FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS DE ELCHE

GRADO EN SEGURIDAD PÚBLICA Y PRIVADA

CURSO ACADÉMICO: 2021 / 2022

TRABAJO FIN DE GRADO

CIBERCRIMINALIDAD EN ESPAÑA Y COVID-19:

LA EVOLUCIÓN DEL FRAUDE A TRAVÉS DE INTERNET Y EL DESPLAZAMIENTO DE OPORTUNIDADES DELICITVAS.

Alumno: Luis de la Barrera de Lamo.

Tutora: Dévika Pérez Medina.

Resumen.

El fraude a través de Internet y su evolución durante la pandemia por la COVID-19 merece especial análisis al haber aumentado de forma estrepitosa, siendo esta la conducta de mayor incidencia recogida en los informes de cibercriminalidad emitidos por las diferentes instituciones. El desarrollo masivo de las Tecnologías de Información y Comunicación (TIC), la infinidad de servicios que ofrece Internet, junto con las medidas de confinamiento adoptadas por los poderes públicos, fueron factores que influyeron a los ciudadanos a utilizar Internet de forma desmesurada, teniendo por tanto que adecuar sus hábitos a las nuevas circunstancias y de alguna manera continuar con su vida normal. Por consiguiente, multitud de ciudadanos se sumaron al uso de Internet y trasladaron sus actividades cotidianas al espacio virtual, lo que implicó el incremento de riesgos en el ciberespacio. Por lo expuesto, el presente trabajo pretende abordar la evolución del fraude a través de Internet y analizar su incidencia durante los tiempos de pandemia, mediante la revisión de diversos estudios relacionados con el fenómeno indicado, con el objeto de aproximarse a la realidad y generar conocimiento para futuros estudios. Tras el análisis realizado, se puede llegar a la conclusión que existe una correlación entre el aumento del fraude mediante dispositivos informáticos con el uso de Internet, al igual que se percibe un cambio de actividades cotidianas como consecuencia de las medidas de confinamiento, hecho que provocó el aumento de riesgos en el "ciberespacio" y, por consiguiente, un incremento de oportunidades ciberdelictivas.

Palabras clave**:** cibercriminalidad, COVID-19, fraude online, estafa informática y desplazamiento de oportunidades delictivas.

Abstact.

Internet fraud and its evolution during the COVID-19 pandemic deserves special analysis as it has increased dramatically, being the behavior with the highest incidence reported in the cybercrime reports issued by the different institutions. The massive development of Information and Communication Technologies (ICT), the infinity of services offered by the Internet, together with the confinement measures adopted by the public authorities, were factors that influenced citizens to use the Internet in a disproportionate way, thus having to adapt their habits to the new circumstances and somehow continue with their normal life. Consequently, a multitude of citizens joined the use of the Internet and transferred their daily activities to the virtual space, which implied the increase of risks in cyberspace. Therefore, this paper aims to address the evolution of fraud through the Internet and analyze its incidence during the pandemic times, by reviewing various studies related to the phenomenon indicated, in order to approach the reality and generate knowledge for future studies. After the analysis carried out, it can be concluded that there is a correlation between the increase in fraud through computer devices and the use of the Internet, as well as a change in daily activities as a consequence of the confinement measures, which led to an increase in risks in "cyberspace" and, consequently, an increase in cybercrime opportunities.

Keywords: cybercrime, COVID-19, online fraud, computer fraud and displacement of criminal opportunities.

Índice

1. Introducción.

En la actualidad, el fraude a través de medios informáticos abarca varios aspectos que influyen y favorecen en su desarrollo. Antes de abordar los datos registrados por las instituciones, se considera adecuado describir por separado algunos de los elementos que intervienen, para poder entender mejor este fenómeno y los motivos de su evolución.

1.1. Ciberseguridad frente a la cibercriminalidad: nuevos riesgos.

La globalización junto con el desarrollo tecnológico presenta nuevos desafíos para multitud de actores sociales, principalmente para los Estados, por lo que requiere una respuesta que haga frente a estos problemas y así poder proteger a la sociedad[1]. Entre algunos de esos desafíos se puede destacar el fenómeno de la ciberdelincuencia, el cual precisa que los poderes públicos articulen los mecanismos y sistemas de protección ante los riesgos y ataques que se llevan a cabo a través del ciberespacio[2], de modo que deben garantizar la seguridad frente a estas agresiones. En este sentido, se pronuncia el Convenio sobre la Ciberdelincuencia aprobado en Budapest el 23 de noviembre de 2001, cuyo documento recoge la necesidad de proteger a la sociedad frente a la cibercriminalidad como consecuencia de la digitalización, la convergencia y la globalización de las redes informáticas[3].

La criminalidad informática se define como aquel fenómeno sometido a constantes cambios, cuyo ámbito nuclear se encuentra la manipulación de ordenadores con el fin de conseguir ventajas patrimoniales (Tiedemann, 2000). El derecho informático es el conjunto de derechos y normas que regulan los efectos jurídicos surgidos de la relación entre el derecho y la informática (H. Fernández, 2014). El cibercrimen implica daños informáticos, transferencias económicas no consentidas, sabotear datos e infraestructuras informáticas, por lo que suscita mayor complejidad que le delito cometido en el espacio físico, al desenvolverse en un lugar con nuevas realidades (ciberespacio) que implica realizar técnicas especializadas, involucrando una compleja transformación que genera dificultades doctrinales (Posada, 2017). Así pues, el

[1] Véase Estudio sobre la Cibercriminalidad en España 2019, cuyo documento recoge la complejidad del fenómeno http://www.interior.gob.es/web/archivos-y-documentacion/informe-sobre-la-cibercriminalidad-en-espana

[2] Véase el Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

[3] https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

cibercrimen adopta diversas formas, tanto tradicionales como nuevas modalidades, pero las legislaciones se muestran muchas veces lentas (Álvarez, 2001) y los poderes públicos no tienen las herramientas necesarias para hacer frente a estas formas de criminalidad (Devia, 2017), por lo que es necesario promover nuevas respuestas normativas que se adecuen a los avances tecnológicos para luchar contra las dificultades que se dan en dicho ámbito (Sain, 2018).

Si se acude a la Real Academia Española el concepto de "*seguridad ciudadana*" se define como aquella *"situación de tranquilidad pública y de libre ejercicio de los derechos individuales, cuya protección efectiva se encomienda a las fuerzas del orden público"*, lo que entraña una protección de su integridad física y patrimonial. A este respecto, son las autoridades gubernativas las que deben de garantizar la "*seguridad jurídica*", que no es otra cosa que la "*cualidad del ordenamiento jurídico que implica la certeza de sus normas y la previsibilidad de su aplicación*"[4]. En un sentido semejante se pronuncia Recasens (2007) al entender la seguridad ciudadana como aquellas condiciones que permiten a las personas tener la posibilidad comprensible de disponer de sus bienes y derechos en una posición de equilibrio social garantizada por los poderes públicos.

Por lo tanto, el Estado es el que debe de actuar como garante de la seguridad y de los derechos de sus ciudadanos, como bien recoge la Constitución Española de 1978 a lo largo de su texto, siendo una de las principales misiones que tienen asignados las autoridades[5]. Una de las principales preocupaciones es la de garantizar la seguridad en el ciberespacio, por lo que se adoptan diferentes medidas para preservar el desarrollo social y la libertad de las personas (Ley de Seguridad Nacional, 2015[6]). La ciberseguridad se configura como el mecanismo adecuado para combatir los riesgos que se puedan desencadenar en el ciberespacio y de esta forma garantizar la información que fluye a través del medio (Núñez y Carhuancho, 2020), que no solo protege los ataques dirigidos

[4] Véase términos referidos en: https://dle.rae.es/seguridad

[5] Véase el preámbulo de la Constitución Española de 1978, el cual recoge *"Proteger a todos los españoles y pueblos de España en el ejercicio de sus derechos humanos, sus culturas y tradiciones, lenguas e instituciones"* https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

[6] Véase artículo 10 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional *"Ámbitos especiales de la Seguridad Nacional"* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389#:~:text=Esta%20ley%20tiene%20por%20objeto,c)%20La%20gesti%C3%B3n%20de%20crisis Y Orden PARA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo Nacional de Ciberseguridad https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-799

a infraestructuras, sino también los derechos y libertades de las personas usuarias del ciberespacio (Crespo, 2019).

En resumen, los poderes públicos deben de intervenir mediante el ordenamiento jurídico y establecer los mecanismos suficientes para hacer frente a aquellas conductas ilícitas que ponen en riesgo los derechos de los ciudadanos en los diferentes ámbitos de su vida, considerando que la mejor forma de protección social es mediante la regulación de la Ley Orgánica 10/1995, del Código Penal[7]. Entre sus objetivos se destaca proteger a los cibernautas cuando naveguen por la Red, puesto que la ciberseguridad es un elemento que compone las políticas gubernamentales para lograr la seguridad y el bienestar económico de cada país (ITU, 2009), ya que el ciberespacio sirve de medio para que los cibercriminales realicen sus conductas delictivas (Sánchez, 2012).

