOT)* que, en estos días, se postula como una de las amenazas para la intimidad de los usuarios[30]. 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.

Una tercera característica de las TIC, en el plano técnico, es la posibilidad de anonimato y simulación de identidad que ofrece a sus usuarios[31]. Son muchos y muy diversos los delitos cuya comisión puede verse beneficiada por esta cuestión, puesto 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.

Si versamos sobre las infracciones potenciadas por el confinamiento, los delitos de denegación de servicio o el intrusismo informático en un sistema de información ajeno son ilícitos que son habitualmente cometidos de forma anónima, tras una dirección IP o, incluso, sin

25 Las siguientes obras muestran la evolución de los usos de los ciudadanos de Internet y la creciente importancia de la red en su día a día: ROMEO CASABONA, Carlos María, "De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal" … *op. cit.,* p. 3, VALIENTE GARCÍA, Francisco Javier, "Comunidades virtuales en el ciberespacio", en Doxa comunicación: revista interdisciplinar de estudios de comunicación y ciencias sociales, núm. 2, Universidad San Pablo-CEU, Madrid, 2004, pp. 137-150 o HERNÁNDEZ MORENO, Alberto, "Ciberseguridad y confianza en el ámbito digital", en Información Comercial Española, ICE: revista de economía, núm. 897, Ministerio de Economía, Industria y Competitividad, Madrid, 2017, pp. 55-66.

26 En MIRÓ LLINARES, Fernando, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* Editorial Marcial Pons, Madrid, 2012, p. 191 se explica la vital importancia de la contribución de la víctima en los ciberdelitos, puesto que sin la interacción inicial de esta a través de los estímulos creados por el ciberdelincuente nunca existiría el delito.

27 VILLACAMPA ESTIARTE, Carolina, "El delito de *online child grooming* o propuesta sexual telemática a menores", en *Delitos contra la libertad e indemnidad sexual de los menores,* VILLACAMPA ESTIARTE, Carolina (coord.), Editorial Thomson Reuters Aranzadi, Pamplona, 2015, pp. 156-158.

28 En DE PABLO SERRANO, Alejandro, *Honor, injurias y calumnias. Los delitos contra el honor en el Derecho histórico y en el Derecho vigente español,* Editorial Tirant lo Blanch, Valencia, 2018, p. 313 se introducen los delitos de injurias y calumnias y, en concreto, se analiza la agravante por publicidad que presentan ambos delitos en donde es posible subsumir los casos en los que los mensajes injuriosos o calumniosos son vierten en Internet.

29 WEIMANN, Gabriel, *Terrorism in cyberspace,* Editorial Columbia University Press, Nueva York, 2015. Nos referimos sobre todo a los delitos de enaltecimiento del terrorismo.

30 HILGENDORF, Eric, "Die strafrechtliche Regulierung des Internet als Aufgabe eines modernen Technikrechts" … *op. cit.,* p. 830.

31 LESSIG, Lawrence, "Las leyes del ciberespacio" … *op. cit.,* pp. 171-179 u OWEN, Tim, "The Problems of Virtual Criminology", en *New perspectives on cybercrime,* OWEN, Tim, NOBLE, Wayne y SPEED, Faye Christabel (coord.), Editorial Palgrave MacMillan, Preston, 2017, pp. 177-193.

dejar ningún tipo de huella virtual[32], a no ser que se trate de un ciberataque con fines reivindicativos[33]. En la misma línea, los delitos contra la indemnidad sexual de menores que introducíamos antes se ven fomentados por la opción de simulación de identidad que ofrece la red, siendo el *child grooming* el delito paradigmático aquí[34], puesto que los ciberagresores fingen ser jóvenes de edad similar a sus víctimas y estas nunca aceptarían la interacción con los victimarios si conociesen su verdadera identidad.

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[35]. Por último, también delitos contra el honor o contra la libertad (amenazas[36], *stalking[37]) son cometidos, en ocasiones, bajo identidades falsas en la red.*

En cuarto lugar, los fenómenos de permanencia y *automatismo* 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.

Uno de los primeros autores en introducir estos conceptos fue Rovira del Canto[38], quien ilustraba con el concepto *permanencia* que la red permite cierta repetición y automatismo respecto de la conductas delictivas[39]. 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 la doctrina alemana[40], 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[41].

Así pues, históricamente y en la medida en la que la delincuencia informática ha ido evolucionando, ha constituido un elemento básico para la comisión de delitos patrimoniales en masa, como las estafas o los daños informáticos, dado que se trata de delitos que

32 Expone VIOTA MAESTRE, Manuel, "Problemas relacionados con la investigación de los denominados delitos informáticos (ámbito espacial y temporal, participación criminal y otros)", en Cuadernos penales José María Lidón, núm. 4, Universidad de Deusto, Bilbao, 2007, p. 242 que la huella electrónica o digital o rastro en Internet se trata de la información sobre nuestra dirección IP que vamos dejando en cada servicio de Internet que utilizamos al navegar con nuestro ordenador: como cuando enviamos un correo electrónico o visitamos una página web. Nuestra actividad en Internet, por tanto, deja rastro, pero existen métodos para evitar este control o disfrazar de alguna manera nuestra actividad en la red. Por otro lado, por medio de los *proxys,* la red cuenta con unos intermediarios que se usan normalmente para aislar una red interna en Internet.

33 En DE LA CUESTA ARZAMENDI, José Luis y PÉREZ MACHÍO, Ana Isabel, "Ciberdelincuentes y cibervíctimas", en *Derecho penal informático*, DE LA CUESTA ARZAMENDI, José Luis (dir.), Editorial Civitas-Thomson Reuters, Pamplona, 2010, p. 104 se expone que, en sus inicios, existía un grupo de *hackers* que accedían a los sistemas de información de empresas y multinacionales, no con fines de lucro, sino con ánimo reivindicativo respecto de la gestión del poder en la sociedad y la premisa de que la información debería ser un bien de dominio público y acceso abierto.

34 VILLACAMPA ESTIARTE, Carolina, "El delito de *online child grooming* o propuesta sexual telemática a menores" … *op. cit.,* pp. 156-158.

35 LLOBET ANGLÍ, Mariona, "Delitos contra el orden público", en *Lecciones de Derecho penal. Parte especial,* SILVA SÁNCHEZ, Jesús-María (coord.), Editorial Atelier, Barcelona, 2015, p. 435.

36 RAGUÉS I VALLÈS, Ramón, "Delitos contra la libertad", en *Lecciones de Derecho penal. Parte especial,* SILVA SÁNCHEZ, Jesús-María (coord.), Editorial Atelier, Barcelona, 2015, pp. 105-106.

37 VILLACAMPA ESTIARTE, Carolina y PUJOLS PÉREZ, Alejandra, "El delito de *stalking* en el Código Penal español", en Stalking: *análisis jurídico, fenomenológico y victimológico,* VILLACAMPA ESTIARTE, Carolina (coord.), Editorial Thomson Reuters Aranzadi, Pamplona, 2018, pp. 183-194.

38 ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos,* Editorial Comares, Granada, 2002, pp. 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.

39 ALASTUEY DOBÓN, M. Carmen, "Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial", en Informática y Derecho: revista iberoamericana de Derecho informático, núm. 4, UNED, Madrid, 1994, p. 459.

40 SIEBER, Ulrich, "Criminalidad informática: peligro y prevención", en *Delincuencia informática,* MIR PUIG, Santiago (dir.), Editorial PPU, Barcelona, 1992, pp. 29-30 o FISCHER, Thomas, *Computer-Kriminalität,* Editorial Paul Haupt, Berna, 1979, p. 14.

41 También en clave alemana, en GERCKE, Marco y BRUNST, Phillip W., *Praxishandbuch Internetstrafrecht… op. cit.,* pp. 29-31 se aborda la característica de automatización que presentan los ciberdelitos. En concreto, se abordan los envíos masivos de correos SPAM, los *botnets,* los daños causados por *softwares* maliciosos y la afectación a las empresas. En el mismo sentido, se destaca la automatización en los ciberdelitos en: BERGAUER, Christian, *Das materielle Computerstrafrecht,* Editorial Jan Sramek, Viena, 2016, pp. 10-11. En la misma línea, HILGENDORF, Eric, "Die strafrechtliche Regulierung des Internet als Aufgabe eines modernen Technikrechts" … *op. cit.,* pp. 829-830.

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[42].

En lo que hace referencia a los delitos fomentados por el confinamiento provocado por la crisis sanitaria que analizamos en este trabajo, 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 que ha derivado en las conductas de *phishing*.

En otro orden de cosas, la contracción del espacio y su relativización[43] ha traído, además de la discusión en torno a la competencia territorial y al tribunal nacional competente en cada caso[44], la oportunidad para los cibercriminales de poder cometer su actividad ilícita desde casi cualquier parte del mundo y, a su vez, la opción de que los efectos de estos delitos puedan desplegarse también en cualquier lugar.

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[45], el hurto de tiempo[46] 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.

Los delitos relevantes en este análisis (la estafa informática, el intrusismo informático, la denegación de servicio y los delitos contra la indemnidad sexual de los menores) también se han visto enormemente beneficiados por la característica espacial de Internet. A pesar de que, en su caso, se trata de delitos que pueden ser cometidos sin la necesidad de distanciamiento espacial, de la misma manera que ocurre con la posibilidad de anonimato que proporciona la red, el hecho de que puedan cometerse a distancia es un elemento diferenciador a la hora de la toma de la decisión delictiva por parte de los cibercriminales.

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 de la ciberdelincuencia en los próximos años.

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. 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[47].

Así, de la primera cuestión se han visto beneficiados precisamente los delitos de estafa informática y los delitos contra la libertad e indemnidad sexuales, entre otros. El engaño bastante necesario para la consuma-

42 ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos… op. cit.,* pp. 77-79, ALASTUEY DOBÓN, M. Carmen, "Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial" … *op. cit.,* p. 459, SIEBER, Ulrich, "Criminalidad informática: peligro y prevención" … *op. cit.*, pp. 29-30, FISCHER, Thomas, *Computer-Kriminalität… op. cit.,* p. 14 o GERCKE, Marco y BRUNST, Phillip W., *Praxishandbuch Internetstrafrecht… op. cit.,* pp. 29-31.

43 DAVARA RODRÍGUEZ, Miguel Ángel, *Manual de Derecho informático,* Editorial Aranzadi Thomson Reuters, Pamplona, 2015, pp. 400-401, HILGENDORF, Eric, "Die strafrechtliche Regulierung des Internet als Aufgabe eines modernen Technikrechts" … *op. cit.,* p. 830, MIRÓ LLINARES, Fernando, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio… op. cit.,* pp. 146-148 o FLOR, Roberto, "La legge penale nello spazio, fra evoluzione tecnológica e difficoltà applicative", en *Cybercrime,* CADOPPI, Alberto, CANESTRARI, Stefano, MANNA, Adelmo y PAPA, Michele (coord.), Editorial Utet Giuridica, Milán, 2019, pp. 142-191.

44 Esta problemática ha sido ampliamente abordada por la doctrina, como por ejemplo en: BARRIO ANDRÉS, Moisés, *Ciberdelitos: amenazas criminales del ciberespacio,* Editorial Reus, Madrid, 2017, pp. 44-45, ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos… op. cit.,* pp. 98-100 o DE LA CUESTA ARZAMENDI, José Luis, PÉREZ MACHÍO, Ana Isabel y SAN JUAN GUILLÉN, César, "Aproximaciones criminológicas a la realidad de los ciberdelitos", en *Derecho penal informático*, DE LA CUESTA ARZAMENDI, José Luis (dir.), Editorial Civitas-Thomson Reuters, Pamplona, 2010, p. 91.

45 Una trabajo sobre este delito en: FARALDO-CABANA, Patricia, "Defraudación de telecomunicaciones y uso no consentido de terminales de telecomunicación: dificultades de delimitación entre los arts. 255 y 256 CP", en *Un Derecho penal comprometido: libro homenaje al Prof. Dr. Gerardo Landrove Díaz,* NÚÑEZ PAZ, Miguel Ángel (coord.), Editorial Tirant lo Blanch, Valencia, 2011, p. 376.

46 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* p. 130.

47 MIRÓ LLINARES, Fernando, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio… op. cit.,* pp. 148-151, ESER, Albin, "Internet und internationales Strafrecht", en *Rechtsfragen des Internet und der Informationsgesellschaft,* LEIPOLD, Dieter (coord.), Editorial C. F. Müller, Heidelberg, 2002, pp. 309-310, DAVARA FERNÁNDEZ DE MARCOS, Elena y DAVARA FERNÁNDEZ DE MARCOS, Laura, *Delitos informáticos,* Editorial Thomson Reuters Aranzadi, Pamplona, 2017, p. 38, ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos… op. cit.,* pp. 96-97 o VIOTA MAESTRE, Manuel, "Problemas relacionados con la investigación de los denominados delitos informáticos (ámbito espacial y temporal, participación criminal y otros)" … *op. cit.,* p. 243-248.

ción de la estafa, en los casos que hemos introducido en el apartado anterior, se da por medio de una interacción entre victimario y víctima sin necesidad de que coincidan al mismo tiempo en Internet, puesto que el estímulo enviado por el sujeto activo es un correo electrónico, un anuncio o cualquier otro contenido alojado en la web que el sujeto pasivo puede consultar cuando quiera. Del mismo modo, la interacción por medio de, por ejemplo, un chat en la red que existe entre los dos sujetos necesarios para la consumación de, por ejemplo, un delito de *child grooming* no debe ser necesariamente coincidente en el tiempo, sino que tanto el ciberagresor como su víctima pueden contestar a los mensajes en el momento en el que ellos tengan conexión a la red.

Por último, muchas de las características ya mencionadas hasta el momento en este apartado nos llevan a subrayar la facilidad de encubrimiento y la dificultad de persecución por parte de las autoridades que preside los ciberdelitos[48]. Elementos técnicos como la facilidad de alteración de la huella informática[49], el anonimato en los cibercrímenes o el simple hecho de que es necesaria una capacidad técnica mínima para navegar con plena conocimiento de la red[50] ayudan a argumentar las postura de que existe una cifra negra[51] muy importante en la ciberdelincuencia.

3. La regulación de los ciberdelitos de estafa informática, intrusismo informático, denegación de servicio y los ciberdelitos contra la indemnidad sexual de los menores en el Código Penal español

Así pues, tras observar la proliferación de ciertos ciberdelitos en tiempos de confinamiento y haber estudiado las características del ciberespacio que definen la comisión de los mismos, nos centramos ahora en una breve introducción de las infracciones penales más comunes en virtud de lo expuesto en el apartado primero del trabajo.

El delito de estafa informática está regulado en el artículo (art., en adelante) 248. 2 del Código Penal[52] (CP, en adelante), donde el apartado a) afirma que serán también reos del delito descrito en el tipo básico cuando el error que conduce al engaño preceptivo en la estafa sea causado por "alguna manipulación informática o artificio semejante"[53].

Es posible interpretar el concepto *manipulación informática*[54] identificándolo con la acción de intervenir en un sistema informático alterando, modificando u ocultando datos o modificando las instrucciones de un

48 ANARTE BORRALLO, Enrique, "Incidencia de las nuevas tecnologías en el sistema penal: aproximación al Derecho penal en la sociedad de la información", en Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento, núm. 1, Universidad de Huelva, Huelva, 2001, p. 203, DAVARA FERNÁNDEZ DE MARCOS, Elena y DAVARA FERNÁNDEZ DE MARCOS, Laura, *Delitos informáticos… op. cit.,* pp. 38-39, MATA Y MARTÍN, Ricardo M., *Delincuencia informática y Derecho penal,* Editorial Edisofer, Madrid, 2001, p. 26, DE LA CUESTA ARZAMENDI, José Luis, PÉREZ MACHÍO, Ana Isabel y SAN JUAN GUILLÉN, César, "Aproximaciones criminológicas a la realidad de los ciberdelitos" … *op. cit.,* p. 89, ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos… op. cit.,* p. 83, WERNERT, Manfred, *Internetkriminalität,* Editorial Boorberg, Stuttgart, 2017, pp. 36-40, HILGENDORF, Eric y VALERIUS, Brian, *Computer- und Internetstrafrecht,* Editorial Springer, Berlin, 2012, pp. 233-236 o BARRIO ANDRÉS, Moisés, *Ciberdelitos: amenazas criminales del ciberespacio… op. cit.,* p. 37.

49 ROMEO CASABONA, Carlos María, "De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal" … *op. cit.,* p. 3 o VALIENTE GARCÍA, Francisco Javier, "Comunidades virtuales en el ciberespacio" … *op. cit.,* p. 139.

50 MATA Y MARTÍN, Ricardo M., *Delincuencia informática y Derecho penal… op. cit.,* p. 27, WERNERT, Manfred, *Internetkriminalität… op. cit.,* 2017, pp. 36-40 o HILGENDORF, Eric y VALERIUS, Brian, *Computer- und Internetstrafrecht… op. cit.,* pp. 233-236.

51 Este concepto hace referencia al número de ciberdelitos que, a pesar de ser cometidos, no forman parte de las estadísticas. Las razones que explican este fenómeno son diversas: el hecho de que ciertas víctimas no sean conscientes de que han sido atacadas por un ciberdelito, los casos en los que las víctimas son menores y no encuentran un canal de denuncia adecuado, la falta de confianza en los canales de denuncia, el sentimiento de vergüenza hacia una posible ridiculización social, el sentimiento de culpabilidad por haber contribuido con actos necesarios a la perpetración del delito y, en relación con las empresas, el hecho de que una denuncia puede ser más perjudicial para la empresa en términos de reputación que una posible restitución o reparación del daño causado por el ciberdelito. Todo esto es analizado en profundidad en: MIRÓ LLINARES, Fernando, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio… op. cit.,* pp. 289-291 y 295, REYNA ALFARO, Luis Miguel, "Aproximaciones criminológicas al delito informático", en Capítulo Criminológico, vol. 31, núm. 4, Universidad del Zulia, Venezuela, 2003, p. 99, DE LA CUESTA ARZAMENDI, José Luis y PÉREZ MACHÍO, Ana Isabel, "Ciberdelincuentes y cibervíctimas" … *op. cit.*, pp. 116-118 o MORÓN LERMA, Esther, *Internet y Derecho penal: hacking y otras conductas ilícitas en la red,* Editorial Aranzadi, Pamplona, 2002, p. 27.

52 España, *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*, "BOE" núm. 281, de 24/11/1995.

53 DE URBANO CASTRILLO, Eduardo, "Los delitos informáticos tras la reforma del CP de 2010", en *Delincuencia informática: tiempos de cautela y amparo,* DE URBANO CASTRILLO, Eduardo (coord.), Editorial Thomson Reuters Aranzadi, Pamplona, 2012, pp. 22-23, QUERALT JIMÉNEZ, Joan J., *Derecho penal español. Parte especial,* Editorial Atelier, Barcelona, 2010, pp. 517-518, VELASCO NÚÑEZ, Eloy, *Delitos cometidos a través de Internet: cuestiones procesales,* Editorial La Ley, Madrid, 2010, pp. 42-43 o BUTTON, Mark y CROSS, Cassandra, *Cyber frauds, scams and their victims,* Editorial Routledge, Nueva York, 2017, pp. 46-51.

54 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* p. 126.

programa determinado, es decir, cualquier utilización irregular de un sistema informático[55].

El apartado b), por su lado, castiga la fabricación, introducción, posesión o facilitación de programas informáticos dirigidos específicamente a la comisión de las estafas previstas en el artículo. Previsión que deja impunes las conductas relativas a *softwares* que no presenten la específica finalidad de cometer una estafa[56].

En tercer lugar, el apartado c) del precepto considera también estafa la utilización de tarjetas de crédito o débito o cheques de viaje, o de sus datos, en perjuicio del titular o un tercero. Este precepto fue introducido por la reforma de la Ley Orgánica 5/2010[57] con el fin de cerrar la discusión doctrinal[58] referente a la laguna relativa a la subsunción penal de delitos basados en la utilización de estos medios de pago o de los datos que contienen, sin necesidad de utilizar las tarjetas materialmente, para llevar a cabo operaciones en perjuicio del titular[59]. Un ejemplo recurrente de ello es la copia de tarjetas o *carding.*

Para cerrar la presentación de este delito, cabe apuntar que existen dos variantes de estafa informática en función del objeto del engaño en la conducta: la estafa sociológica y la estafa mecánica[60].

En la primera, la más cercana a la estafa clásica, el engaño se lleva a cabo sobre una persona y este conduce a que esta cometa un error, el cual lleva al acto de disposición patrimonial, creando un perjuicio[61]. Estos son los casos, por ejemplo, de las cartas nigerianas[62]. Otro ejemplo[63] lo constituyen las ventas de artículos por Internet con pago anticipado, cuyo elemento adquirido por el comprador nunca es entregado, desapareciendo además cualquier rastro del supuesto vendedor o, a pesar de que el producto sea entregado, este no reúne las condiciones pactadas.

Es dentro de las estafas sociológicas, por lo tanto, donde encontramos dos de las estafas informáticas más comunes durante el confinamiento: los casos de entrega defectuosa de los materiales sanitarios comprados por Internet y los supuestos en los que el adquiriente ni siquiera recibe lo acordado en su domicilio.

Un supuesto de corte similar lo constituyen los casos de falsas subastas, en las que la víctima puja por un bien que nunca recibirá, siendo objeto además de pujas falsas por parte del propio criminal o de cómplices del mismo, con el fin de aumentar el precio finalmente pagado por el comprador[64].

---

55 El término *artificio semejante,* sin embargo, resulta algo más complicado de concretar. BARRIO ANDRÉS (*idem*) propone una doble interpretación: a) igualarlo a la manipulación informática para poder incluir los casos en los que el objeto violentado no se trate de un sistema de información propiamente dicho o b) asimilarlo a lo informático, donde tendrían cabida toda conducta con afectación a un sistema informático.

56 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* p. 127.

57 España, *Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal,* "BOE" núm. 152, de 23/06/2010, pp. 54.811-54.883.

58 Un par de ejemplos de dicho debate en DE LA MATA BARRANCO, Norberto J. y HERNÁNDEZ DÍAZ, Leyre, "Los delitos vinculados a la informática en el Derecho penal español", en *Derecho penal informático*, DE LA CUESTA ARZAMENDI, José Luis (dir.), Editorial Civitas-Thomson Reuters, Pamplona, 2010, p. 166, en MORENO VERDEJO, Jaime, "Algunas cuestiones acerca de la estafa informática y uso de tarjetas (Incidencia del Anteproyecto de 2006 de reforma del Código Penal", en Cuadernos penales José María Lidón, núm. 4, Universidad de Deusto, Bilbao, 2007, pp. 200-226 o en ABOSO, Gustavo Eduardo y ZAPATA, María Florencia, *Cibercriminalidad y Derecho penal: la información y los sistemas informáticos como nuevo paradigma del Derecho penal. Análisis doctrinario, jurisprudencial y derecho comparado de los denominados "delitos informáticos",* Editorial B de F Montevideo, Uruguay, 2006, pp. 77-83.

59 En BARRIO ANDRÉS, Moisés, *Ciberdelitos: amenazas criminales del ciberespacio… op. cit.,* p. 98 se expone que esta reforma legislativa dio además respuesta a la Decisión Marco del Consejo sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, 28 de mayo de 2001.

60 REY HUIDOBRO, Luis Fernando, "La estafa informática: relevancia penal del *phishing* y el *pharming*", en La ley penal: revista de Derecho penal, procesal y penitenciario, núm. 101, Wolters Kluwer, Madrid, 2013, p. 2.

61 CRUZ DE PABLO, José Antonio, *Derecho penal y nuevas tecnologías: aspectos sustantivos,* Editorial Grupo Difusión, Madrid, 2006, pp. 38-47.

62 Comunicaciones por parte de ciberdelincuentes a sus víctimas en las cuales les prometen que van a recibir una gran cantidad de dinero pero que, en el proceso de recepción de dicha cuantía, los criminales se hacen con datos personales y bancarios de los supuestos benefactores, así como consiguen que estos efectúen pagos en calidad de impuestos por la transacción de un dinero que nunca reciben. Estos comportamientos ilícitos basados en la obtención, por parte de los cibercriminales, de datos de carácter personal fueron previstos ya en los años 70 por SIEBER en su obra SIEBER, Ulrich, *Computerkriminalität und Strafrecht,* Editorial Carl Heymanns, Colonia, 1977, pp. 24-28, donde alertaba de la posibilidad de aparición de estas conductas y de la necesidad de adoptar medidas de carácter político para su prevención, debido a la cantidad de datos y valores de los ciudadanos que acertadamente previó que se introducirían en los ordenadores del futuro.

63 GILLESPIE, Alisdair A., *Cybercrime: key issues and debates,* Editorial Routledge, London, 2019, pp. 155-160.

64 Más ejemplos de estafas sociológicas por medios informáticos o cibernéticos en esta misma línea en BARRIO ANDRÉS, Moisés, *Ciberdelitos: amenazas criminales del ciberespacio… op. cit.,* pp. 94-95: uso no autorizado de tarjetas de crédito tras obtener los datos en

Ahora bien, el principal supuesto de hecho subsumible en el art. 248. 2 CP y, a su vez, uno de los más comunes durante el confinamiento causado por la alerta sanitaria del COVID-19 es el caso del *phishing*[65].

El *phishing* se trata de una estafa informática basada en que el *phisher* consigue información confidencial de la víctima, generalmente sobre datos de tarjetas de crédito o similares, con el fin de llevar a cabo transacciones patrimoniales a su favor[66]. Dicha información, de forma general, es obtenida por el delincuente por medio de la suplantación de identidad y la creación de una esfera de confianza en el sujeto pasivo. El criminal diseña una página web simulando fielmente el portal de banca electrónica de la víctima, para invitarle a introducir sus contraseñas y datos de acceso, mediante una comunicación vía correo electrónico[67]. Estos casos son análogos a los presentados en el capítulo primero del trabajo, donde la OMS alertaba de estas conductas a los usuarios de su página web.

La segunda modalidad de estafa informática es la mecánica. La distinción con la sociológica es que lo que se manipula en estos casos son máquina o elementos de naturaleza similar, en lugar de los usuarios de Internet.

La principal práctica delictiva en estos casos es el *pharming*[68]. Esta técnica tiene un funcionamiento similar al *phishing,* en el sentido en el cual también busca la suplantación de identidad de una página de confianza de la víctima para producir el error y que esta proporcione sus datos bancarios, por ejemplo. Sin embargo, no es coincidente en el engaño inicial que produce dicho error ya que, como decimos, la manipulación se lleva a cabo sobre la propia máquina (un ordenador en este caso), al redirigir fraudulentamente al usuario a un destino web similar en apariencia creado por el delincuente, en lugar del sitio web que el comando introducido por la víctima debería devolver. Esta manipulación se consigue gracias a la alteración de las direcciones DNS o *Domain Name Server*[69].