1.2. Las Tecnologías de Información y Comunicación y el uso de Internet.

La aparición de las Tecnologías de la Información y Comunicación (TIC) en la vida de los ciudadanos junto con el uso de Internet ha generado aspectos muy positivos en el crecimiento de las sociedades (Méndez y Pérez, 2020), hasta el punto de que ha pasado a ocupar un lugar primordial en los quehaceres cotidianos de las personas como bien indica el Centro de Investigaciones Sociológicas (CIS) en el año 2015[8] (Espinosa, 2019). Cada vez están más presentes las TIC en la vida social y existe una tendencia a la digitalización (ITU, 2009[9]). Probablemente, se deba al desarrollo de multitud de dispositivos a bajo-medio coste que permiten conectarse a la Red desde cualquier parte del mundo, ello unido a la multitud de servicios que ofrece Internet (Espinosa, 2019). Este puede ser uno de los factores que fundamenta el aumento de su utilización.

Uno de los aspectos positivos que se puede destacar y que ofrece Internet es la posibilidad de que personas que se encuentran distanciadas a miles de kilómetros puedan interactuar en un mismo lugar "ciberespacio", lo que significa que reduce las distancias, elimina las fronteras y permite comunicar información prácticamente sin límites, de manera que el espacio se contrae y la intercomunicación se expande, de modo que existen menos limitaciones relacionadas con el espacio y el tiempo (Miró Llinares, 2011). Esto

[7] Véase la exposición de motivos de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
[8] Barómetro de marzo de 2015. Estudio Nº 3057. Centro de Investigaciones Sociológicas.
[9] https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

quiere decir que aquellos usuarios que cuenten con dispositivos tecnológicos y conexión a Internet tienen infinidad de posibilidades, entre las cuales se destacan las compras online, interactuar con otras personas a través de las redes sociales, teletrabajar, asistir a videoconferencias, entre otras muchas.

En cambio, no todos los aspectos que rodean a Internet son positivos. El ciberespacio se configura como un área donde el internauta puede compartir información de forma abierta y en múltiples direcciones (Pérez-San José et al., 2012), lo que quiere decir que no son meros receptores de información, sino que interactúan de manera activa. Estas circunstancias pueden dar lugar a que Internet se convierta en un ámbito lleno de riesgos, sobre todo para aquellos usuarios que no cuenten con los conocimientos suficientes, ya que pueden comprometer sus datos personales, intimidad o bienes, sin percatarse de ello. Estas vulnerabilidades que presentan algunos internautas son conocidas y aprovechadas por los ciberdelincuentes para conseguir su objetivo (Solari, 2021). En consecuencia, las peculiaridades que rodean al ciberespacio en ciertos casos se pueden considerar elementos generadores de riesgo y facilitadores del cibercrimen (Miró Llinares, 2011), ya que el delito informático tiene una naturaleza internacional como consecuencia del desarrollo de las comunicaciones entre los distintos países, que hace desaparecer las fronteras y supera las barreras nacionales (Rovira del Canto, 2002).

Pues bien, el ciberdelito se da por la expansión tecnología que requiere la unión de una maquina y el hombre en un entorno virtual (Cámara, 2020); la utilización de las TIC requiere conocimientos informáticos (R. Pérez et al., 2018); Internet es un medio que utilizan algunos actores criminales (Aguilar, 2015), proporciona anonimato (Sánchez, 2012) y dificulta la autoría (Espinosa, 2019) y; las TIC junto con la evolución de Internet ha creado una nueva forma de delincuencia conocida como el cibercrimen (Soto, 2012), cuya expansión se debe a la comodidad que ofrece para cometer la conducta ilícita sin tener contacto directo con la víctima (Devia, 2017). Parece ser que la era de la globalización junto con el desarrollo social ha traído nuevos riesgos digitales que atentan contra la funcionalidad de las infraestructuras informáticas y necesita la intervención institucional.

1.3. La crisis sanitaria por la COVID-19 y factores que influyen en la evolución de la cibercriminalidad.

La pandemia por la COVID-19 provocó que los gobiernos adoptaran medidas restrictivas de confinamiento para así poder reducir los riesgos de contagio entre los ciudadanos de la población y de alguna manera controlar la crisis sanitaria. En este sentido el Gobierno de España aprueba el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria provocada por la COVID-19[10]. Como consecuencia de las medidas restrictivas, los ciudadanos modificaron sus rutinas habituales y cambiaron la forma de interactuar (FIADYS, 2020), pasando multitud de actividades que se realizaban en el mundo físico al mundo virtual (Miró Llinares, 2021).

Es aquí donde adquiere importancia la utilización de las TIC y el aumento de las conexiones a Internet, como bien sostiene los informes de We Are Social (2020)[11] al indicar que existe un incremento del uso de la tecnología conectada a Internet por parte de la ciudadanía en el periodo de pandemia. Ante el miedo de posibles contagios, el gobierno ordenó el distanciamiento social y el confinamiento en sus domicilios, por lo que de alguna forma la situación propició a que los ciudadanos utilizaran con mayor asiduidad los dispositivos tecnológicos conectados a Internet (Miró Llinares, 2021). Así pues, se tuvieron que adaptar a las nuevas circunstancias con el objeto de continuar con su vida y de alguna manera seguir interactuando con otras personas, realizar sus compras, teletrabajar, asistir a conferencias, compartir o consultar información, entre múltiples posibilidades (Rodríguez, 2021). Este hecho conllevó a que multitud de ciudadanos sin los conocimientos suficientes se conectaran a Internet y expusieran sus vulnerabilidades en la Red, circunstancia bien conocida por los ciberdelincuentes cuyo objetivo era obtener beneficios patrimoniales mediante acciones ilícitas (CNN-CERT, 2020).

Esta afirmación se refleja en algunos de los peligros alertados por diferentes instituciones como la Interpol (2020) o Europol (2020) entre los que se desatacan: a) dominios maliciosos con el nombre de coronavirus o semejantes; b) riego de ciberseguridad en las empresas al tener sus empleados que teletrabajar desde sus equipos domésticos y; ataques “ransomware” dirigidos a instituciones de las que podían sacar más

[10] https://www.boe.es/eli/es/rd/2020/03/14/463
[11] https://wearesocial.com/es/blog/2020/01/digital-2020-espana/

provecho, como es el caso de laboratorios (tenían investigaciones en curso para luchar contra el coronavirus) y centros hospitalarios (no se podían permitir el colapso dada la urgente necesidad). El "phishing" o estafa se presenta como una de las principales amenazas, seguidas del "malware/ransomware", dominios maliciosos y noticias falsas (Interpol, 2020[12]).

Las circunstancias que rodean la pandemia se pueden considerar como caldo de cultivo para ciertas conductas delictivas en el ciberespacio, generando así más oportunidades, existiendo relación entre cotidianeidad, oportunidad y delincuencia (Miró Llinares, 2021). En este sentido, diversas instituciones emiten recomendaciones a la población para reducir los peligros que se producen en el ciberespacio. Un ejemplo de ello es la Unión Europea que advierte al personal de empresas en situación de trabajo a distancia de los riesgos existentes en el medio virtual (Cockburn y Hurtado, 2021).

En conclusión, la crisis sanitaria derivada de la COVID-19 forzó a que los ciudadanos desplazaran ciertas actividades cotidianas del mundo físico al mundo virtual (Buil et al., 2021), lo que generó un cambio de rutinas, dejando así un escenario apropiado para su análisis desde la óptica de las teorías criminológicas, concretamente, desde el enfoque de las oportunidades delictivas (Rodríguez, 2021).

1.4.El desplazamiento de las oportunidades delictivas: del espacio físico al virtual.

Como se ha visto hasta el momento, la criminalidad en el entorno virtual se expande de tal manera que genera nuevas oportunidades conforme se extiende el uso de Internet (Solari, 2021). Además, si se acude a los datos registrados durante el confinamiento por la COVID-19 se puede apreciar un incremento del uso de las TIC, más conexiones a Internet (INE, 2020), un aumento de riesgos en el ciberespacio con motivo del teletrabajo desde casa (Cockburn y Hurtado, 2021), un crecimiento acelerado de "phishing/estafas", "malware/ransomware", dominios maliciosos y noticias falsas (Interpol, 2020) y un descenso de delincuencia en el espacio físico (Buil et al., 2021); lo que quiere decir que las actividades cotidianas trazan las oportunidades delictivas (Miró Llinares, 2021).

[12] COVID-19 Cybercrime Analysis Report- August 2020 (5).pdf

A este respecto, parece interesante abordar el citado fenómeno desde el prisma de las teorías de la oportunidad, ya que puede resultar un mecanismo práctico de prevención frente al delito (Miró Llinares, 2011), puesto que los datos advierten de una probable relación entre los elementos que intervienen y su evolución: fraude, tecnología, Internet y Covid-19.

Se parte de la base que la expansión tecnológica junto con la multitud de servicios que ofrece Internet ha generado diversas oportunidades delictivas que han crecido y mejorado con el tiempo. Además, las medidas de confinamiento por la COVID-19 han promovido un uso masivo de medios tecnológicos conectados a Internet, hecho que ha generado aumentos de riesgos en el ciberespacio y motivo por el cual las instituciones accionaron todas las alertas (FIADYS, 2020).

Sin ánimo de ahondar más por el momento, estudios como los realizados por Miró Llinares (2021) señalan que existe relación entre las actividades cotidianas y la posibilidad de convertirse en víctima de un determinado delito, de modo que si se reducen las oportunidades se reduce la acción delictiva. Asimismo, diversos estudios ponen de manifiesto la evolución ascendente de los ciberdelitos durante el periodo de confinamiento (Buil et al., 2020).