En segundo lugar, el intrusismo informático está regulado junto con los delitos de descubrimiento y revelación de secretos, en concreto, en el art. 197 bis. 1 y se concreta en acceder o facilitar el acceso a un sistema de información o mantenerse en el mismo vulnerando las medidas de seguridad. Esta conducta es también conocida tradicionalmente por el término anglosajón *hacking*[70].

Existen dos principales debates doctrinales relativos a esta conducta. El primero hace referencia al bien jurídico protegido por la misma, cuestión que abordaremos en el apartado que sigue y en referencia a todos los ciberdelitos aquí analizados. El segundo, por su lado, se centra en los verbos típicos expuestos por el tipo.

Por un lado, con la acción de acceder el legislador busca castigar la intromisión física o remota en todo o parte de un sistema de información pero, en todo caso, vulnerando las medidas de seguridad establecidas para impedirlo, por lo que la falta de estas medidas conlleva necesariamente la atipicidad de la conducta. Ahora bien, dado que la reforma de 2015[71] ha suprimido la necesidad de que el acceso al sistema sea efectivo, parece correcto afirmar que es suficiente con el mero acceso, sin necesidad de abrir o gestionar los archivos contenidos en dicho sistema de información. Por otro, la conducta de mantenerse en el sistema abarcaría los supuestos en los que el acceso al mismo es lícito, pero más adelante la voluntad del propietario del espacio cambia, y en los que el acceso no es consentido, pero

---

una supuesta comprobación de edad del usuario, marketing multinivel al estilo de las cartas nigerianas, siendo estas una concreción de este fenómeno, según el cual el sujeto pasivo acaba por realizar actos de disposición patrimonial a modo de comisiones por un beneficio superior que nunca llega, ofertas de negocios potencialmente muy provechosos que requieren de una mínima (en comparación) inversión inicial, prestaciones de servicios inexistentes de pago anticipado (servicios turísticos, en su mayoría, como paquetes de viaje, transporte, alojamiento o servicios de calidad inferior a la pagada) o venta de medicamentos falsificados por Internet.

65 En estrecha relación con el *phishing,* en los últimos años se ha desarrollado una conducta consistente en utilizar a terceros, denominados "muleros" en la doctrina, para que estos lleven a cabo transferencias del dinero obtenido inicialmente de la estafa informática a cuentas en países extranjeros, generalmente, a cambio de una comisión de la cuantía defraudada. En MIRÓ LLINARES, Fernando, "La respuesta penal al ciberfraude: especial atención a la responsabilidad de los muleros del *phishing*", en Revista electrónica de ciencia penal y criminología, núm. 15, Universidad de Granada, Granada, 2013 se aborda la cuestión de la responsabilidad de estos intermediarios y su posible imputación respecto de los delitos de estafa informática (como partícipes) e, incluso, blanqueo de capitales (como autores), en relación con la regulación de las Ley Orgánica 5/2010.

66 DAVARA FERNÁNDEZ DE MARCOS, Elena y DAVARA FERNÁNDEZ DE MARCOS, Laura, *Delitos informáticos… op. cit.,* pp. 108-110.

67 KRISCHKER, Sven, *Das Internetstrafrecht vor neuen Herausforderungen,* Editorial Logos, Berlin, 2014, p. 29.

68 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* p. 129.

69 FERNÁNDEZ TERUELO, Javier Gustavo, *Cibercrimen: los delitos cometidos a través de Internet,* Editorial Constitutio Criminalis Carolina, Madrid, 2007, p. 30.

70 MORÓN LERMA, Esther, *Internet y Derecho penal: hacking y otras conductas ilícitas en la red… op. cit.,* p. 42.

71 España, *Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*, "BOE" núm. 77, de 31/03/2015, pp. 27.061-27.176.

no vulnera ninguna medida de seguridad como para ser incluido en el mero acceso al sistema[72].

Así pues, si volvemos a los ciberdelitos más comunes durante el confinamiento, esta figura corresponde con el caso de la intromisión en el sistema informático del Hospital Universitario de Brno, en el caso en el que hubiesen desconectado su sistema de información por el hecho de que los *hackers* hayan accedido al sistema.

En sentido contrario, si los *hackers* no sólo entraron al sistema informático del Hospital, sino que fueron ellos mismos quienes interrumpieron su funcionamiento estaríamos ante la conducta de denegación de servicio o *Denial of Service (DoS)* que presentamos a continuación.

La conducta está recogida en el art. 264 bis, tras los daños informáticos, y consiste en obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno de manera grave y por medio de las conductas que describe el tipo[73].

En la práctica estos ilícitos encajan, como decimos, con los ataques masivos de denegación de servicio, que persiguen sobrecargar o saturar los recursos de un sistema de información concreto hasta hacerlo inoperativo por medio de su bloqueo temporal. Es habitual su comisión por medio de redes de ordenadores controlados a distancia o *botnets,* que envían correos *spam* de forma masiva con el objetivo de propagar virus o causar dicha DoS[74].

Este tipo penal prevé también conductas agravadas: la primera está recogida en el propio apartado primero del art. 264 bis y se refiere a los escenarios en los que se perjudica de forma relevante la actividad normal de un colectivo afectado por la conducta ilícita; la segunda hace referencia a las circunstancias del apartado segundo del art. 264 y la tercera, por su lado, se recoge en el apartado tres y se redacta en los mismos términos que la agravante del art. 264. 3[75].

Así pues, de una lectura del artículo es sencillo deducir la existencia de una problemática sobre la indeterminación conceptual que deja en manos de la discrecionalidad del juzgador la apreciación o no de las circunstancia agravantes con base en lo que estime que los conceptos "de manera grave" o "de forma relevante", entre otros, significan en cada supuesto[76].

Para terminar, los delitos contra la indemnidad sexual de los menores están recogidos en los artículos (arts., en adelante) 183 bis y 183 ter, además del delito de pornografía infantil que recoge el 189 CP.

Por un lado, el delito de abuso sexual es introducido por el art. 183 bis CP y castiga el hacer presenciar a un menor de 16 años actos de carácter sexual o hacerle partícipe en actos de naturaleza sexual, con fines sexuales para el sujeto activo, independientemente de que éste participe o no en el referido acto. En su segundo párrafo, este artículo recoge una modalidad agravada para las ocasiones en las cuales lo presenciado por el menor sea un abuso sexual. Este delito fue incluido en la reforma de nuestro CP del año 2010, para cumplir con las exigencias de la Directiva 2011/93/UE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil[77].

Esta modalidad permite su comisión fuera de la red, pero es la irrupción de Internet la que ha convertido el ilícito en una práctica habitual sobre todo en el ciberespacio, donde es más sencillo hacer presenciar a menores actos de carácter sexual por medio del envío instantáneo de los materiales objeto del delito[78]. Algo que, sin lugar a dudas, pone el peligro la libertad e indemnidad sexual de nuestros menores y se trata de una amenaza de gravedad directamente proporcional al tiempo en el que estos dedican a sus relaciones por Internet sin supervisión.

Por otro lado, en el art. 183 ter encontramos el delito de *child grooming*. Concepto entendido como el contacto por medio de las TIC con un menor de 16 años para concertar un encuentro sexual, con actos materiales encaminados al acercamiento (183 ter. 1 CP), o para que el menor le muestre material pornográfico en el que

72 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* pp. 93-94.

73 Estas conductas son las del delito de daños informáticos, la introducción o transmisión de datos o la destrucción, dañado, inutilización, eliminado o sustitución de un sistema informático, telemático o de almacenamiento de información electrónica, tal y como se especifica en: DAVARA FERNÁNDEZ DE MARCOS, Elena y DAVARA FERNÁNDEZ DE MARCOS, Laura, *Delitos informáticos… op. cit.,* pp. 115-118 o DE URBANO CASTRILLO, Eduardo, "Los delitos informáticos tras la reforma del CP de 2010" … *op. cit.*, pp. 23-24.

74 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* p. 116.

75 QUERALT JIMÉNEZ, Joan J., *Derecho penal español. Parte especial… op. cit.,* pp. 640-645.

76 FERNÁNDEZ TERUELO, Javier Gustavo, *Cibercrimen: los delitos cometidos a través de Internet… op. cit.,* p. 114.

77 Unión Europea, *Directiva del Parlamento Europeo y del Consejo, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil,* de 13 de diciembre de 2011, 2011/93/UE, "DOUE" núm. 335, de 17/12/2011, pp. 1-14.

78 VILLACAMPA ESTIARTE, Carolina, "El delito de *online child grooming* o propuesta sexual telemática a menores" … *op. cit.*, pp. 160-169.

aparezca un menor (183 ter. 2 CP)[79]. Esta última modalidad delictiva se conoce habitualmente como *sexting.*

La principal distinción con respecto del abuso sexual es que el *child grooming* y el *sexting* sí se tratan de ciberdelitos en sentido estricto, al sólo poder cometerse por Internet o, tal y como reza el artículo, "a través del teléfono o de cualquier otra tecnología de la información y la comunicación"[80] y, por consiguiente, son idóneas para que su comisión presente un crecimiento en época de confinamiento de la población.

En concreto, el delito de acercamiento o *child grooming*[81] se trata de un delito de peligro que no precisa del contacto físico entre víctima y victimario, ya que es suficiente para su apreciación el hecho de que este último lleve a cabo acciones deliberadamente orientadas a establecer una relación de control sobre el menor con el fin de "disminuir sus inhibiciones y preparar el terreno para el abuso sexual de la víctima"[82]. Presenta además una agravante específica en el propio art. 183 ter. 1 para los casos en los que dicho acercamiento se obtenga por medio de coacción, intimidación o engaño.

Por su lado, el *sexting* se concreta en el embaucamiento de un menor por medio de las TIC para obtener o conseguir la exhibición de material pornográfico.

Esta conducta fue introducida por la Ley Orgánica 1/2015, a pesar de que la responsabilidad por estos actos se depuraba por medio de la tentativa del delito de pornografía infantil hasta la reforma[83]. Pero, de nuevo, la delimitación de la aplicación de este delito genera dudas, en el sentido en el que podría igualmente aplicarse el apartado primero del art. 189 en ciertos casos, por lo que la doctrina y el propio Tribunal Supremo[84] se decantan por aplicar la tentativa del delito de *sexting* solo cuando no se obtenga el material sexual.

4. ¿Qué valores debemos proteger? La discusión en torno al bien jurídico protegido por los ciberdelitos más comunes durante el confinamiento

Visto todo lo anterior, este cuarto apartado busca ser un reflejo de las diferentes propuestas doctrinales existentes en lo que a los bienes jurídicos protegidos en los cuatro ciberdelitos analizados se refiere.

La relevancia de este análisis reside en que, en el momento en el que los ciudadanos introducimos cada vez más valores en el ciberespacio, siendo en esta ocasión el confinamiento derivado del COVID-19 la causa de este fenómeno, en algunos de los delitos cuya comisión es más común surge la cuestión de si el interés protegido son los bienes jurídicos tradicionalmente tutelados por nuestra legislación penal o nuevos valores relacionados con los sistemas de información en sí mismos.

Comenzando por el delito de estafa informática, existe acuerdo en la doctrina en indicar que el bien ju-

79 Esta aclaración es necesaria vistos los diferentes usos que se le han dado a la figura anglosajona del *child grooming,* la cual ha sido también utilizada para designar la figura recogida en el art. 183 bis CP, según se describe en VILLACAMPA ESTIARTE, Carolina, "El delito de *online child grooming* o propuesta sexual telemática a menores" … *op. cit.,* pp. 139-146.

80 POWELL, Anastasia y HENRY, Nicola, *Sexual violence in a digital age,* Editorial Macmillan, Londres, 2017, p. 49 o MALDONADO GUZMÁN, Diego J., "El mal denominado delito de *grooming online* como forma de violencia sexual contra menores. Problemas jurídicos y aspectos criminológicos", en Revista electrónica de estudios penales y de la seguridad, núm. extra 5, Editorial Jurídica Continental, Costa Rica, 2019, pp. 1-18.

81 La cuestión que más debate doctrinal ha suscitado sobre esta conducta es las relaciones concursales de la misma con el resto de los delitos contra la indemnidad sexual, a pesar de que es el propio artículo quien expone que las penas aparejadas al tipo se impondrán "sin perjuicio de las penas correspondientes a los delitos en su caso cometidos". Esto es así, porque se incurre en un *non bis in idem* si se castiga la conducta del acercamiento junto con alguno de los delitos de entre los arts. 183 y 189 del CP. La propuesta de la doctrina es la de tratar esta relación concursal como un concurso de normas, y no como uno de delitos, y poder así proceder a la imputación del segundo delito contra la indemnidad sexual cometido, absorbiendo el delito de *child grooming,* al considerarlo un mero acto preparatorio. Reservaríamos la opción de que formara parte de un concurso de delitos en los casos en los que concurra junto con un delito no recogido entre los arts. 183 y 189 CP. Son sólo algunos ejemplos del interés tanto en el ámbito doctrinal, como jurisprudencial, en obras tanto de académicos, como de miembros de la carrera judicial: SÁNCHEZ ESCRIBANO, María Isabel Montserrat, "Propuesta para la interpretación de la cláusula concursal recogida en el art. 183 ter 1 (delito de *online child* grooming)", en Revista de Derecho, Empresa y Sociedad (REDS), núm. 12, Dykinson, Madrid, 2018, pp. 141-151, MOLINA MANSILLA, Carmen, "Última doctrina jurisprudencial en torno al delito de *child grooming*: aspectos más significativos de las reglas concursales", en La ley penal: revista de Derecho penal, procesal y penitenciario, núm. 136, Wolters Kluwer, Madrid, 2019, ORTEGA CALDERÓN, Juan Luis, "La aplicación de las reglas concursales con ocasión del delito de *child grooming*: análisis de la evolución jurisprudencial", en Práctica penal: cuaderno jurídico, núm. 93, Sepin editorial jurídica, Madrid, 2018, pp. 13-24 o JORGE BARREIRO, Alberto, "La cláusula concursal del art. 183 ter del Código Penal (*child grooming*)", en *Libro Homenaje al Profesor D. Agustín Jorge Barreiro*, CANCIO MELIÁ, Manuel (coord.), Universidad Autónoma de Madrid, Madrid, 2019, pp. 529-551.

82 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* p. 154.

83 *Idem*, p. 155.

84 Sentencias del TS, 864/2015, 10 de diciembre, ECLI: ES:TS:2015:5809 y 527/2015, 22 de septiembre, ECLI: ES:TS:2015:4179.

rídico protegido en este caso es el patrimonio[85], tanto en la redacción actual del delito, como respecto de la evolución de la misma en las diferentes reformas. Ahora bien, el consenso desaparece su versamos sobre el contenido material del patrimonio en la estafa y, en concreto, en la estafa informática.

Barrio Andrés[86], aporta una visión generalista del concepto indicando que lo protegido es el patrimonio "globalmente considerado".

No obstante, Cáceres Ruiz[87] apuesta por una visión jurídica del patrimonio, en contraposición con la interpretaciones económica y económico-jurídica o mixta[88], esto es así porque interpreta que la estafa protege el valor patrimonio como un "conjunto de derechos patrimoniales de una persona, esto es, aquellos valores económicos que son reconocidos como derechos subjetivos patrimoniales por el derecho objetivo". Esta concepción no está exenta de crítica por su excesiva vaguedad[89].

Por otro lado, Sánchez Bernal[90] defiende una concepción amplia del patrimonio como bien jurídico protegido en el caso de la estafa informática, desde la cual incluye todos los derechos, bienes y relaciones jurídicas de que puede ser titular un sujeto. Galán Muñoz[91] se pronuncia en la misma dirección, argumentando que no es posible concebir una visión subjetiva del patrimonio, sancionando tan solo la frustración de la utilidad deseada por el titular respecto de sus valores económicos, porque se estarían utilizando concepciones civilistas para fundamentar la antijuricidad de la conducta.

Eso sí, un punto en el que confluyen las opiniones de todos los autores es que no son coincidentes las concepciones de patrimonio como bien jurídico protegido del delito de la estafa informática y la estafa tradicional, puesto que lo lesionado en cada caso presenta caracteres distintos, por el hecho de que con la modalidad informática el sujeto activo tiene acceso, en ocasiones, al *dinero contable*[92]. Así las cosas, la concepción amplia o global del patrimonio parece la más acertada para salvar este escollo.

En otro orden de cosas, existen voces que invitan a pensar que el patrimonio no es el único bien jurídico protegido en el caso de la estafa y que existen valores colectivos dignos de tutela penal que derivan de los riesgos creados por la sociedad de la información y, en concreto, de Internet, puesto que el ámbito de afectación de los ciberdelitos no se limita a un territorio concreto, ni a una sola víctima[93].

Así pues, Barrio Andrés[94] adelantaba que en los delitos ciber-económicos podría ser necesaria la protección del orden socioeconómico como bien jurídico colectivo, por la capacidad de estos ilícitos de afectar a un número muy elevado de patrimonios sin necesidad de ajustarse a las reglas espacio-temporales vigentes, dada su condición de ciberdelitos y la sujeción a los caracteres que hemos presentado en el apartado segundo del estudio.

Galán Muñoz, por su parte, proponía la tutela penal de valores colectivos en la estafa informática como bienes jurídicos de naturaleza mediata como complemento a la protección inmediata del patrimonio, de la misma manera en la que los valores colectivos son protegidos en el Derecho penal económico. En concreto, abogaba

85 ALMENAR PINEDA, Francisco, *Ciberdelincuencia*, Editorial Juruá, Oporto, 2018, pp. 137, BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* p. 125 o GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 CP,* Editorial Tirant lo Blanch, Valencia, 2005, p. 240.

86 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* p. 125.

87 CÁCERES RUIZ, Luis, *Delitos contra el patrimonio: aspectos penales y criminológicos. Especial referencia a Badajoz,* Editorial Vision Net, Madrid, 2006, p. 22.

88 La visión económica del patrimonio hace referencia, en opinión de CÁCERES RUIZ, al conjunto de valores económicos de los que dispone una persona y la mixta, por su lado, a esa misma valoración siempre que esté reconocida por el ordenamiento jurídico. Esta última visión permite excluir los bienes poseídos ilegítimamente, por ejemplo.

89 SÁNCHEZ BERNAL, Javier, "El bien jurídico protegido en el delito de estafa informática", en Cuadernos del Tomás, núm. 1, Colegio Mayor Tomás Luis de Victoria, Salamanca, 2009, p. 116.

90 *Idem*, p. 119-121.

91 GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 CP… op. cit.,* pp. 240-243.

92 El concepto de *dinero contable* hace referencia a que el dinero disponible para los criminales en el caso en los que los delitos contra el patrimonio, como la estafa, sean cometidos por Internet no se limita a lo que la víctima disponga en un momento concreto, sino que se amplía a todo lo disponible en el sistema informático o la plataforma informática vulnerada. Lo que habitualmente suele constituir un valor superior.

93 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* p. 121.

94 BARRIO ANDRÉS, Moisés, "La ciberdelincuencia en el Derecho español", en Revista española de las Cortes Generales, núm. 83, Congreso de los Diputados, Madrid, 2011, pp. 292-294 o BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* p. 121.

por la protección del buen funcionamiento de los sistemas informáticos como bien jurídico intermedio[95].

Ambas formulaciones, sin embargo, presentan un claro inconveniente[96], puesto que meras afectaciones de peligro abstracto al bien jurídico colectivo podrían ser idóneas para la consumación del tipo cuando el estado de ejecución de la acción estaría muy alejado de lo que se pretende proteger con la estafa informática.

Además, parecen tensionar especialmente los principios de intervención mínima, exclusiva protección de bienes jurídicos y lesividad. El primer principio se ve comprometido desde el momento en el que resulta suficiente con la referencia al patrimonio para la tipificación de la conducta. El principio de exclusiva protección de bienes jurídicos cuestiona si el correcto funcionamiento de los sistemas de información debería ser un valor protegido penalmente. En tercer lugar, el principio de lesividad exige que el bien jurídico colectivo orden socioeconómico se vea afectado mínimamente, a pesar de tratarse de una afectación de peligro abstracto.

En lo que a la respuesta a los mandatos a nivel internacional se refiere, la reciente Directiva 2019/713/UE[97] se centra en el uso fraudulento de instrumentos de pago, materiales e inmateriales, distintos al efectivo, por lo que no invita a la protección de un bien jurídico de titularidad colectiva de forma paralela.

Tampoco parece idónea aquí una posible referencia a la confidencialidad, integridad y disponibilidad de los sistemas informáticos, puesto que es una mera manipulación informática puntual (o el conocimiento de ciertos datos para el caso del art. 248. 2 c)) lo que lleva al sujeto activo a la comisión de la estafa y no una intromisión en el conjunto del sistema informático. Esto es, la utilización de la red como una herramienta alternativa de comisión de la estafa. Algo que va en consonancia con la ubicación del fraude informático en el art. 8 del Convenio de Budapest[98], dentro del Título dedicado a los delitos informáticos en genérico, sin referencia alguna a la protección de más bienes jurídicos que el propio patrimonio del perjudicado y sin que el delito sean incluido en el Título primero que sí presenta una referencia especial a la seguridad de los sistemas informáticos[99].

En conclusión, la corriente mayoritaria introduce que el bien jurídico protegido por la estafa informática es el patrimonio desde un punto de vista global y amplio, para dar cabida a todos los derechos, bienes y relaciones jurídicas de la víctima. Resulta muy cuestionable la protección de bienes jurídicos de titularidad colectiva relacionados con el orden socioeconómico o los sistemas de información en este ciberdelito.

Si continuamos con el delito de intrusismo informático del art. 197 bis. 1, nos topamos con una figura que presenta una interesante discusión sobre el bien jurídico que protege, entre quienes defienden la protección de los valores tradicionales como la intimidad o el patrimonio y quienes abogan por la tutela de los sistemas de información, principalmente.

Los defensores de la primera opción abogan por que, a pesar de que el intrusismo informático no exija para su consumación el acceso a ningún archivo, dato o programa por parte del autor, sino tan solo la conducta de acceder o facilitar el acceso o mantenerse en un sistema de información sin permiso, el mero hecho de entrometerse en dicho sistema podría crear, por ejemplo, una afectación de peligro abstracto en la intimidad personal y familiar de la víctima[100].

Ahora bien, el hecho de que la conducta estuviese prevista en el art. 197. 3, junto con los delitos de descubrimiento y revelación de secretos, y que la reforma introducida por la Ley Orgánica 1/2015 haya relegado al intrusismo informático al art. 197 bis denota la intención por parte del legislador de establecer una separación, al menos sistemática, entre estos ilícitos[101].

De hecho, el propio Preámbulo de la Ley Orgánica 1/2015 introducía la previsión legal de los delitos relativos a los sistemas informáticos apuntando que "se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal… por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos".

Es más, en opinión de Jorge Barreiro[102] en el caso en el que el bien jurídico protegido por el intrusismo

95 GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 CP… op. cit.,* p. 197.

96 SÁNCHEZ BERNAL, Javier, "El bien jurídico protegido en el delito de estafa informática" … *op. cit.,* p. 119.

97 Unión Europea, *Directiva del Parlamento Europeo y del Consejo, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo,* de 17 de abril de 2019, 2019/713/UE, "DOUE" núm. 123, de 10/05/2019, pp. 18-29.

98 Consejo de Europa, *Convenio sobre la Ciberdelincuencia,* hecho en Budapest, 23 de noviembre de 2001, "BOE" núm. 226, de 17/09/2010, pp. 78.847-78.896.

99 De hecho, el Título I de la Sección dedicada al derecho sustantivo en el Capítulo II del Convenio es denominado: "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos".

100 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.*, p. 91.

101 ALMENAR PINEDA, Francisco, *Ciberdelincuencia… op. cit.*, p. 119.

102 JORGE BARREIRO, Alberto, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Memento Práctico Penal 2016,* MOLINA FERNÁNDEZ, Fernando (coord.), Editorial Francis Lefebvre, Madrid, 2015, p. 1043.

informático sea la intimidad, no sería posible subsumir en este precepto los accesos ilícitos a sistemas informáticos públicos y no tendría sentido la menor pena prevista para el apartado 2 del artículo[103], relativo a las interceptaciones no públicas de datos.

Almenar Pineda[104] coincide con este planteamiento y añade que en ese caso se plantearían problemas de delimitación entre los delitos del 197 bis. 1 y 197. 2 y que precisamente quedarían atípicas las conductas que el legislador pretende tutelar, como los accesos a sistemas de información que, sin ser de ámbito privado, no presentan información pública, como los de la Administración, por ejemplo.

Son estas las razones que llevan a la mayor parte de la doctrina a decantarse por la formulación de un nuevo bien jurídico para este delito en relación con los sistemas informáticos.

Barrio Andrés[105], Hurtado Adrián[106] o Núñez Castaño[107] proponen que el valor protegido por el delito de intrusismo informático es la seguridad de los sistemas informáticos y de las redes.

Visión que comparten Anarte Borrallo y Doval País[108] cuando afirman que el delito afecta a la seguridad del tráfico informatizado y que es este valor que protege por medio de una relación de peligro abstracto. Ahora bien, debido a su ubicación sistemática, estos autores añaden que el delito se trata al fin y al cabo de una protección anticipada de la intimidad.

Por su parte, Muñoz Conde[109] lleva a cabo una pequeña matización de esta postura apuntando que, a pesar de que el delito de intrusismo informático proteja directamente la seguridad de los datos y de los sistemas informáticos, dentro de esta seguridad se tutela también la intimidad y los datos que se encuentren dentro del sistema.

A su vez, teniendo en cuenta también que el art. 197 bis. 1 se encuentra incluido en el título de delitos contra la intimidad, Morales García[110] propone que el bien jurídico protegido sea el domicilio informático, como punto de encuentro de la protección de la seguridad de los sistemas de información y la intimidad y como fenómeno con cierto paralelismo con el delito de allanamiento de morada que, del mismo modo, castiga la entrada indebida y la permanencia en propiedad ajena. Definiéndolo como el derecho a mantener los espacios de actuación en red y su contenido al margen de los accesos no deseados.

El domicilio informático como bien jurídico del delito de intrusismo ha tenido también su reflejo jurisprudencial con la sentencia de la AP de Vizcaya, 90307/2014, de 23 de julio[111] que, aún con la regulación de la reforma de 2010, apuntaba que "lo que se protege es la libertad informática o más exactamente el domicilio informático de una persona, no siendo relevante la naturaleza de los datos contenidos en el sistema informático pudiendo ser de naturaleza personal, familiar, económicos o de otra índole que pertenezcan al ámbito privada de dicha persona".

A modo de resumen de lo planteado hasta el momento, puede introducirse la opinión de Morales Prats[112], quien considera que el valor protegido es la seguridad de las redes y los sistemas informáticos, dado el mandato de los instrumentos internacionales como el Convenio de Budapest y la clasificación que lleva a cabo de las infracciones penales, pero que esta afirmación no es incompatible con la protección del domicilio informático, al ser este uno de los componentes de dicha seguridad, ni con que la tutela de este delito deba centrarse en las vulneraciones de la seguridad que afecten a la intimidad, teniendo en cuenta la ubicación sistemática del tipo.