2. Marco teórico

2.1. El fraude a través de medios informáticos: conceptualización y aspectos generales.

El fraude o defraudación hace referencia a la conducta o artimaña para obtener un beneficio patrimonial (Balmaceda, 2011) y la estafa se entiende como una conducta fraudulenta que induce a error a un tercero para apropiarse de un bien (Devia, 2017). Cuando esta conducta se comete a través de la Red se describe como un fenómeno creciente que sobresale del resto (Miró Llinares, 2013a), hasta el punto de que se considera la modalidad contra la propiedad que más predomina (Williams, 2016) y el crimen más persistente en el ciberespacio (Miró Llinares, 2013a).

Su estudio surge con motivo de la comisión de fraudes informáticos asociados a transferencias electrónicas de fondos (Picotti, 2013), cuyo resultado produce grandes perjuicios económicos (Kemp & Moneva, 2020), ocupando un papel central en la

cibercriminalidad. La acción fraudulenta de perjuicios patrimoniales a terceros se considera una de las conductas más desarrolladas en la Red (Fernández, 2007). El incremento exponencial de las operaciones por medio del correo electrónico y el uso de los servicios bancarios a través de Internet trajo consigo nuevas formas de delincuencia y defraudación, según muestra los datos ofrecidos por el Observatorio de Seguridad de la Información adscrito al Instituto Nacional de las Tecnologías y Comunicación (Bicarregui, 2008). Asimismo, el volumen de transacciones financieras que se realizan a diario motiva el surgimiento de actividades ilícitas como, por ejemplo, la suplantación de identidad, los delitos informáticos dirigidos al fraude y otras actividades (Chiriguayo, 2015). Además, el fraude en línea es uno de los delitos relacionados con la informática que se cometen a gran escala todos los días y los daños financieros causados son enormes (ITU, 2009).

Los casos de fraude informático suponen casi el 90% del cibercrimen en el territorio español, siendo por tanto la conducta criminal que más incidencia tiene en el ciberespacio según los datos registrados desde hace años por el Ministerio del Interior[13]. Estos datos se encuentran reflejados en el Sistema Estadístico de Criminalidad (SEC) y provienen de las infracciones penales conocidas por las Fuerzas y Cuerpos de Seguridad (Cerezo y García, 2020). Así bien, se registran como fraude informático las estafas bancarias, las estafas a través de tarjetas de crédito, débito o cheques de viaje, así como, otras estafas, empleando como medio para su comisión Internet/ informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs, correos electrónicos y redes sociales; por lo que queda relacionado el fraude informático con la estafa.

Cabe destacar que las TIC adquieren importancia como nuevo medio para su comisión, dado que aparecen comportamientos propios de la estafa como, por ejemplo, el hecho de detectar búsquedas de información sensible para posteriormente cometer fraudes (Miró Llinares, 2013a). Hay que tener en cuenta que las formas de fraude se han incrementado en tiempos de pandemia (Moreno, 2020), ya que los delincuentes se han aprovechado de la situación para sustraer dinero e información mediante diferentes

[13] https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/portal/datos.html?type=pcaxis&path=/Datos5/&file=pcaxis

modalidades de estafa (González y Álvarez, 2020). Además, las sociedades muestran una dependencia respecto a las tecnologías que les está haciendo más vulnerables frente a posibles ataques cibernéticos y al fraude en la Red (Sánchez, 2012).

En definitiva, el fraude a través de Internet involucra el uso de dispositivos electrónicos (Monsurat, 2020) y se considera una actividad ilícita que pone en peligro la seguridad de los sistemas sociales, así como, lesiona los intereses jurídicos individuales (Oxman, 2013). Parece que la expansión tecnológica ha multiplicado cuantitativamente el fraude informático (Devia, 2017).

2.2. El derecho como fuente de regulación ante los nuevos riesgos.

El Derecho se configura como el sistema de control social con el objeto de mantener la convivencia humana pacífica, por lo que se debe de adecuar a las nuevas realidades y prevenir aquellas conductas que pongan en riesgo los derechos de los ciudadanos (Devia, 2017). Es con la llegada del ciberespacio cuando el fenómeno delictivo se incrementa de forma exponencial, pues la era de la información multiplica las oportunidades delictivas (Pons, 2017). La introducción de la gestión y asignación de activos patrimoniales en la informática han permitido que se puedan realizar transmisiones injustas (Fernández, 2007). Esto quiere decir que las nuevas tecnologías junto con la conexión a Internet han generado nuevas oportunidades delictivas, por lo que es necesaria la intervención institucional, siendo un problema global que no entiende de fronteras (Miró Llinares, 2011).

2.2.1. Convenio Internacional sobre la Ciberdelincuencia. Budapest, 2001.

Ante los riesgos surgidos en las redes informáticas con fines delictivos, los Estados miembros de la Unión Europea muestran su preocupación y, como consecuencia de ello, aprueban el Convenio sobre la Ciberdelincuencia en Budapest el 23 de noviembre de 2001, considerada la principal herramienta internacional en regular dicha materia (Devia, 2017). En aras de aunar esfuerzos y con el objetivo de proteger a la sociedad frente al cibercrimen, establecen un modelo de legislación “tipo” mediante la homologación de normas y la mejora de la cooperación internacional (Vílchez, 2020), para así poder actuar de forma rápida y fiable. Su propósito es prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas,

redes y datos informáticos, lo que supone tipificarlos como conductas delictivas con el fin de garantizar la protección social.

Por consiguiente, es imprescindible regular ciertas conductas llevadas a cabo en el ciberespacio, como es el claro ejemplo del fraude informático, ya que la manipulación informática difícilmente puede entrar dentro del tipo básico de estafa al no poderse aplicar el elemento de engaño, puesto que los ordenadores y programas no se pueden engañar (López, 2018). Teniendo en cuenta el avance de las nuevas tecnologías y la gran cantidad de formas de comisión delictiva, el Tratado Internacional abarca los casos de *"delitos informáticos"* en su Título II, recogiendo el fraude informático en su artículo 8*:*

> *"Las partes adoptarán las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegitima un beneficio económico para uno mismo o para otra persona (Convenio sobre la Ciberdelincuencia de Budapest, 2001)".*

Como se puede apreciar, el presente Convenio surge de la preocupación por las nuevas formas delictivas y los nuevos riesgos que asumen la sociedad producto de los avances tecnológicos. De forma general, recoge los aspectos relacionados con el desarrollo de las nuevas tecnologías, establece las bases para adecuar las normativas nacionales de los Estados signatarios, con el objeto de garantizar los bienes jurídicos que afectan a las personas. De esta manera, incluye aquellas conductas que transgreden los derechos de los ciudadanos en el ámbito virtual, protegiendo así la funcionalidad informática (Mayer, 2017). Este Convenio fue ratificado por España en el año 2010[14].

2.2.2. Derecho Penal Español: Ley Orgánica 10/1995, del Código Penal.

Previa a la aprobación de la Ley Orgánica 10/1995, los delitos informáticos resultaban atípicos para los tribunales, dado que no eran visibles ni tangibles y, por lo tanto, no se podía aplicar la norma. Es decir, no se podía aplicar la conducta punible de

[14] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

estafa sobre una máquina, puesto que las maquinas no se les puede engañar (Fernández, 2007), sentido en el que se pronuncia la Sentencia del Tribunal Supremo de 19 de abril de 1991.

Con la aprobación de la Ley Orgánica 10/1995 queda patente la protección de determinadas conductas que anteriormente se quedaban en el aire, como es el caso concreto del fraude informático. Al incluir en el apartado 2 del artículo 248 "*manipulación informática o artificio semejante*" se salva esta dificultad jurídica, permitiendo así castigar como estafa la obtención de datos sensibles mediante la manipulación informática que sin mediar consentimiento permitiera posteriormente percibir una transferencia económica a favor del autor y en perjuicio de la víctima.

A pesar de existir una manipulación informática, el legislador considera adecuado castigar como estafa dicha conducta, puesto que el destinatario que sufre el error y el engaño es un ser humano y sufre un perjuicio patrimonial (Miró Llinares, 2013a). Sin embargo, el principal objetivo que el legislador tenía cuando incluyó este tipo penal era el de castigar aquellas conductas fraudulentas que realizaban los empleados de entidades bancarias y obtenían transferencias a su favor sin consentimiento de sus titulares. De hecho, este artículo se comenzó a aplicar para castigar operaciones fraudulentas ejecutadas con tarjetas de crédito en cajeros automáticos (Fernández, 2007). Ahora bien, después de varias modificaciones, el artículo 248 del Código Penal queda recogido dentro del Título XIII *"Delitos contra el patrimonio y el orden socioeconómico"* Capítulo VI *"De las defraudaciones"* Sección 1 *"De las estafas*" de la siguiente manera:

> *"1. Cometen estafa los que con ánimo de lucro utilizaren engaño bastante para producir error en otro induciéndole a realizar un acto de disposición en perjuicio propio o ajeno.*
>
> *2. También se consideran reos de estafa: a) Los que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro; b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en ese artículo; c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje,*

o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero (Ley Orgánica 10/1995)[15] *"*.

De esta forma se libra la dificultad jurídica que presentaba el anterior Código Penal para castigar aquellas conductas ilícitas en las que se obtienen datos confidenciales mediante manipulación informática y sin el consentimiento de su titular que, posteriormente, permiten recibir una transferencia económica en beneficio de su autor y en perjuicio de un tercero (Miró Llinares, 2013a).