---

103 Reflexión que comparte TOMÁS-VALIENTE LANUZA, Carmen, "Título X: delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Comentarios al Código Penal,* GÓMEZ TOMILLO, Manuel (dir.), Editorial Lex Nova, Valladolid, 2010, pp. 802-803.

104 ALMENAR PINEDA, Francisco, *Ciberdelincuencia… op. cit.*, p. 122.

105 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.*, p. 92.

106 HURTADO ADRIÁN, Ángel Luis, "Accesos informáticos ilícitos", en *Reforma del Código Penal,* ALBA FIGUERO, Carmen (coord.), Editorial El Derecho, Madrid, 2010, p. 127.

107 NÚÑEZ CASTAÑO, Elena, "Lección XII: delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Nociones Fundamentales de Derecho penal,* GÓMEZ RIVERO, María del Carmen (coord.), Editorial Tecnos, Madrid, 2010, p. 230.

108 ANARTE BORRALLO, Enrique y DOVAL PAÍS, Antonio, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Derecho Penal. Parte especial, volumen 1. La protección penal de los intereses jurídicos personales,* BOIX REIG, Francisco Javier (dir.), Editorial Iustel, Madrid, 2010, p. 455.

109 MUÑOZ CONDE, Francisco y LÓPEZ PEREGRÍN, María del Carmen, *Derecho penal. Parte especial,* Editorial Tirant lo Blanch, Valencia, 2017, p. 277.

110 MORALES GARCÍA, Óscar, "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas", en *La reforma penal de 2010: análisis y comentarios*, QUINTERO OLIVARES, Gonzalo (dir.), Editorial Aranzadi, Pamplona, 2010, pp. 185-186.

111 Sentencia de la AP Vizcaya, 90307/2014, de 23 de julio, ECLI: ES:APBI:2014:1696.

112 MORALES PRATS, Fermín, "Título X: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Comentarios a la parte especial del Derecho penal,* QUINTERO OLIVARES, Gonzalo, (dir.), Editorial Aranzadi, Pamplona, 2011, p. 482.

Sentencia Almenar Pineda[113] aportando que la seguridad de los sistemas informáticos comprende la confidencialidad, integridad y disponibilidad de los sistemas y que es este el bien jurídico protegido por el delito de forma directa, sin obviar que existe protección indirecta respecto de otros valores entre los que se encuentra la intimidad, pero sin ser necesariamente el único. El autor incluye en esta tutela indirecta otros valores como la propiedad, el secreto de empresa o el patrimonio e indica que la protección de los sistemas de información asegura una adelantamiento de las barreras de protección que garantiza una mejor protección de valores básicos de los ciudadanos.

De la Mata Barranco[114] o Carrasco Andrino[115] son también defensores de la confidencialidad, integridad y disponibilidad de los sistemas informáticos como valor protegido por el delito de intrusismo informático, pues contienen información sensible para la intimidad, el honor, el patrimonio, etc. y, además, de estos sistemas informáticos dependen las infraestructuras y los servicios electrónicos de la sociedad de la información.

En el mismo sentido, Rueda Martín[116] se posiciona a favor de la protección de la confidencialidad, integridad y disponibilidad de los sistemas informáticos y aporta argumentos para justificar la necesidad político-criminal de proteger este bien jurídico. En primer lugar, defiende que este valor merece tutela penal, y no solo administrativa, desde el momento en el que tanto nuestra vida privada, como el funcionamiento de las instituciones públicas son claramente dependientes de los sistemas informáticos y contienen cantidades descomunales de información protegida y clave para la garantía del funcionamiento del Estado. En segundo término, apunta que la protección penal de este valor busca el cumplimiento de las exigencias comunitarias en esta materia, derivadas en su mayoría de la Directiva 2013/40/UE[117], relativa a los ataques contra sistemas de información y el Convenio de Ciberdelincuencia del Consejo de Europa de 2001. Siendo esta armonización de legislaciones más necesaria aún desde que la amenaza de los cibercriminales a los sistemas informáticos es global y no afecta a territorios concretos. Por último, añade que la potencialidad multiplicadora que presentan las acciones llevadas a cabo en el ciberespacio convierten en esta clase de ilícitos en dignos de la mayor respuesta por parte del ordenamiento.

No obstante, existen también opiniones como las de Morón Lerma[118] que, a pesar de que identifican la seguridad de los sistemas informáticos como un nuevo valor social, difuso e inmaterial de indudable interés, descartan su identificación como bien jurídico merecedor de tutela penal por contravenir los principios de intervención mínima y proporcionalidad.

Si dirigimos la mirada a cómo se regula y se interpreta este mismo delito en el extranjero, tampoco recabamos una respuesta unívoca sobre el bien jurídico protegido en este delito. Para empezar, podemos mencionar el art. 615 ter del CP italiano donde, en opinión de Fiandaca y Musco[119], se protege la *privacy* informática, como exigencia de que el uso de un sistema informático se produzca en unas condiciones de libertad y autonomía idóneas para permitir la integridad del propio sistema y de sus datos.

En el caso alemán, por su lado, existen voces diferenciadas sobre lo que protege el art. 202a del Strafgesetzbuch (StGB, en adelante). Mientras que parte de la doctrina señala que el bien jurídico se trata del poder de disposición sobre la información contenida en los datos que tiene el titular de los mismos y se proyecta sobre intereses económicos, además de la intimidad, Möhrenschlager[120], por su parte, vincula el delito con la protección del secreto personal, con estrecha relación con la intimidad, pero sin necesidad de que los datos afectados por el acceso ilícito se traten efectivamente de secretos.

Para terminar con las referencias al bien jurídico protegido por el intrusismo informático, cabe mencionar que el propio Convenio de Budapest incluye dentro del Título de delitos enunciado como "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos" las conductas de acceso ilícito, interceptación ilícita, interferencia en datos y sistemas y abuso de dispositivos. No cabe duda de que el hecho de que el propio Título haga referencia

113 ALMENAR PINEDA, Francisco, *Ciberdelincuencia… op. cit.*, pp. 128-129.

114 DE LA MATA BARRANCO, Norberto J. y HERNÁNDEZ DÍAZ, Leyre, "El delito de daños informáticos: una tipificación defectuosa", en Estudios penales y criminológicos, núm. 29, Universidad de Santiago de Compostela, Santiago de Compostela, 2009, p. 328.

115 CARRASCO ANDRINO, María del Mar, "El delito de acceso ilícito a los sistemas informáticos", en *Comentarios a la reforma penal de 2010,* ÁLVAREZ GARCÍA, Francisco José y GONZÁLEZ CUSSAC, José Luis (dir.), Editorial Tirant lo Blanch, Valencia, 2010*,* p. 249.

116 RUEDA MARTÍN, María Ángeles, *La nueva protección de la vida privada y de los sistemas de información en el Código Penal,* Editorial Atelier, Barcelona, 2018*,* pp. 64-65.

117 UNIÓN EUROPEA, *Directiva del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información*, de 12 de agosto de 2013, 2013/40/UE, "DOUE" núm. 218, de 14/08/2013, pp. 8-14.

118 MORÓN LERMA, Esther, *Internet y Derecho penal: hacking y otras conductas ilícitas en la red… op. cit.,* p. 85.

119 FIANDACA, Giovanni y MUSCO, Enzo, *Diritto penale. Parte speciale,* Editorial Nicola Zanichelli, Módena, 2013, pp. 244-245.

120 MÖHRENSCHLAGER, Manfred, "Computer crimes and other crimes against information technology in Germany", en *Information Technology crime: national legislation and international initiatives*, SIEBER, Ulrich (ed.), Editorial Carl Heymanns, Colonia, 1994*,* p. 137.

al valor que pretende proteger es un indicador de que el valor que los ordenamientos jurídico-penales de los estados deben tutelar es la confidencialidad, integridad y disponibilidad de los sistemas informáticos[121]. Algo que confirma el propio Preámbulo del Convenio cuando afirma que busca "prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos".

Ahora bien, a mi juicio, es defendible también la postura que aboga por que este hecho no es relevante, si tenemos en cuenta que el resto de los Títulos de los dedicados al Derecho penal sustantivo en el Convenio no hacen referencia al bien jurídico protegido por las conductas[122], sino que se trata de una clasificación trivial.

En tercer término, el delito de denegación de servicio del art. 264 bis, en virtud de la doctrina mayoritaria, protege el patrimonio de la persona física o jurídica que canalice su actividad por medio del sistema informático cuyo funcionamiento es obstaculizado o interrumpido.

No obstante, Barrio Andrés[123] propone que el bien jurídico tutelado en los delitos de daños informáticos en general es la información contenida en los sistemas informáticos. Argumenta que, hasta la reforma de la Ley Orgánica 5/2010, el tipo exigía un perjuicio económico para su consumación y, por tanto, era defendible su tutela del patrimonio. Esto es así, porque las acciones que especificaba la regulación eran las de destruir, alterar, inutilizar o dañar de cualquier otro modo datos, programas o documentos electrónicos, lo que invitaba a concluir que existía la necesidad de causar un perjuicio patrimonial por reparación o sustitución del objeto material dañado.

Ahora bien, en dicha reforma se amplió su ámbito de aplicación por medio de su tipificación de forma separada y dotando al tipo de autonomía sistemática[124] y la inclusión de las acciones de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles los datos, programas o documentos informáticos, junto con la previsión del DoS. Línea que ha continuado la reforma de la Ley Orgánica 1/2015. Por ello, concluye que el legislador ya no hace referencia al daño patrimonial que pueda causarse a la víctima, sino que se centra en el perjuicio que pueda sufrir por el hecho de no poder utilizar en condiciones óptimas la información que guarda en sus sistemas informáticos.

En la misma línea, la Sentencia de la AP de Madrid, 345/2013, de 3 de junio[125] se pronuncia en un sentido similar al subrayar la separación de la conducta de daños informáticos y su ubicación sistemática propia y afirmar que recoge "un elenco de conductas más amplio, para solventar así todo el debate en relación a su alcance (…) pasando a contemplar prácticamente cualquier injerencia en un programa ajeno (…) conductas todas éstas que no dejan de ser exponente de un funcionamiento anómalo de un sistema informático".

Es más, esta previsión de la formulación de un nuevo bien jurídico para el delito de daños informáticos fue introducida incluso en un momento anterior a la reforma de la Ley Orgánica 5/2010 por parte de De la Mata Barranco y Hernández Díaz[126] cuando afirmaban que los daños informáticos no afectan a bienes materiales o corpóreos, sino a realidades inmateriales de igual o superior valor como los documentos, programas o datos informáticos, además de la posibilidad de uso de un sistema informático. Y que, en consecuencia, podrían barajarse como bienes jurídicos para el delito de daños informáticos e, incluso, el resto de los delitos informáticos la información, la accesibilidad a la información o la accesibilidad y la integridad de la información contenida en los sistemas informáticos.

Si dirigimos la vista hacia los instrumento supranacionales, es de nuevo relevante a efectos del bien jurídico que los arts. 4 y 5 del Convenio de Ciberdelincuencia, que introducen los daños informáticos y la denegación de servicio, se encuentran dentro del Título 1 dedicado a los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, lo que constituye otro argumento para considerar la integridad y la disponibilidad de los sistemas informáticos como bien jurídico protegido por el delito de DoS[127].

121 ALMENAR PINEDA, Francisco, *Ciberdelincuencia… op. cit.*, pp. 127-129 o RUEDA MARTÍN, María Ángeles, *La nueva protección de la vida privada y de los sistemas de información en el Código Penal… op. cit.,* pp. 51-52.

122 Así, el Título 2 se trata de "Delitos informáticos", el Título 3 "Delitos relacionados con el contenido" y el Título 4 "Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines".

123 BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos… op. cit.,* pp. 109-117.

124 Concluimos esto porque antes de la regulación introducida por la Ley Orgánica 5/2010 el delito de daños informáticos se preveía en el art. 264. 2 CP como una modalidad agravada del tipo básico de daños y no como un delito autónomo.

125 Sentencia de la AP de Madrid, 345/2013, de 3 junio, ECLI: ES:APM:2013:8388.

126 DE LA MATA BARRANCO, Norberto J. y HERNÁNDEZ DÍAZ, Leyre, "El delito de daños informáticos: una tipificación defectuosa" … *op. cit.*, pp. 325-333. En este artículo se critica la localización del delito de daños informáticos en el CP anterior a 2010 y se esgrimen los argumentos del bien jurídico protegido y de los mandatos internacionales para argumentar su tipificación separada que, finalmente, llegó con la reforma de la Ley Orgánica 5/2010 y fue confirmada por la Ley Orgánica 1/2015.

127 DE LA MATA BARRANCO, Norberto J. y HERNÁNDEZ DÍAZ, Leyre, "El delito de daños informáticos: una tipificación defectuosa" … *op. cit.*, p. 330.

Por último, los delitos entre los analizados en este trabajo que menor discusión presentan en torno al bien jurídico protegido son los delitos contra la indemnidad sexual de los menores de los arts. 183 bis y ter.

Por su lado, las conductas de abuso sexual de menores del art. 183 bis CP, que se concretan en hacer presenciar a un menor de 16 años actos de carácter sexual o hacerle partícipe en actos de naturaleza sexual fueron incluidas en la reforma de la Ley Orgánica 5/2010 y protegen la indemnidad sexual del menor, entendida como el normal desarrollo y formación de su identidad sexual[128].

No cabe duda de que el hecho de que este delito se pueda cometer por Internet es un elemento clave para la proliferación del injusto y sin duda se trata de uno de los pilares de la decisión delictiva de los ciberagresores. Ahora bien, esto no implica la necesidad de tutela de nuevos bienes jurídicos en el ciberespacio, al menos, en este caso concreto.

Por último, el art. 183 ter de nuestro CP recoge los delitos conocidos como *child grooming* o *sexting* o acercamiento y embaucamiento sexual por medio de las TIC.

El bien jurídico protegido en ambos casos es la indemnidad sexual[129] que en este caso se concreta en "la libertad en formación en el terreno sexual del menor de 16 años a fin de preservar así su bienestar psíquico y normal socialización en esta esfera"[130].

El propio Preámbulo de la Ley Orgánica 5/2010, donde se introdujo este delito por vez primera[131], expone que "resulta indudable que en los casos de delitos sexuales cometidos sobre menores el bien jurídico a proteger adquiere una dimensión especial por el mayor contenido de injusto que presentan estas conductas" y que "mediante las mismas se lesiona no sólo la indemnidad sexual, entendida como el derecho a no verse involucrado en un contexto sexual sin un consentimiento válidamente prestado, sino también la formación y desarrollo de la personalidad y sexualidad del menor"[132].

No obstante, esta nueva dimensión afecta tan solo a la indemnidad sexual de los menores víctimas de estos delito, ya que en los casos de *child grooming* y *sexting* Internet se comporta como una herramienta facilitadora de su comisión.

5. Conclusiones y toma de postura: la previsión de nuevas conductas para la protección de viejos valores

Sentado todo lo anterior, este apartado trata de dar una respuesta completa a la cuestión sobre qué bienes jurídicos se protegen por medio de los ciberdelitos, centrándonos en las cuatro modalidades delictivas de ciberdelincuencia que hemos analizado en este estudio por el hecho de ser las más comunes durante el confinamiento provocado por la crisis sanitaria del COVID-19. Para este fin vamos a llevar a cabo un análisis crítico de los cuatro cibercrímenes atendiendo, claro está, al valor protegido por cada uno de ellos y a cómo influye en los mismos el hecho de que su perpetración tenga lugar en el ciberespacio.

Si comenzamos con el delito de estafa informática, en virtud del examen que hemos completado en el apartado anterior, podemos concluir que la doctrina mayoritaria se decanta por la protección del patrimonio, desde una vertiente global, como bien jurídico protegido. A su vez, existen voces que abogan por la tutela de valores colectivos como el orden socioeconómico o el buen funcionamiento o la confidencialidad, integridad y disponibilidad de los sistemas de información.

A mi juicio, el único valor protegido en el delito de estafa es el patrimonio globalmente considerado. Tal y como hemos avanzado antes, la previsión de valores colectivos en este delito podría llevar a sinsentidos como la criminalización de conductas que tan solo revistan un ataque de peligro abstracto a estos bienes jurídicos. Además, su tutela pone en tela de juicio principios penales fundamentales como el de intervención mínima, exclusiva protección de bienes jurídicos y lesividad y los mandatos internacionales, con el Convenio de Budapest como principal exponente, no catalogan la estafa informática como delito susceptible de afectar a los sistemas de información.

En concreto, resulta una quimera la posible protección del orden socioeconómico por medio de un delito que, a pesar de que puedan llevarse a cabo conductas de forma simultánea gracias a las bondades de Internet, no deja de afectar a un solo patrimonio por cada acción y solo es susceptible de afectar a los patrimonios cuyos titulares hayan introducido valores relacionados con el mismo en la red como, por ejemplo, las claves de la banca *online*.

128 VILLACAMPA ESTIARTE, Carolina, "El delito de *online child grooming* o propuesta sexual telemática a menores" … *op. cit.*, pp. 156-158.

129 *Idem,* pp. 169-183.

130 GÓRRIZ ROYO, Elena, "*Online child grooming* en Derecho penal español", en InDret: revista para el análisis del Derecho, núm. 2, Universidad Pompeu Fabra, Barcelona, 2016, pp. 16-17.

131 La Ley Orgánica 5/2010 preveía el delito de *child grooming* en el art. 183 bis. Sin embargo, tras la reforma introducida por la Ley Orgánica 1/2015, este delito está previsto en el art. 183 ter, como se desprende de nuestro análisis.

132 ALMENAR PINEDA, Francisco, *Ciberdelincuencia… op. cit.*, pp. 133-134.

Tampoco comparto una posible protección de los sistemas de información como bien jurídico por varias razones.

La primera es que dependiendo de la modalidad de estafa informática que analicemos el posible nivel de afectación a los sistemas de información, aunque mínimo en todo caso, será muy diferente. En los casos de estafa mecánica, donde lo violentado es el ordenador del usuario estafado y la manipulación se basa en redireccionar a la víctima a una página fraudulenta en lugar de la que quería acceder, no existe intromisión en ningún sistema informático. Por otro lado, en los supuestos de estafa sociológica, podemos encontrarnos casos con afectaciones superiores e inferiores de estos sistemas. En un caso como los que hemos identificado en el apartado primero, propios de los tiempos de confinamiento, como el de la falta de entrega del producto adquirido en una compra por Internet no existe afectación a ningún sistema informático. Sin embargo, en los supuestos como sobre los que alertaba la OMS, donde los cibercriminales buscan hacerse con las claves de sus víctimas, es posible afirmar que sí se violenta la seguridad y la confidencialidad de un sistema de información. Por esto, no es posible afirmar que un delito protege un bien jurídico que en ciertos casos queda impune y, en otros, se lesiona o se pone en peligro de forma manifiesta.

En segundo lugar, en estos casos en los que un delito de estafa informática es susceptible de afectar a un sistema de información sigue siendo discutible si este hecho es suficiente como para considerarlo un bien jurídico protegido, teniendo en cuenta los principios de intervención mínima y exclusiva protección de bienes jurídicos, que nos recuerda que tan solo debemos proteger penalmente los valores indispensables para el desarrollo personal y en sociedad de los ciudadanos. De hecho, en estos casos el ciberdelincuente tan solo afectará a una parte mínima del sistema de información en cuestión: la relativa a un cliente de una entidad bancaria, por ejemplo, dentro de un sistema con miles de parcelas dedicadas a cada cliente.

Por último, si algo es latente es que la intención del cibercriminal en todos los casos de estafa informática es el enriquecimiento personal, la obtención de un beneficio, siendo prueba de esto el ánimo de lucro necesario para la apreciación del tipo. Así pues, es posible concluir que el autor de un delito de estafa informática no tiene interés en violentar o no un sistema de información y que, en cualquier caso, tan solo dará este paso si en última instancia esto le lleva a conseguir el rédito económico buscado. Por lo que, en la misma línea que el uso de la red para la consumación del delito, el hecho de afectar a un sistema de información es, en todo caso, una herramienta o medio para la consecución del fin último de lesionar el patrimonio de su víctima.

En el delito de intrusismo informático, por su parte, la doctrina mayoritaria coincide en defender la seguridad o la confidencialidad, integridad y disponibilidad de los sistemas informáticos como bien jurídico protegido.

A mi parecer, sin embargo, esta posición debe ser rechazada por dos razones fundamentales. Para empezar, la normativa internacional no da una respuesta inequívoca a esta cuestión en favor de la protección de este valor, tal y como afirman los defensores de esta idea. Si bien es cierto que el delito de intrusismo informático suele catalogarse como un delito contra los sistema de información, tal y como hemos expuesto en el apartado anterior, estas clasificaciones que se reflejan en los instrumentos internacionales no separan los distintos ciberdelitos por los valores que protegen, sino que se trata de clasificaciones basadas en criterios cambiantes dependiendo del instrumento e, incluso, dentro de una misma norma. Además, los preámbulos y exposiciones de motivos, también recogidas en el apartado que precede a este, no indican que el delito de intrusismo informático protege los sistemas informáticos de forma explícita, sino que simplemente buscan la separación con los delitos que protegen la intimidad, por el hecho de que no siempre protegen este valor y, de hacerlo, lo protegen por medio de la figura del peligro abstracto.

Ahora bien, el principal argumento es que los sistemas de información son un elemento de demasiada abstracción como para ser protegidos por el aparato penal del Estado y no son más que una ficción virtual que contiene otros valores fundamentales, como el patrimonio y la intimidad, generalmente. Es decir, del mismo modo en que la red juega como medio de comisión de ciberdelitos en el ciberespacio, los sistemas de información son una herramienta para guardar y custodiar valores tradicionales en el espacio virtual.

Prueba de ello es que los cibercriminales no persiguen el simple acceso o el mantenimiento en el sistema de información, sino que buscan obtener un rédito económico del mismo (como en los casos de estafas informáticas o ciber secuestros, entre otros) o buscan vulnerar la intimidad de alguien. En los casos en los que el delito que apreciemos sea el de intrusismo informático, porque los hechos tan solo sean subsumibles en el tipo del 197 bis. 1, observaremos una afectación de peligro abstracto en los bienes jurídicos patrimonio o intimidad que, a mi juicio, son los bienes jurídicos protegidos en este delito, según el caso. En el momento en el que el desvalor de resultado avance del peligro abstracto a la lesión, podrán entrar en juego los delitos contra el patrimonio como el hurto o la estafa y los delitos contra la intimidad como los delitos de descubrimiento y revelación de secretos.

Como hemos visto, existen también voces, tanto doctrinales como jurisprudenciales, que abogan por el do-

micilio informático como valor protegido por el delito. A mi parecer, esto no hace más que confirmar la teoría de que la intimidad es el verdadero valor protegido en estos casos. Esto es así, porque existe un claro paralelismo entre el delito de allanamiento de morada, que castiga también la entrada o el mantenimiento en una propiedad ajena, y el delito de intrusismo informático y, al fin y al cabo, lo que están reconociendo los defensores de esta idea es que, del mismo modo que la entrada en el domicilio físico de una persona se traduce en un atentado contra su intimidad por la gran cantidad de información que este hecho puede proporcionar a su autor, la entrada en el domicilio informático de alguien conlleva una afectación de nivel similar en ese mismo bien jurídico. Más aún si tenemos en cuenta que cada vez introducimos más valores en el ciberespacio y que este es un fenómeno que, tal y como hemos concluido aquí, se ha visto potenciado por el confinamiento provocado por el COVID-19.

En tercer lugar, el delito de denegación de servicio protege el patrimonio si seguimos la corriente mayoritaria, la cual lo cataloga como un delito de daños informáticos.

En este trabajo se comparte esta opinión y se rechazan los planteamientos que presentan la información y los sistema de información como valor protegido por el hecho de que de nuevo se tratan de conceptos inmateriales de carácter virtual cuya traslación en el mundo de real se trata, en este caso, del patrimonio, en el sentido en el que una denegación de servicio causa un perjuicio económico al titular del sistema de información atacado.

Como ejemplo ilustrativo podemos traer a colación el ataque al Hospital Universitario de Brno que ha tenido lugar durante la crisis del COVID-19 y que ha derivado en un perjuicio económico a la administración encargada de su gestión, puesto que han tenido que trasladar a los enfermos a otros centros médicos y se han visto obligados a reprogramar intervenciones no urgentes. Es decir, ha tenido consecuencias en el mundo real que pueden traducirse, en última instancia, en la necesidad de emplear más recursos económicos para llevar a cabo el mismo trabajo, además de los obvios costes de reparación del sistema informático. En el ciberespacio, por su lado, ha derivado en la imposibilidad de acceso a cierta información durante un tiempo determinado, pero considero que este es un valor virtual intermedio que no presenta la suficiente gravedad para poder ser protegido penalmente, en virtud del principio de intervención mínima.

En último término, no existen dudas sobre que los ciberdelitos contra la indemnidad sexual de los menores protegen su libertad e indemnidad sexual, por mucho de que sean cometidos en la red.

En este caso, Internet funciona como un medio de comunicación anónimo, instantáneo y con separación espacial que resulta idóneo para actuar como medio de comisión de estas infracciones, pero sin que se vean comprometidos valores cibernéticos en ninguna de sus modalidades.

Así las cosas, en general, es posible plantear dos niveles de afectación a los sistemas de información, dependiendo de qué función cumpla el uso de Internet en la perpetración de cada ciberdelito. A pesar de que, en cualquier caso, nunca se trate del bien jurídico protegido.

El primer nivel es el mínimo y corresponde con los casos en los que la red es un mero medio de comunicación entre víctima y victimario: estos son los casos de la estafa informática cuando la conducta es la de no enviar el producto prometido o enviarlo con condiciones distintas a las pactadas y de los ciberdelitos contra la indemnidad sexual de los menores. Es latente que el papel de Internet aquí es el de servir de canal entre los dos sujetos y que el autor del delito se aprovecha de los caracteres criminológicos del ciberespacio que hemos presentado en el apartado segundo para facilitar su ataque a los valores patrimonio e indemnidad sexual, según el caso.

El segundo nivel, por su parte, presenta una afectación superior a los sistemas de información, por el hecho de que el ciberdelincuente accede al menos a una parte del mismo: estos son los casos de las estafas informáticas en las que el delincuente se hace con información privilegiada, los casos de estafa mecánica, los casos de intrusismo informático y de denegación de servicio. Aquí el sistema informático en cuestión se ve alterada de alguna forma, pero esto no significa que se trate del bien jurídico protegido, sino que el victimario utiliza la intromisión en dicho espacio virtual para lograr un beneficio económico (o causar un perjuicio patrimonial) o una afectación a la intimidad ajena.

En conclusión, de todo lo expuesto en este estudio podemos concluir que los ciberdelitos analizados, los más comunes durante el confinamiento, protegen los valores tradicionales patrimonio e intimidad.