2.3. Elementos que intervienen en la estafa y su bien jurídico protegido.

La estafa es uno de los delitos más clásicos cometidos contra el patrimonio. Así lo refleja algunos de los textos más antiguos como, por ejemplo, el Código de Hammurabi (1750 a.C) que contemplaba algunos casos de este injusto (Devia, 2017). Como se ha visto hasta el momento, en España el delito de estafa se encuentra recogido en el artículo 248 del Código Penal, concretamente, en el Título XIII *"Delitos contra el patrimonio y el orden socioeconómico"* Capítulo VI *"De las defraudaciones"* Sección 1 *"De las estafas*". En este apartado se va a abordar los elementos que intervienen en la estafa.

Se parte de la base que no basta con que el autor obtenga un resultado ni que este ilícito se cometa de cualquier manera (Izquierdo, 2016), sino que debe de haber una relación de causalidad entre los siguientes elementos: la intención, el ánimo de lucro, el engaño, el error y la disposición ajena patrimonial (Fernández, 2007). En este sentido se pronuncia el Tribunal Supremo mediante la Sentencia Nº 187/2002, de 8 de febrero, de la Sala Segunda de lo Penal, señalando que tiene que haber relación de causalidad entre el engaño provocado y el perjuicio experimentado. En la misma dirección se pronuncia el Tribunal Supremo mediante Sentencia Nº 465/2012, de 1 de junio, de la Sala Segunda de lo Penal, indicando que el perjuicio ha de aparecer vinculado causalmente con la acción engañosa[16]. Por tanto, el engaño debe de ser capaz de inducir al error para disponer del patrimonio en perjuicio de una persona (Leyton, 2014), siendo un elemento esencial en la acción ilícita (Balmaceda, 2011) para percibir la transferencia patrimonial de la víctima (Alas, 2015). Asimismo, el elemento típico se sitúa en generar un perjuicio patrimonial

[15] https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
[16] https://laleydigital-laleynext-es.publicaciones.umh.es/Content/Logout_es.html

(Schlack, 2008), sin olvidar que la conducta delictiva requiere dolo y ánimo de lucro (Mayer y Oliver, 2020).

El delito de estafa común no deja de ser un acto negociable (Izquierdo, 2016) en el que se produce una interacción entre un autor que emplea diferentes métodos de engaño y una víctima que se desprende de un bien económico en perjuicio de su patrimonio (Alas, 2015). En términos generales, la estafa se puede considerar como una conducta fraudulenta en la que se induce a error para apropiarse de manera indebida un derecho patrimonial, obteniendo un beneficio y causando un perjuicio a otro (Devia, 2017). Sin embargo, parece que el desarrollo social y los avances tecnológicos han influido en la evolución del fraude, ya que los delincuentes han adquirido métodos más sofisticados para obtener beneficios patrimoniales de terceros. De esta manera el fraude adopta nuevas formas en el ciberespacio (Núñez y Carhuancho, 2020). De hecho, el fraude informático se relaciona con la estafa puesto que afecta al mismo bien jurídico protegido, pero con distinciones en sus tipos de conductas (Mayer y Oliver, 2020). En base a lo expuesto, cabe indicar la principal diferencia de la estafa informática que es la "manipulación informática o artificio semejante", la cual se puede equiparar con el acto de disposición (Balmaceda, 2011), para posteriormente obtener una transferencia no consentida de activos patrimoniales.

En este sentido, el legislador incluye como estafa una acción que difería de la estafa convencional, donde el "error" y el "engaño" se suprimen por el "artificio tecnológico o manipulación informática" para llevar a cabo la acción, ya que a diferencia de una persona una maquina no puede sufrir engaño o error, dado que esta opera con las instrucciones que se le introducen (Balmaceda, 2011). Al respecto, se pronuncia la Sentencia del Tribunal Supremo de 20 de noviembre de 2001, recogiendo que el engaño consustancial a la interacción personal es sustituido por la manipulación informática o artificio semejante como medio para la comisión de la defraudación (Fernández, 2007). Por otra parte, con la regulación de los delitos informáticos, el legislador pretende garantizar la denominada "*funcionalidad informática*", entendida como el conjunto de condiciones que permiten realizar las operaciones informáticas dentro de un marco tolerable de riesgo (Mayer, 2017), por lo que el delito de estafa informática comparte un bien jurídico común con el resto de ciberdelitos, además del bien jurídico protegido específico.

2.4. Modalidades de fraude contra el patrimonio mediante recursos informáticos.

El fraude online es un fenómeno creciente que adquiere diferentes formas (Miró Llinares, 2011), pero tienen un objetivo común que es el de obtener un beneficio patrimonial en perjuicio de otro (Miró Llinares, 2013a). En el Código Penal español se pueden diferenciar dos tipos de estafas, por lo que a continuación y de forma breve se exponen algunos ejemplos para poder entender mejor su distinción. Ambos tipos de conductas guardan estrecha relación, aunque varían sus elementos para su equiparación (Balmaceda, 2011).

2.4.1. La estafa básica en el ciberespacio.

El primer apartado trata de abordar aquellas conductas de estafa que se desarrollan en el ciberespacio y que se pueden encuadrar dentro del artículo 248.1 del Código Penal. Las más comunes son aquellas que implican la venta de un producto a través de una red social sin que el comprador lo reciba, o bien cuando el comprador anula el cargo una vez que lo ha recibido (López, 2018). Otra conducta que encaja dentro de la estafa común y que se comete a través de la Red es la estafa piramidal denominada tipo "Ponzi". Esta se trata de una operación fraudulenta de inversión que implica el pago de intereses a los inversores de su propio dinero invertido o de los nuevos inversores (López et al., 2020). También se pueden destacar el denominado "Phishing Car", que consiste en ofrecer vehículos lujosos a precios bajos con la excusa de que se encuentra fuera del país (Bicarregui, 2008); las "estafas de lotería" que se caracteriza por el envío de spam a través de correos electrónicos en el que se le informa a la víctima que ha ganado un premio de una cantidad alta de dinero y para adquirirlo debe de abonar una cantidad, desconociendo que la cantidad que va a ingresar es el objeto de defraudación (Miró Llinares, 2013a); o las "*Cartas Nigerianas*" conocida como "Scam 419" que consiste en recibir un correo en el que promete un negocio muy rentable (Devia, 2017).

Este tipo de estafa puede adoptar diferentes formas, pero no deja de ser una estafa común, ya que reúne todos y cada uno de sus elementos esenciales: intención, ánimo de lucro, engaño, error y disposición ajena patrimonial; pero con la diferencia que se comete a través de medios informáticos, sirviendo la Red como vehículo del ilícito. De esta manera, el autor goza de los beneficios que ofrece la Red, como la de permitir una mayor visibilidad online (Miró Llinares, 2011) y, por consiguiente, un aumento de victimización

(Miró Llinares, 2013b), al igual que proporciona anonimato de modo que dificulta su autoría (Espinosa, 2019). En conclusión, este delito de estafa afecta al patrimonio de las personas, pero no se considera estafa informática cuando se comete a través de las redes sociales (López, 2018).

2.4.2. La estafa informática.

El segundo apartado trata de abordar aquellas conductas de estafa que se desarrollan en el ciberespacio y que se pueden encuadrar dentro del artículo 248.2 del Código Penal. Los métodos más comunes que se relacionan con el fraude informático son mediante la difusión de "softwares malwares" que tratan de infiltrarse en los equipos informáticos de las víctimas con fines defraudatorios (Bicarregui, 2008). Así pues, los ciberdelincuentes tratan de obtener beneficios a través de diversas estrategias, entre las que se destacan el "phishing" o "pharming", cuyo objetivo es apoderarse de la información confidencial de la víctima para después obtener un beneficio patrimonial (Oxman, 2013) mediante técnicas de ingeniería social.

Por un lado, está el llamado "phishing" que se presenta generalmente mediante el envío de correos electrónicos y aparenta proceder de fuentes fiables como, por ejemplo, entidades bancarias, en el que se suele incluir un enlace de página web falsa con aspecto idéntico que invita a su cliente a dar información confidencial sobre sus cuentas bancarias, tarjetas de crédito o débito. En algunos casos redirige a la víctima a una página fraudulenta que permite captar sus datos personales y en otros casos se presenta en forma de formulario que hay que rellenar en el propio e-mail. Una variante del phishing es el denominado "pharming", resultando ser un método más sofisticado que consiste en manipular los servidores DNS para redireccionar el nombre de un dominio a una página web idéntica en la que el defraudador obtiene los datos de la víctima como, por ejemplo, la obtención de los datos bancarios introducidos por la persona cuando realiza una compra online (Fernández, 2007).

En resumen, estas son algunas de las conductas que requiere conocimientos informáticos para realizar la "manipulación", utilizando para ello "técnicas de ingeniería social" que consisten en utilizar un aliciente para llamar la atención de la persona y lograr que actúe como el autor quiere (Bicarregui, 2008). Así bien, se dan los elementos contemplados en el artículo 248.2 del Código Penal cuando existe ánimo de lucro y se

consiguen los datos de la víctima mediante manipulación informática, realizando posteriormente una transferencia económica a favor del autor sin consentimiento y en perjuicio de la persona afectada.

2.5. Las teorías de la oportunidad adaptadas al contexto cibercriminal.

Como se ha podido comprobar en los anteriores apartados, el fraude llevado a cabo mediante dispositivos informáticos se produce con cierta frecuencia en el día a día de los ciudadanos (Bicarregui, 2008). Así bien, se considera adecuado tomar su estudio desde el prisma de las teorías de la oportunidad (Felson y Clarke, 1998) con el objeto de darle un enfoque práctico a la prevención de este fenómeno (Miró Llinares, 2013b), puesto que los resultados denotan que existe relación entre las actividades cotidianas y la incidencia del fraude a través de Internet (Miró Llinares, 2021).

Es evidente que las teorías criminológicas estudian el delito en un momento y lugar concreto, aspecto que difiere del ciberespacio, puesto que no es un espacio físico (Solari, 2021). Esto quiere decir que, mientras que la conducta delictiva llevada a cabo en el espacio físico se identifica en un lugar concreto y un momento determinado (Cohen y Felson, 1979), los delitos informáticos se pueden cometer a miles de kilómetros sin ser preciso tener contacto con la víctima (Devia, 2017) y el injusto no tiene porqué coincidir con un momento concreto (Oxman, 2013), sino que se puede cometer tanto en ese momento como tras pasado un tiempo. Sin embargo, a pesar de las diferencias sustanciales que existen entre ambos ámbitos, dichas teorías se consideran el eje central de la criminología ambiental y contempla ciertos aspectos que se pueden trasladar al ciberespacio, pudiendo resultar efectivas para evitar su comisión, por lo que ocupan un papel central en la prevención (Miró Llinares, 2013b). A este respecto y para una mejor comprensión de los siguientes apartados se expone de manera breve y comprensible los detalles básicos de las teorías de la oportunidad (Felson y Clarke, 1998) que se pueden clasificar en:

1) Teoría de las actividades cotidianas: pone de manifiesto que el delito se produce cuando coinciden un delincuente motivado, un objetivo o víctima y la ausencia de un guardián en un momento y en un lugar determinado (Cohen y Felson, 1979).
2) Teoría del patrón delictivo: parte de la base que tiene que haber una combinación de infractor y víctima en un momento y lugar determinado, al igual que tiene que

acontecer tres elementos clave: nodos, rutas y límites (Brantingham y Brantingham, 1993a, 1993b). De esta teoría se destaca que el delito se comete en los lugares donde frecuentan las actividades rutinarias.

3) Teoría de la elección racional: plantea que los infractores buscan la obtención de beneficios y toman sus decisiones atendiendo al balance entre riesgo y éxito, quedando la teoría resumida a que el delincuente tiene intención, es racional y toma una decisión específica (Cornish y Clarke, 1986).

En este sentido, Cornish y Clarke (2003) proponen 25 técnicas para prevenir las situaciones que dan pie al delito, cuyos objetivos se centran en aumentar el esfuerzo del delincuente, los riesgos que asume, disminuir los beneficios, reducir las provocaciones y eliminar sus excusas. Asimismo, Felson y Clarke (1998) proponen 10 principios para explicar la relación entre delito y oportunidad, donde ponen de manifiesto que las oportunidades simbolizan un papel central en la causa del delito.

Teniendo en cuenta lo dispuesto en dichas teorías, aunque el ciberespacio es diferente al espacio físico, es cierto que para que se cometa la conducta delictiva tiene que darse los tres elementos citados, es decir, un delincuente motivado, un objetivo o víctima y la ausencia de un guardián. En segundo lugar, para que se cometa el delito tiene que coincidir con un lugar que genere oportunidades para los delincuentes, ámbito que suele coincidir con aquellos donde se llevan a cabo las actividades cotidianas. Cabe recordar que, si no hay oportunidad, difícilmente puede haber delito. En tercer lugar, el delincuente es un ser racional que actúa con intención y toma una decisión en función de los riesgos beneficios que puede asumir con la acción. A este respecto, hay que considerar que el ciberespacio ofrece anonimato (Sánchez, 2012) y la posibilidad de llegar a más víctimas, aspecto destacable en los fraudes a través de Internet (Miró Llinares, 2013b). Este puede ser uno de los motivos que incentive la delincuencia a través del ciberespacio.

Otro aspecto que puede incitar a los ciberdelincuentes a llevar el ilícito a través de este medio es la dificultad que tienen las autoridades para determinar su autoría (Espinosa, 2019), puesto que al desenvolverse en un ámbito transnacional (Miró Llinares, 2013b) que no entiende de fronteras, requiere emplear arduos métodos de investigación que difícilmente se llevan a la práctica. En este caso y en relación con los elementos de la teoría de las actividades cotidianas se puede materializar la falta o ausencia de guardián. Igualmente, otra consideración que puede alentar el aumento del cibercrimen, es que el

avance tecnológico proporciona a los ciberdelincuentes maneras más sofisticadas para obtener sus beneficios, mostrándose las normativas mucho más lentas que los desarrollos tecnológicos (ITU, 2009).

Sin entrar en más valoraciones puesto que se desarrollará en apartados siguientes, el cibercrimen se produce cuando existe una combinación de los elementos indicados y se previene si dejan de existir, por lo que parece que las teorías de la oportunidad guardan estrecha relación con la prevención de las conductas delictivas llevadas a cabo en el ciberespacio.

3. Objetivos, hipótesis y propósitos.

3.1. Objetivos.

El principal objetivo de este trabajo es conocer la situación en la que se encuentra el fraude cometido en el ciberespacio y describir los factores que han podido incidir en su desarrollo. En concreto, se pretende conocer la progresión de este fenómeno, hacer hincapié durante la crisis sanitaria por el "coronavirus" y ver si de alguna manera han podido influir las actividades cotidianas de los ciudadanos. Este objetivo se pretende lograr mediante la revisión de otros estudios y el análisis de las cifras registradas por las Fuerzas y Cuerpos de Seguridad de España publicadas por el Sistema Estadístico de Criminalidad. Es cierto que los datos que se registran no siempre abarcan la cifra real de las conductas ilícitas, puesto que existe la cifra negra (Montiel, 2016), ya que en ocasiones los hechos no son denunciados por vergüenza, porque son cantidades económicas ínfimas o porque las víctimas consideran que puede significar una pérdida de tiempo y dinero. Sin embargo, permite aproximarse a la realidad y conocer su gravedad.

Como primera cuestión, se plantea si el incremento de los fraudes a través de Internet se debe al aumento de las TIC por el cambio de las rutinas cotidianas como consecuencia de las medidas de confinamiento o si por el contrario se tratan de factores independientes unos de los otros. Por otra parte, interesa comparar las cifras existentes de fraude con otros delitos informáticos para conocer su valor dentro de la ciberdelincuencia. Como objetivo final, se busca concienciar de los riesgos que se originan en el ciberespacio y así promover habilidades para que los ciudadanos no caigan en las redes de la cibercriminalidad. Solo mediante su continuo análisis a través de la comunidad científica

permitirá arrojar luz a las políticas públicas para conseguir una sociedad más sana tecnológicamente.

3.2. Hipótesis.

La hipótesis que se plantea en el presente trabajo se encuentra relacionada con el fraude, la expansión tecnológica, el uso de Internet, la crisis sanitaria por la Covid-19 y el desplazamiento de oportunidades. Partiendo de la base que varios estudios apuntan a una posible relación entre estos elementos, se considera adecuado abordar la siguiente hipótesis: "Si la crisis sanitaria por la Covid-19 ha originado un cambio en las rutinas cotidianas, de manera que ha acelerado la expansión tecnológica y el uso de Internet, entonces ha incrementado las oportunidades delictivas en el ciberespacio y ha provocado el aumento del fraude a través de Internet". A su vez, surgen varias cuestiones a resolver a lo largo de este trabajo. Realmente, la crisis sanitaria por la Covid-19 ¿ha provocado un cambio de rutinas cotidianas? ¿ha desplazado las oportunidades delictivas del mundo físico al virtual? ¿ha acelerado la expansión tecnológica y el uso de Internet? ¿se trata de un fenómeno independiente que no causa efecto en la evolución del fraude a través de Internet? o ¿únicamente ha servido de "acelerador" en la evolución natural del fraude informático? Asimismo, se plantean otras cuestiones como ¿han aumentado todos los fraudes online por igual? ¿han aumentado solo ciertos ciberfraudes? ¿se han reducido los delitos en el espacio físico?

3.3. Propósitos.

Pues bien, el propósito es contrastar las cuestiones planteadas con los estudios revisados y los datos recabados, para así poder obtener un conocimiento más exhaustivo sobre la relación entre los fenómenos anteriormente referidos, quedando detallado en los siguientes apartados.

4. Metodología y recopilación de datos.

4.1. Aspectos éticos.

El presente estudio se ha desarrollado considerando los principios éticos que rigen los estudios científicos, teniendo en cuenta que el fenómeno del fraude a través de Internet ha tenido un impacto reseñable en la sociedad durante los últimos años. Además, se ha

respetado el derecho a la propiedad intelectual de los trabajos que anteceden y se han referenciado en el apartado específico. Previamente a su realización, se ha recibido el código de investigación responsable "TFG.GSP.DPM.LDLBDL.220411" emitido por el órgano competente. El contenido del trabajo ha sido supervisado por Doña Dévika Pérez Medina, docente de la Facultad de Ciencias Jurídicas de la Universidad Miguel Hernández de Elche. Asimismo, se han tenido en cuenta las normas específicas recogidas en la guía de elaboración Trabajo de Fin de Grado publicadas en el campus del Grado en Seguridad Pública y Privada, por lo que obedece a los preceptos éticos y legales en su elaboración y redacción.