Además de todos los argumentos aportados para construir esta afirmación, este hecho va en consonancia con los principios penales de intervención mínima, exclusiva protección de bienes jurídicos y lesividad. Observamos la intervención mínima porque el Derecho penal debe traducirse en su mínima expresión siempre que cumpla con las exigencias político-criminales de lucha contra el delito y, en este caso, estamos previendo las mismas conductas sin necesidad de tutelar nuevos valores con la expresión más gravosa la de potestad sancionadora estatal. Cumplimos también las exigencias de los principios de exclusiva protección de bienes jurídicos y lesividad, porque la creación de nuevos va-

lores penalmente relevantes traería consigo, necesariamente, la justificación de por qué consideramos que los sistemas de información deben protegerse por medio del Derecho penal y, en el caso de que estos argumentos fuesen convincentes, haría falta aún la constatación de que el bien jurídico de los sistemas de información percibe una lesividad suficiente como para merecer una tutela penal. Algo difícil de probar teniendo en cuenta de que los ataques a los sistemas de información que hemos descrito aquí afectan, generalmente, a una pequeña parte del mismo.

Si algo es latente, ahora bien, es que el confinamiento provocado por la crisis sanitaria del COVID-19 no ha venido más que a reafirmar esta teoría. Como hemos comentado en varias ocasiones en este estudio, se trata de un evento que ha potenciado el fenómeno según el cual los ciudadanos introducimos cada vez más valores en el ciberespacio y el hecho de que hayamos trasladado una parcela mayor de nuestras vidas a la red ha derivado en que la criminalidad se haya desplazado del espacio delictivo tradicional al mundo virtual.

Pero, ¿por qué han decidido los criminales trasladar su actividad a Internet? ¿Qué valores o intereses están buscando los ciberdelincuentes en el ciberespacio? Los mismos valores que perseguían en el mundo real, antes de la irrupción de Internet y antes del confinamiento. En otras palabras, la principal razón por la que la actividad delictiva se ha desplazado a la red es que es allí donde se encuentran en estos momentos los valores tradicionales como la intimidad y el patrimonio, lo que prueba que son estos los valores que debemos proteger en el ciberespacio y no los relativos a los sistemas de información, que no son más que una ficción virtual que, en mayor o menor medida, funcionan como un medio o herramienta para poder trasladar los bienes jurídicos tradicionales al ciberespacio.

FUENTES CONSULTADAS

1. Libros

ABOSO, Gustavo Eduardo y ZAPATA, María Florencia, *Cibercriminalidad y Derecho penal: la información y los sistemas informáticos como nuevo paradigma del Derecho penal. Análisis doctrinario, jurisprudencial y derecho comparado de los denominados "delitos informáticos",* Editorial B de F Montevideo, Uruguay, 2006.

ALMENAR PINEDA, Francisco, *Ciberdelincuencia*, Editorial Juruá, Oporto, 2018.

BARRIO ANDRÉS, Moisés, *Ciberdelitos: amenazas criminales del ciberespacio,* Editorial Reus, Madrid, 2017.

BARRIO ANDRÉS, Moisés, *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos,* Editorial Wolters Kluwer, Madrid, 2018.

BARRIO ANDRÉS, Moisés, *Derecho público y propiedad intelectual: su protección en Internet,* Editorial Reus, Madrid, 2017.

BERGAUER, Christian, *Das materielle Computerstrafrecht,* Editorial Jan Sramek, Viena, 2016.

BUTTON, Mark y CROSS, Cassandra, *Cyber frauds, scams and their victims,* Editorial Routledge, Nueva York, 2017.

CÁCERES RUIZ, Luis, *Delitos contra el patrimonio: aspectos penales y criminológicos. Especial referencia a Badajoz,* Editorial Vision Net, Madrid, 2006.

CRUZ DE PABLO, José Antonio, *Derecho penal y nuevas tecnologías: aspectos sustantivos,* Editorial Grupo Difusión, Madrid, 2006.

DAVARA FERNÁNDEZ DE MARCOS, Elena y DAVARA FERNÁNDEZ DE MARCOS, Laura, *Delitos informáticos,* Editorial Thomson Reuters Aranzadi, Pamplona, 2017.

DAVARA RODRÍGUEZ, Miguel Ángel, *Manual de Derecho informático,* Editorial Aranzadi Thomson Reuters, Pamplona, 2015.

DE PABLO SERRANO, Alejandro, *Honor, injurias y calumnias. Los delitos contra el honor en el Derecho histórico y en el Derecho vigente español,* Editorial Tirant lo Blanch, Valencia, 2018.

FERNÁNDEZ DÍAZ, Carmen Rocío, *El Derecho penal frente al espionaje empresarial,* Editorial Tirant lo Blanch, Valencia, 2018.

FERNÁNDEZ TERUELO, Javier Gustavo, *Cibercrimen: los delitos cometidos a través de Internet,* Editorial Constitutio Criminalis Carolina, Madrid, 2007.

FIANDACA, Giovanni y MUSCO, Enzo, *Diritto penale. Parte speciale,* Editorial Nicola Zanichelli, Módena, 2013.

FISCHER, Thomas, *Computer-Kriminalität,* Editorial Paul Haupt, Berna, 1979, p. 14.

GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 CP,* Editorial Tirant lo Blanch, Valencia, 2005.

GERCKE, Marco y BRUNST, Phillip W., *Praxishandbuch Internetstrafrecht,* Editorial W. Kohlhammer, Stuttgart, 2009.

GILLESPIE, Alisdair A., *Cybercrime: key issues and debates,* Editorial Routledge, London, 2019.

HILGENDORF, Eric y VALERIUS, Brian, *Computer- und Internetstrafrecht,* Editorial Springer, Berlin, 2012.

KRISCHKER, Sven, *Das Internetstrafrecht vor neuen Herausforderungen,* Editorial Logos, Berlin, 2014.

MATA Y MARTÍN, Ricardo M., *Delincuencia informática y Derecho penal,* Editorial Edisofer, Madrid, 2001.

MIRÓ LLINARES, Fernando, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio,* Editorial Marcial Pons, Madrid, 2012.

MORÓN LERMA, Esther, *Internet y Derecho penal: hacking y otras conductas ilícitas en la red,* Editorial Aranzadi, Pamplona, 2002.

MUÑOZ CONDE, Francisco y LÓPEZ PEREGRÍN, María del Carmen, *Derecho penal. Parte especial,* Editorial Tirant lo Blanch, Valencia, 2017.

POWELL, Anastasia y HENRY, Nicola, *Sexual violence in a digital age,* Editorial Macmillan, Londres, 2017.

QUERALT JIMÉNEZ, Joan J., *Derecho penal español. Parte especial,* Editorial Atelier, Barcelona, 2010.

ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos,* Editorial Comares, Granada, 2002.

RUEDA MARTÍN, María Ángeles, *La nueva protección de la vida privada y de los sistemas de información en el Código Penal,* Editorial Atelier, Barcelona, 2018.

SIEBER, Ulrich, *Computerkriminalität und Strafrecht,* Editorial Carl Heymanns, Colonia, 1977.

VELASCO NÚÑEZ, Eloy, *Delitos cometidos a través de Internet: cuestiones procesales,* Editorial La Ley, Madrid, 2010.

WEIMANN, Gabriel, *Terrorism in cyberspace,* Editorial Columbia University Press, Nueva York, 2015.

WERNERT, Manfred, *Internetkriminalität,* Editorial Boorberg, Stuttgart, 2017.

2. Capítulos de libro

ANARTE BORRALLO, Enrique y DOVAL PAÍS, Antonio, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Derecho Penal. Parte especial, volumen 1. La protección penal de los intereses jurídicos personales,* BOIX REIG, Francisco Javier (dir.), Editorial Iustel, Madrid, 2010.

CARRASCO ANDRINO, María del Mar, "El delito de acceso ilícito a los sistemas informáticos", en *Comentarios a la reforma penal de 2010,* ÁLVAREZ GARCÍA, Francisco José y GONZÁLEZ CUSSAC, José Luis (dir.), Editorial Tirant lo Blanch, Valencia, 2010.

DE LA CUESTA ARZAMENDI, José Luis y PÉREZ MACHÍO, Ana Isabel, "Ciberdelincuentes y cibervíctimas", en *Derecho penal informático*, DE LA CUESTA ARZAMENDI, José Luis (dir.), Editorial Civitas-Thomson Reuters, Pamplona, 2010.

DE LA CUESTA ARZAMENDI, José Luis, PÉREZ MACHÍO, Ana Isabel y SAN JUAN GUILLÉN, César, "Aproximaciones criminológicas a la realidad de los ciberdelitos", en *Derecho penal informático*, DE LA CUESTA ARZAMENDI, José Luis (dir.), Editorial Civitas-Thomson Reuters, Pamplona, 2010.

DE LA MATA BARRANCO, Norberto J. y HERNÁNDEZ DÍAZ, Leyre, "Los delitos vinculados a la informática en el Derecho penal español", en *Derecho penal informático*, DE LA CUESTA ARZAMENDI, José Luis (dir.), Editorial Civitas-Thomson Reuters, Pamplona, 2010.

DE URBANO CASTRILLO, Eduardo, "Los delitos informáticos tras la reforma del CP de 2010", en *Delincuencia informática: tiempos de cautela y amparo,* DE URBANO CASTRILLO, Eduardo (coord.), Editorial Thomson Reuters Aranzadi, Pamplona, 2012.

ESER, Albin, "Internet und internationales Strafrecht", en *Rechtsfragen des Internet und der Informationsgesellschaft,* LEIPOLD, Dieter (coord.), Editorial C. F. Müller, Heidelberg, 2002.

FARALDO-CABANA, Patricia, "Defraudación de telecomunicaciones y uso no consentido de terminales de telecomunicación: dificultades de delimitación entre los arts. 255 y 256 CP", en *Un Derecho penal comprometido: libro homenaje al Prof. Dr. Gerardo Landrove Díaz,* NÚÑEZ PAZ, Miguel Ángel (coord.), Editorial Tirant lo Blanch, Valencia, 2011.

FLOR, Roberto, "La legge penale nello spazio, fra evoluzione tecnológica e difficoltà applicative", en *Cybercrime,* CADOPPI, Alberto, CANESTRARI, Stefano, MANNA, Adelmo y PAPA, Michele (coord.), Editorial Utet Giuridica, Milán, 2019.

GARCÍA ALBERO, Ramón, "Pornografía infantil y reforma penal", en *Delitos contra la libertad e indemnidad sexual de los menores,* VILLACAMPA ESTIARTE, Carolina (coord.), Editorial Thomson Reuters Aranzadi, Pamplona, 2015.

HURTADO ADRIÁN, Ángel Luis, "Accesos informáticos ilícitos", en *Reforma del Código Penal,* ALBA FIGUERO, Carmen (coord.), Editorial El Derecho, Madrid, 2010.

JORGE BARREIRO, Alberto, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Memento Práctico Penal 2016,* MOLINA FERNÁNDEZ, Fernando (coord.), Editorial Francis Lefebvre, Madrid, 2015.

JORGE BARREIRO, Alberto, "La cláusula concursal del art. 183 ter del Código Penal (*child grooming*)", en *Libro Homenaje al Profesor D. Agustín Jorge Barreiro*, CANCIO MELIÁ, Manuel (coord.), Universidad Autónoma de Madrid, Madrid, 2019.

LLOBET ANGLÍ, Mariona, "Delitos contra el orden público", en *Lecciones de Derecho penal. Parte especial,* SILVA SÁNCHEZ, Jesús-María (coord.), Editorial Atelier, Barcelona, 2015.

MÖHRENSCHLAGER, Manfred, "Computer crimes and other crimes against information technology in Germany", en *Information Technology crime: national legislation and international initiatives*, SIEBER, Ulrich (ed.), Editorial Carl Heymanns, Colonia, 1994.

MORALES GARCÍA, Óscar, "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas", en *La reforma penal de 2010: análisis y comentarios*, QUINTERO OLIVARES, Gonzalo (dir.), Editorial Aranzadi, Pamplona, 2010.

MORALES PRATS, Fermín, "Título X: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Comentarios a la parte especial del Derecho penal,* QUINTERO OLIVARES, Gonzalo, (dir.), Editorial Aranzadi, Pamplona, 2011.

NÚÑEZ CASTAÑO, Elena, "Lección XII: delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Nociones Fundamentales de Derecho penal,* GÓMEZ RIVERO, María del Carmen (coord.), Editorial Tecnos, Madrid, 2010.

OWEN, Tim, "The Problems of Virtual Criminology", en *New perspectives on cybercrime,* OWEN, Tim, NOBLE, Wayne y SPEED, Faye Christabel (coord.), Editorial Palgrave MacMillan, Preston, 2017.

RAGUÉS I VALLÈS, Ramón, "Delitos contra la libertad", en *Lecciones de Derecho penal. Parte especial,* SILVA SÁNCHEZ, Jesús-María (coord.), Editorial Atelier, Barcelona, 2015.

ROMEO CASABONA, Carlos María, "De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* ROMEO CASABONA, Carlos María (coord.), Editorial Comares, Granada, 2006.

SIEBER, Ulrich, "Criminalidad informática: peligro y prevención", en *Delincuencia informática,* MIR PUIG, Santiago (dir.), Editorial PPU, Barcelona, 1992.

TOMÁS-VALIENTE LANUZA, Carmen, "Título X: delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Comentarios al Código Penal,* GÓMEZ TOMILLO, Manuel (dir.), Editorial Lex Nova, Valladolid, 2010.

VILLACAMPA ESTIARTE, Carolina, "El delito de *online child grooming* o propuesta sexual telemática a menores", en *Delitos contra la libertad e indemnidad sexual de los menores,* VILLACAMPA ESTIARTE, Carolina (coord.), Editorial Thomson Reuters Aranzadi, Pamplona, 2015.