4.2. Metodología.

La investigación pura es el balance del problema dirigido a la búsqueda de conocimiento (Baena, 2017) que requiere una estrategia para resolver la cuestión planteada (Hernández, Fernández y Baptista, 2014). De acuerdo con lo indicado, la metodología seleccionada trata sobre la revisión sistemática de estudios previos y el análisis de datos cuantitativos publicados por los organismos oficiales, puesto que es el método que mejor se adapta a las características y necesidades del presente, con el objeto de describir adecuadamente la situación actual, dando paso a las interrogantes planteadas de fraude online en España, tiempos de pandemia y desplazamiento de oportunidades. Al ser un problema de transcendencia global, requiere una investigación desde un enfoque multidisciplinar, considerando que el estudio de los datos estadísticos y la observación desde diferentes perspectivas permite comprender mejor la cuestión (López et al., 2020), obtener un conocimiento aproximado de la realidad y arrojar claridad a su prevención.

Como referencia inicial se han tomado varios estudios previos, además de su regulación normativa, con el propósito de conceptualizar y describir adecuadamente el fenómeno. Así también, se han escogido datos de diversas instituciones, tanto a nivel nacional como internacional, con el objetivo de identificar nexos causales. Sirve como apoyo central del presente los datos publicados en el Portal Estadístico de Criminalidad, el Instituto Nacional Estadístico y el Ministerio del Interior. Además, se complementa con los datos proporcionados por otras instituciones como la Interpol, Europol, Eurostat, Centro Criptológico Nacional (CCN-CERT), Centro de Investigaciones Sociológicas, Google, Action Fraud o We Are Social. La mayoría de los resultados evidencian la magnitud del fraude en el ciberespacio como consecuencia de la expansión tecnológica y

la COVID-19 como causa del cambio de rutinas cotidianas y desplazamiento de oportunidades delictivas. Con los recursos planteados se considera suficiente para despejar las cuestiones planteadas y enunciar algunas conclusiones.

4.3. Recolección de estudios y análisis de datos.

Para la recopilación de los estudios se han utilizado los servicios ofrecidos por la biblioteca digital de la Universidad Miguel Hernández de Elche (UMH), concretamente, las bases de datos ProQuest, Web of Science y La Ley Digital, seleccionando algunos de los que se consideraron más interesantes para la realización del presente. También se han seleccionado varios estudios ofrecidos por las bases de datos Dialnet, Revista de Investigación Criminológica, SciELO, Google Scholar y algunos organismos oficiales, al ser trabajos igualmente interesantes y que previamente no se localizaron en las bases de datos de la UMH. En su búsqueda se han usado varias combinaciones de palabras clave apropiadas al contexto del fenómeno como: "crimen", "estafa", "fraude online", "cibercrimen", "estafa informática", "ciberseguridad", "ciberespacio", "criminalidad", "cibercriminalidad", "COVID-19", "desplazamiento de oportunidades", "actividades cotidianas" y "teorías de la oportunidad". Finalmente, se han escogido algunos de los estudios que constan en las referencias bibliográficas, quedando estos reflejados en apartados siguientes para aclarar algunas de las cuestiones planteadas.

Sobre los datos de fraude informático en España, en su mayoría se han obtenido del Sistema de Estadística de Criminalidad, concretamente del módulo de cibercriminalidad, cuya base comprende los periodos anuales entre el año 2011 y 2020, lo que permite una clara apreciación del fenómeno a lo largo de todo este tiempo y una comparación con los ciberdelitos registrados en el año 2020 "año de pandemia". Como bien se ha adelantado anteriormente, esta base de datos procede de las infracciones registradas por las Fuerzas y Cuerpos de Seguridad (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra, Ertzaintza, Mossos d' Esquadra y distintos Cuerpos de Policía Local), clasificándose en hechos conocidos, hechos esclarecidos, detenciones e investigados y victimizaciones. No hay que obviar que las series históricas se han visto alteradas a partir del 2015 como consecuencia de las modificaciones legislativas, puesto que se incluyen los delitos contra el honor, amenazas y coacciones; y la incorporaron de datos proporcionados por la Ertzaintza y Mossos d'Esquadra. También hay que tener

presente que a la hora de interpretar las series de hechos esclarecidos y victimizaciones la Ertzaintza no ha facilitado datos, por lo que las series no se encuentran completas.

Así bien, el SEC tipifica las conductas y sigue las conceptuaciones que emplea el Convenio de Budapest, añadiendo las infracciones penales de delitos contra el honor, amenazas y coacciones. Si se acude a la tabla de cibercriminalidad, bajo la denominación de "fraude informático" recoge las conductas delictivas contempladas entre los artículos 248 al 251 del Código Penal español. Concretamente, registra aquellas conductas ilícitas que se pueden encuadrar como estafa bancaria, estafa con tarjetas de crédito, débito o cheques de viaje y otras estafas; cuyo medio empleado sea Internet/ informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs, correos electrónicos y redes sociales.

Cabe tener en cuenta que los datos registrados no siempre se ciñen a la realidad, puesto que en ocasiones se rechazan conductas que encajan en la figura delictiva, pero no se registran por su escasa repercusión (Montiel, 2016). Esto quiere decir que existen sesgos y no se pueden sacar conclusiones definitivas, al existir la denominada cifra negra. Al igual ocurre que ciertas conductas ilícitas no son denunciadas por sus víctimas, bien porque en muchas ocasiones se trata de cantidades ínfimas, bien porque las víctimas se sienten avergonzadas al ser burdamente engañadas, o bien porque consideran que puede ser una pérdida de tiempo y dinero.

En otro orden, se ha tomado como base los datos proporcionados por el Instituto Nacional de Estadística, para así comprobar el uso de Internet y la movilidad de las personas durante el periodo de COVID-19. Referente a los datos de usos de tecnología, conexiones a Internet y compras online, los datos han sido recabados de la Encuesta realizada por el INE sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares (2020). En cuanto a los datos publicados de movilidad, provienen del análisis de la posición de más del 80% de los teléfonos móviles en toda España, cuyo análisis ha sido elaborados en estrecha colaboración de los tres principales operadores de telefonía móvil (Orange, Telefonía, Vodafone), centrándose en el estudio de la movilidad de la población durante el estado de alarma.

También, se han recopilado datos publicados por otros organismos, tanto nacionales como internacionales, entre los que se destacan el Ministerio del Interior, Interpol, Europol, Eurostat, Centro Criptológico Nacional, Centro de Investigaciones Sociológicas, Google, Action Fraud o We Are Social, entre otros; entidades que ponen de manifiesto la incidencia de la tecnología en la sociedad, la reducción de la movilidad social y la evolución del fraude a través de medios informáticos en tiempos de pandemia. Tanto los datos recabados del SEC como de otras instituciones se reflejan en los apartados siguientes. En definitiva, la cibercriminalidad ha surgido como consecuencia del desarrollo social y tecnológico. Y la evolución al alza del fraude informático se encuentra marcada por la etapa de la pandemia, por lo que merece especial estudio.

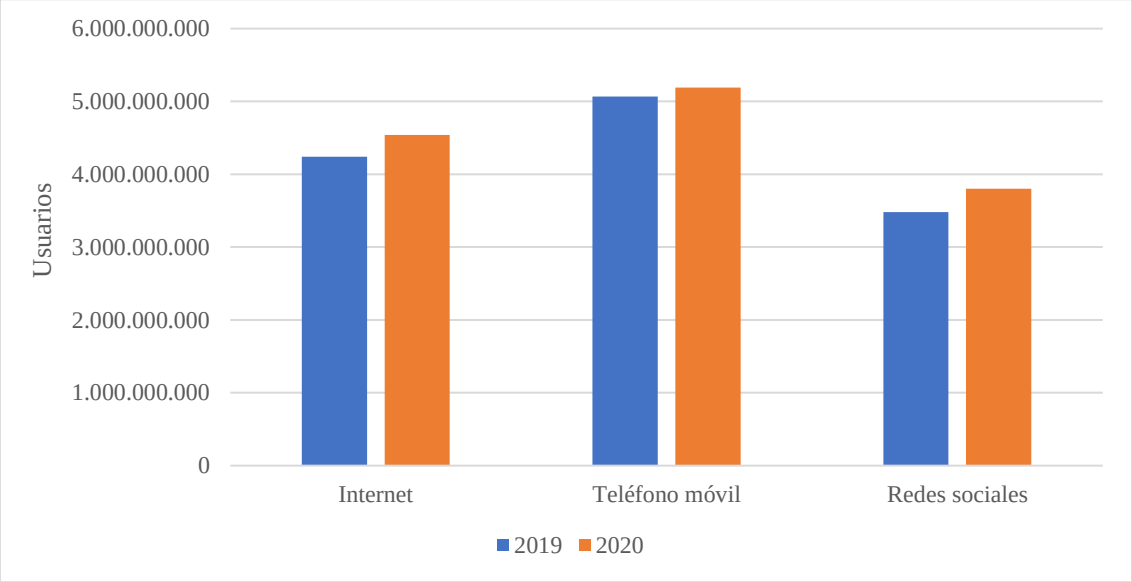
5. Resultados

"We Are Social" pone de manifiesto que existe un alto índice de la utilización de las nuevas tecnologías y se han convertido en una parte primordial de la vida cotidiana de las personas en todo el mundo (López et al., 2020). Esta agencia creativa se encuentra especializada en las tendencias tecnológicas y el uso que hacen las personas. En su informe del año 2020 registra a nivel mundial más de 5.190 millones de usuarios de teléfonos móviles, 4.538 millones usuarios de Internet y 3.800 millones de usuarios activos en redes sociales, lo que significa un aumento respecto al año 2019 de 124 millones de usuarios de teléfonos móviles (2,4%), un ascenso de 298 millones de usuarios de Internet (7%) y un incremento de 321 millones de usuarios activos en las redes sociales (9%). Estos datos se traducen a que los usuarios pasan conectados a Internet 6 horas y 43 minutos al día, lo que equivale a más de 100 días al año. Para una mejor comprensión de los resultados se añade la figura 1 que muestra la evolución del uso tecnológico a nivel mundial.