VILLACAMPA ESTIARTE, Carolina y PUJOLS PÉREZ, Alejandra, "El delito de *stalking* en el Código Penal español", en Stalking: *análisis jurídico, fenomenológico y victimológico,* VILLACAMPA ESTIARTE, Carolina (coord.), Editorial Thomson Reuters Aranzadi, Pamplona, 2018.

3. Artículos de revista

ALASTUEY DOBÓN, M. Carmen, "Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial", en Informática y Derecho: revista iberoamericana de Derecho informático, núm. 4, UNED, Madrid, 1994.

ANARTE BORRALLO, Enrique, "Incidencia de las nuevas tecnologías en el sistema penal: aproximación al Derecho penal en la sociedad de la información", en Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento, núm. 1, Universidad de Huelva, Huelva, 2001.

ASENCIO GUILLÉN, Antonio, "El ciberespacio como sistema y entorno social: una propuesta teórica a partir de Niklas Luhmann", en Comunicación y Sociedad, vol. 31, núm. 1, Universidad de Navarra, Pamplona, 2018.

BARRIO ANDRÉS, Moisés, "La ciberdelincuencia en el Derecho español", en Revista española de las Cortes Generales, núm. 83, Congreso de los Diputados, Madrid, 2011.

DE LA MATA BARRANCO, Norberto J. y HERNÁNDEZ DÍAZ, Leyre, "El delito de daños informáticos: una tipificación defectuosa", en Estudios penales y criminológicos, núm. 29, Universidad de Santiago de Compostela, Santiago de Compostela, 2009.

GÓRRIZ ROYO, Elena, "*Online child grooming* en Derecho penal español", en InDret: revista para el análisis del Derecho, núm. 2, Universidad Pompeu Fabra, Barcelona, 2016.

HERNÁNDEZ MORENO, Alberto, "Ciberseguridad y confianza en el ámbito digital", en Información Comercial Española, ICE: revista de economía, núm. 897, Ministerio de Economía, Industria y Competitividad, Madrid, 2017.

HILGENDORF, Eric, "Die strafrechtliche Regulierung des Internet als Aufgabe eines modernen Technikrechts", en Juristen Zeitung, núm. 17, Mohr Siebeck, Tubinga, 2012.

LESSIG, Lawrence, "Las leyes del ciberespacio", en THEMIS: revista de Derecho, Asociación civil THEMIS, Perú, 2002.

MALDONADO GUZMÁN, Diego J., "El mal denominado delito de *grooming online* como forma de violencia sexual contra menores. Problemas jurídicos y aspectos criminológicos", en Revista electrónica de estudios penales y de la seguridad, núm. extra 5, Editorial Jurídica Continental, Costa Rica, 2019.

MIRÓ LLINARES, Fernando, "La respuesta penal al ciberfraude: especial atención a la responsabilidad de los muleros del *phishing*", en Revista electrónica de ciencia penal y criminología, núm. 15, Universidad de Granada, Granada, 2013.

MOLINA MANSILLA, Carmen, "Última doctrina jurisprudencial en torno al delito de *child grooming*: aspectos más significativos de las reglas concursales", en La ley penal: revista de Derecho penal, procesal y penitenciario, núm. 136, Wolters Kluwer, Madrid, 2019.

MORENO VERDEJO, Jaime, "Algunas cuestiones acerca de la estafa informática y uso de tarjetas (Incidencia del Anteproyecto de 2006 de reforma del Código Penal", en Cuadernos penales José María Lidón, núm. 4, Universidad de Deusto, Bilbao, 2007.

ORTEGA CALDERÓN, Juan Luis, "La aplicación de las reglas concursales con ocasión del delito de *child grooming*: análisis de la evolución jurisprudencial", en Práctica penal: cuaderno jurídico, núm. 93, Sepin editorial jurídica, Madrid, 2018.

REY HUIDOBRO, Luis Fernando, "La estafa informática: relevancia penal del *phishing* y el *pharming*", en La ley penal: revista de Derecho penal, procesal y penitenciario, núm. 101, Wolters Kluwer, Madrid, 2013.

REYNA ALFARO, Luis Miguel, "Aproximaciones criminológicas al delito informático", en Capítulo Criminológico, vol. 31, núm. 4, Universidad del Zulia, Venezuela, 2003.

SÁNCHEZ BERNAL, Javier, "El bien jurídico protegido en el delito de estafa informática", en Cuadernos del Tomás, núm. 1, Colegio Mayor Tomás Luis de Victoria, Salamanca, 2009.

SÁNCHEZ ESCRIBANO, María Isabel Montserrat, "Propuesta para la interpretación de la cláusula concursal recogida en el art. 183 ter 1 (delito de *online child* grooming)", en Revista de Derecho, Empresa y Sociedad (REDS), núm. 12, Dykinson, Madrid, 2018.

VALIENTE GARCÍA, Francisco Javier, "Comunidades virtuales en el ciberespacio", en Doxa comunicación: revista interdisciplinar de estudios de comunicación y ciencias sociales, núm. 2, Universidad San Pablo-CEU, Madrid, 2004.

VIOTA MAESTRE, Manuel, "Problemas relacionados con la investigación de los denominados delitos informáticos (ámbito espacial y temporal, participación criminal y otros)", en Cuadernos penales José María Lidón, núm. 4, Universidad de Deusto, Bilbao, 2007.

4. Jurisprudencia

Sentencia del Tribunal Supremo, 864/2015, 10 de diciembre, ECLI: ES:TS:2015:5809.

Sentencia del Tribunal Supremo, 527/2015, 22 de septiembre, ECLI: ES:TS:2015:4179.

Sentencia de la AP Vizcaya, 90307/2014, de 23 de julio, ECLI: ES:APBI:2014:1696.

Sentencia de la AP de Madrid, 345/2013, de 3 junio, ECLI: ES:APM:2013:8388.

5. Legislación nacional

ESPAÑA, *Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*, "BOE" núm. 77, de 31/03/2015, pp. 27.061-27.176.

ESPAÑA, *Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal,* "BOE" núm. 152, de 23/06/2010, pp. 54.811-54.883.

ESPAÑA, *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*, "BOE" núm. 281, de 24/11/1995.

6. Instrumentos supranacionales

CONSEJO DE EUROPA, *Convenio sobre la Ciberdelincuencia,* hecho en Budapest, 23 de noviembre de

2001, "BOE" núm. 226, de 17/09/2010, pp. 78.847-78.896.

UNIÓN EUROPEA, *Directiva del Parlamento Europeo y del Consejo, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo,* de 17 de abril de 2019, 2019/713/UE, "DOUE" núm. 123, de 10/05/2019, pp. 18-29.

UNIÓN EUROPEA, *Directiva del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información*, de 12 de agosto de 2013, 2013/40/UE, "DOUE" núm. 218, de 14/08/2013, pp. 8-14.

UNIÓN EUROPEA, *Directiva del Parlamento Europeo y del Consejo, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil,* de 13 de diciembre de 2011, 2011/93/UE, "DOUE" núm. 335, de 17/12/2011, pp. 1-14.

UNIÓN EUROPEA, *Reglamento 2016/425/UE del Parlamento Europeo y del Consejo, relativo a los equipos de protección individual*, de 9 de marzo de 2016, DOUE núm. 81, de 31 de marzo de 2016, pp. 51-98.

7. Documentos difundidos por Internet

ABC, *El uso de redes sociales en España aumenta un 55% en la pandemia del coronavirus,* https://www.abc.es/tecnologia/redes/abci-redes-sociales-espana-aumenta-55-por-ciento-pandemia-coronavirus-202003241257_noticia.html?ref=https%3A%2F%2Fwww.google.com%2F (última consulta: 14 de mayo de 2020), 2 de abril de 2020.

ABC, *Un ciberataque bloquea la actividad en un hospital checo en plena pandemia del Coronavirus,* https://www.abc.es/tecnologia/redes/abci-ciberataque-bloquea-actividad-hospital-checo-plena-pandemia-coronavirus-202003141652_noticia.html (última consulta: 14 de mayo de 2020), 14 de marzo de 2020.

ARA, *El COVID-19 desploma els delictes presencials,* https://www.ara.cat/societat/coronavirus-covid-19-delictes-presencials_0_2425557497.html?utm_medium=social&utm_source=twitter&utm_campaign=ara (última consulta: 14 de mayo de 2020), 29 de marzo de 2020.

BUIL-GIL, David, LORD, Nicholas, BARRETT, Emma, DRESNER, Daniel y HIGGINS, Brian, "Profiting from pandemics: COVID-19, changing routines and cyber crimes", en Blog Digital Futures, Universidad de Manchester, http://blog.policy.manchester.ac.uk/digital-futures/2020/03/profiting-from-pandemics-covid-19-changing-routines-and-cyber-crimes/(última consulta: 14 de mayo de 2020), 19 de marzo de 2020.

CAMPOY TORRENTE, Pedro, "¿Flu-ctuaciones delictivas? Los posibles efectos del COVID-19 en la criminalidad", en Blog de la REIC: revista española de investigación criminológica, SEIC: sociedad española de investigación criminológica, https://criminologia.net/2020/03/23/flu-ctuaciones-delictivas-los-posibles-efectos-del-covid-19-en-la-criminalidad/(última consulta: 14 de mayo de 2020), 23 de marzo de 2020.

DEIA, *El confinamiento por el Coronavirus reduce los delitos en Bilbao casi un 90%,* https://www.deia.eus/actualidad/sociedad/2020/04/07/confinamiento-reduce-delitos-bilbao-90/1030007.html (última consulta: 14 de mayo de 2020), 7 de abril de 2020.

DIARIO SUR, *El teletrabajo se dispara para mantener el pulso de la actividad,* https://www.diariosur.es/andalucia/teletrabajo-dispara-mantener-20200403184055nt.html?ref=https:%2F%2Fwww.google.com%2F (última consulta: 14 de mayo de 2020), 3 de abril de 2020.

EL CONFIDENCIAL, *La crisis del COVID-19 que nadie previó: el "e-commerce" colapsa al enviar sus pedidos,* https://www.elconfidencial.com/tecnologia/2020-03-30/coronavirus-ecommerce-pedidos-stock-covid19_2521043/(última consulta: 14 de mayo de 2020), 30 de marzo de 2020.

EUROPA PRESS, *Las videollamadas, los mensajes de voz y el consumo de noticias en directo crecen con las medidas de distancia social,* https://www.europapress.es/portaltic/internet/noticia-videollamadas-mensajes-voz-consumo-noticias-directo-crecen-medidas-distancia-social-20200407121838.html (última consulta: 14 de mayo de 2020), 7 de abril de 2020.

EUROPOL, *Informe Pandemic profiteering: how criminals exploit the COVID-19 crisis,* marzo de 2020, https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic (última consulta: 14 de mayo de 2020), 27 de marzo de 2020, p. 3.

EXPANSIÓN, *COVID-19: el confinamiento acelera la adopción de servicios como Netflix,* https://www.expansion.com/economiadigital/companias/2020/03/29/5e7b8fd8468aeb29108b45e9.html (última consulta: 14 de mayo de 2020), 29 de marzo de 2020.

FUNDACIÓN ANAR, "Informe sobre violencia intrafamiliar durante el confinamiento por Coronavirus", en Página web de la Fundación ANAR, Fundación ANAR, https://www.anar.org/fundacion-anar-refuerza-chat-ayuda-ninos-adolescentes-durante-confinamiento-y-alerta-de-la-gravedad-de-los-casos-detectados/(última consulta 14 de mayo de 2020).

HERALDO, *La Guardia Civil destaca que los delitos bajan a la mitad, pero alerta sobre el cibercrimen,* https://www.heraldo.es/noticias/nacional/2020/03/20/coronavirus-pandemia-guardia-civil-destaca-que-delitos-bajan-a-mitad-pero-alerta-sobre-cibercrimen-1365010.html (última consulta: 14 de mayo de 2020), 20 de marzo de 2020.

LA RAZÓN, *El COVID-19 dispara las compras online en España y aumenta el pesimismo económico*, https://www.larazon.es/economia/20200330/topd6w7vjjddjkjzaccdc6wyjm.html (última consulta: 14 de mayo de 2020), 30 de marzo de 2020.

NATIONAL CRIME AGENCY, "Law enforcement in coronavirus online safety push as National Crime Agency reveals 300,000 in UK pose sexual threat to children", en Página web de la National Crime Agency, Reino Unido, https://www.nationalcrimeagency.gov.uk/news/onlinesafetyathome (última consulta: 14 de mayo de 2020), 4 de abril de 2020.

ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS), *Beware of criminals pretending to be WHO,* https://www.who.int/about/communications/cyber-security (última consulta: 14 de mayo de 2020).

PÚBLIC, *La delinqüència canvia d'escenari i es desplaça durant l'epidèmia,* https://www.publico.es/public/delinqueencia-canvia-d-escenari-i-desplaca-durant-l-epidemia.html (última consulta: 14 de mayo de 2020), 15 de abril de 2020.

VOZ LIBRE, *Colapso en supermercados, escasez y colas interminables ante el cierre escolar por el Coronavirus,* https://vozlibre.com/nacional/colapso-supermercados-escasez-colas-interminables-ante-cierre-escolar-coronavirus-27849/(última consulta: 14 de mayo de 2020), 10 de marzo de 2020.

ZD NET, *Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak,* https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/(última consulta: 14 de mayo de 2020), 13 de marzo de 2020.

20 MINUTOS, *Compras por teléfono, pruebas gratis del COVID-19… Las estafas perpetradas aprovechando la crisis del Coronavirus,* https://www.20minutos.es/noticia/4206878/0/enganos-estafas-perpetradas-crisis-coronavirus/(última consulta: 14 de mayo de 2020), 27 de marzo de 2020.