Revisados los datos del uso de la tecnología en España correspondientes al año 2020 se registra más de 54 millones de usuarios de teléfono móvil, más de 42 millones de usuarios en Internet y 29 millones usuarios activos en las redes sociales. Esos datos expresan un descenso de 153.000 teléfonos móviles, un aumento de más de 1,8 millones de usuarios de Internet y un ascenso 860.000 usuarios activos de las redes sociales; es decir, un descenso respecto al año 2019 del 0,3% de usuarios de teléfono móvil, un aumento del 4,3% de usuarios de Internet y un incremento de 3,1% de usuarios activos de las redes sociales, aspectos que se muestran en la figura 2 para una mejor comprensión.

Figura 1

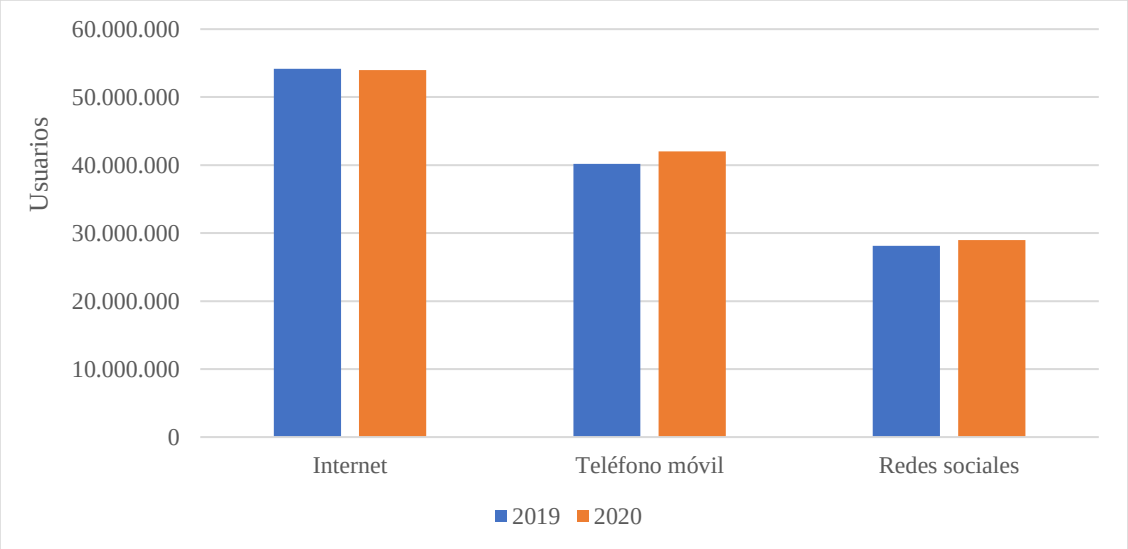
Gráfico sobre los Usos de las Tecnologías a Nivel Mundial.



Fuente: elaboración propia a partir de los datos publicados por We Are Social[17].

Figura 2

Gráfico sobre los Usos de la Tecnología en España.



Fuente: de elaboración propia a partir de los datos publicados por We Are Social.

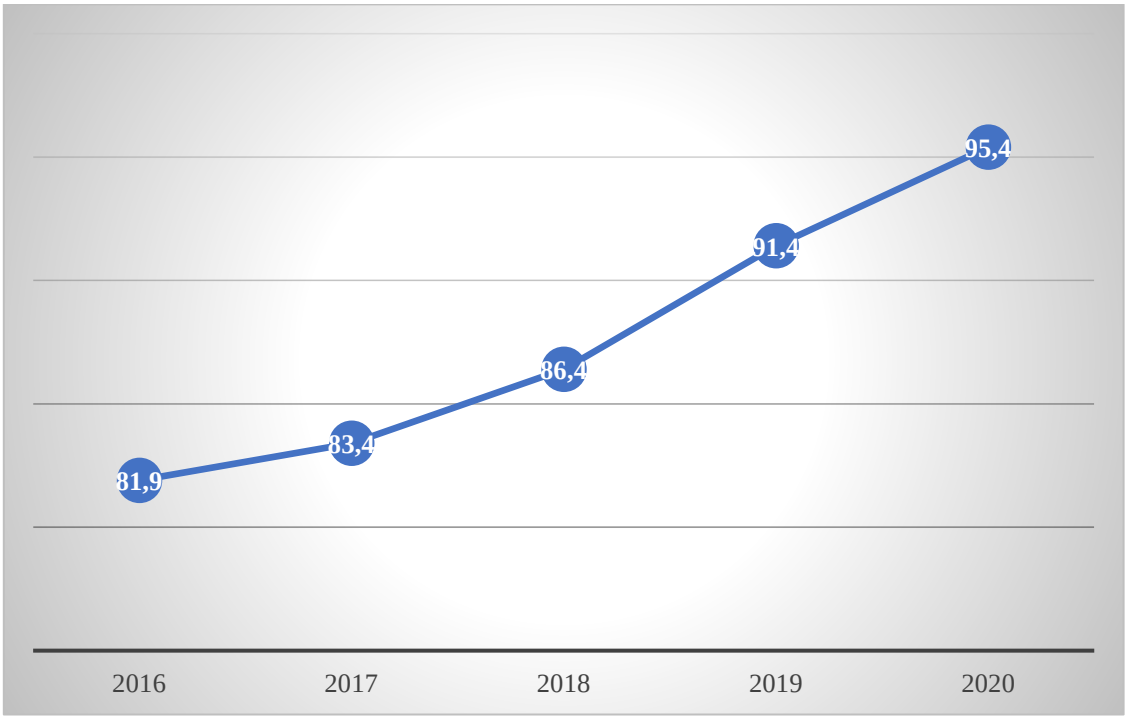
[17] Ambos gráficos: https://wearesocial.com/es/blog/2020/01/digital-2020-espana/

De esta manera, los resultados mostrados por el informe del Digital Global Report sugieren un cambio al alza del uso de las redes sociales, móviles y conexiones a Internet, etapa que coincide con la pandemia por la COVID-19.

La encuesta realizada por el Instituto Nacional de Estadística (INE) sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares trata de abordar varias cuestiones. En la consulta realizada a la población sobre la tenencia de ordenadores en los hogares y si estos se encuentran conectados a Internet, los resultados arrojan una cifra del 80,9% (con ordenador) y 91,4% (conectados a Internet) en el año 2019 y una cifra del 81,4% (con ordenador) y 95,4% (conectados a Internet) en el año 2020, lo que significa un aumento sobre el año anterior del 0.5% y 4% respectivamente, como se aprecia en las figuras 3 y 4.

Figura 3

Gráfico de Viviendas con Acceso a Internet.

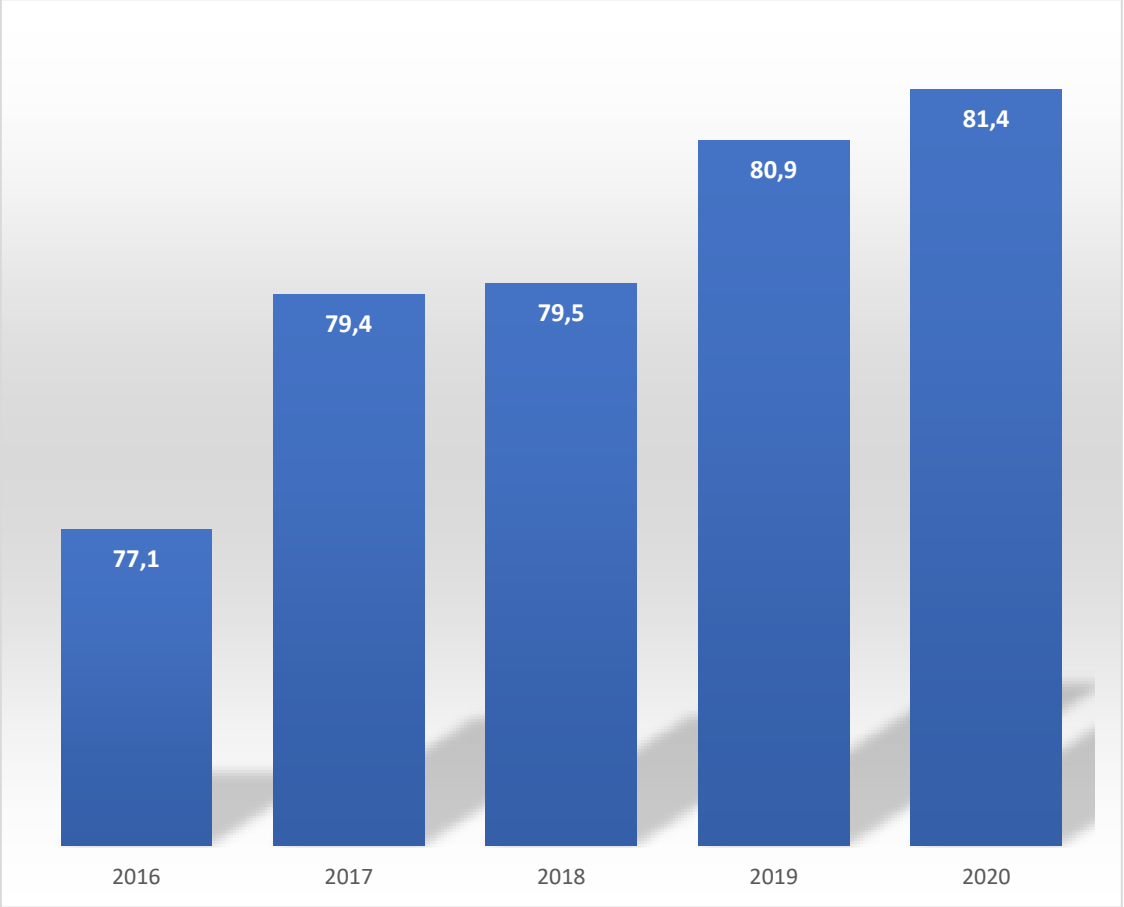


Fuente: elaboración propia a partir de los datos publicados por el INE[18].

[18] Evolución de datos de Viviendas (2006-2020) por tamaño del hogar, hábitat, tipo de equipamiento y periodo (ine.es)

Figura 4

Gráfico de Viviendas con Ordenador.



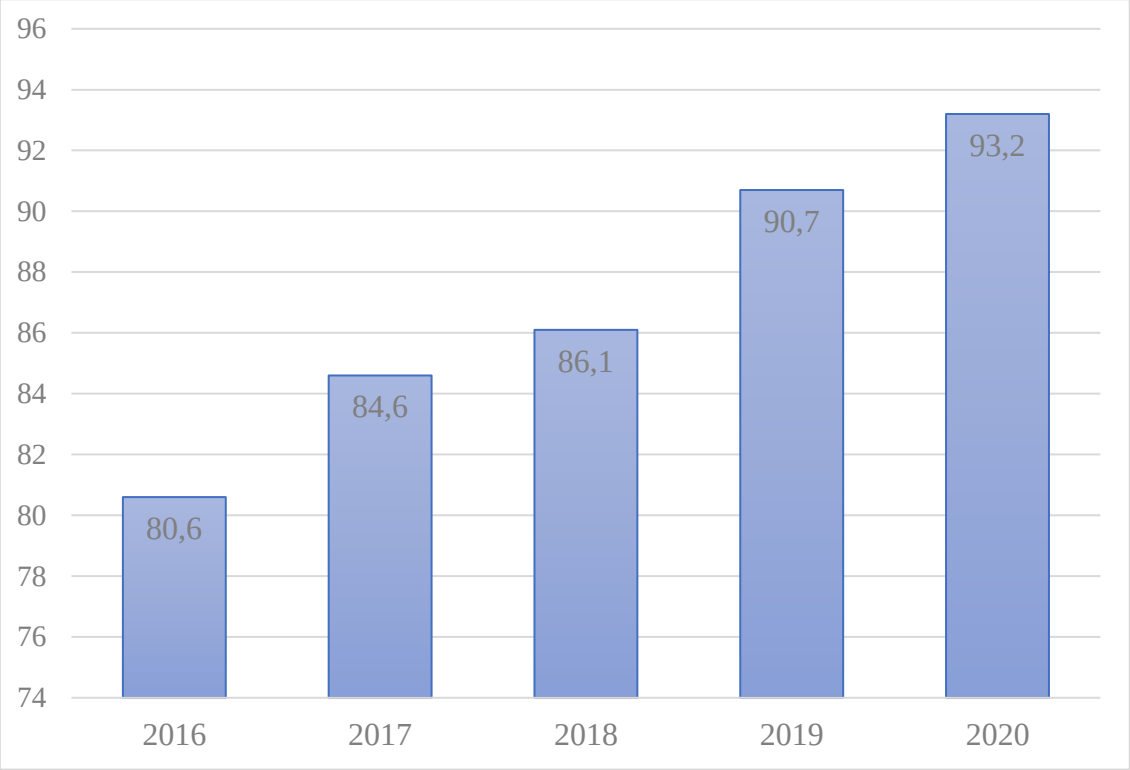
Fuente: elaboración propia a partir de los datos publicados por el INE[19].

Sobre la cuestión planteada a las personas que dicen haber accedido a Internet en los últimos tres meses, la encuesta arroja un resultado del 90,7% en el año 2019 y una cifra del 93,2% en el año 2020, por lo que se aprecia un aumento 2,5% como se expresa la figura 5. Respecto a la cuestión para valorar las personas que dijeron haber comprado en los últimos tres meses por Internet, arroja en 2019 un resultado del 46,9% y en el año 2020 un resultado del 53,8 %, por lo que se aprecia un incremento del 6,9% respecto al año anterior.

[19] Evolución de datos de Viviendas (2006-2020) por tamaño del hogar, hábitat, tipo de equipamiento y periodo (ine.es)

Figura 5

Gráfico de Personas que Utilizaron Internet en los Últimos Tres Meses.



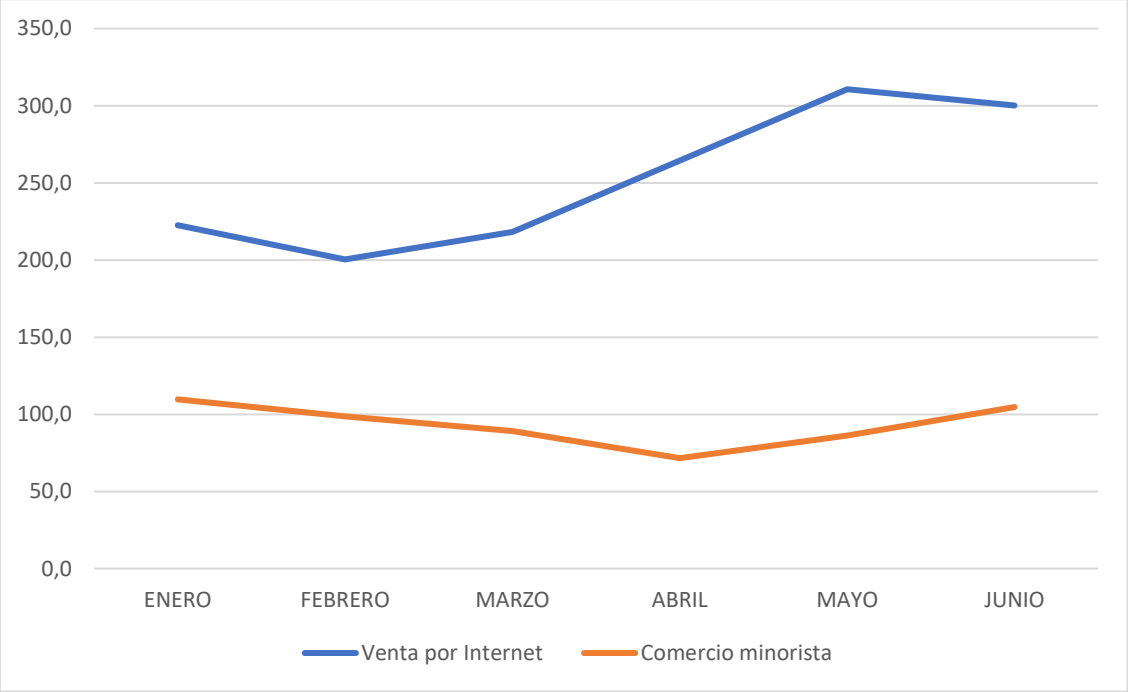
Fuente: elaboración propia a partir de los datos publicados por el INE[20].

Según Eurostat España se sitúa en el año 2020 (con un 95%) por encima de la media de la Unión Europea en relación con las viviendas que tienen acceso a Internet (López et al., 2020). Consultados los datos sobre el comercio minorista español durante el primer semestre del mismo año se aprecia un descenso en el mes de marzo y abril, hecho que cambia en el mes de mayo puesto que recupera su tendencia. En cambio, el canal de ventas por Internet se dispara, se aprecia una fuerte crecida en abril y se mantiene en los siguientes meses. Estos datos estadísticos coinciden con el periodo de más restricciones por la pandemia y refieren un cambio interesante en cuanto al cambio de las actividades cotidianas que se llevan a cabo por parte de la ciudadanía a través de la Red. Para una mejor compresión se indican los resultados en la figura 6.

[20] Evolución de datos de Personas (2006-2020) por características demográficas, tipo de uso de TIC y periodo (ine.es)

Figura 6

Gráfico sobre el comercio al por menor y la venta por Internet.



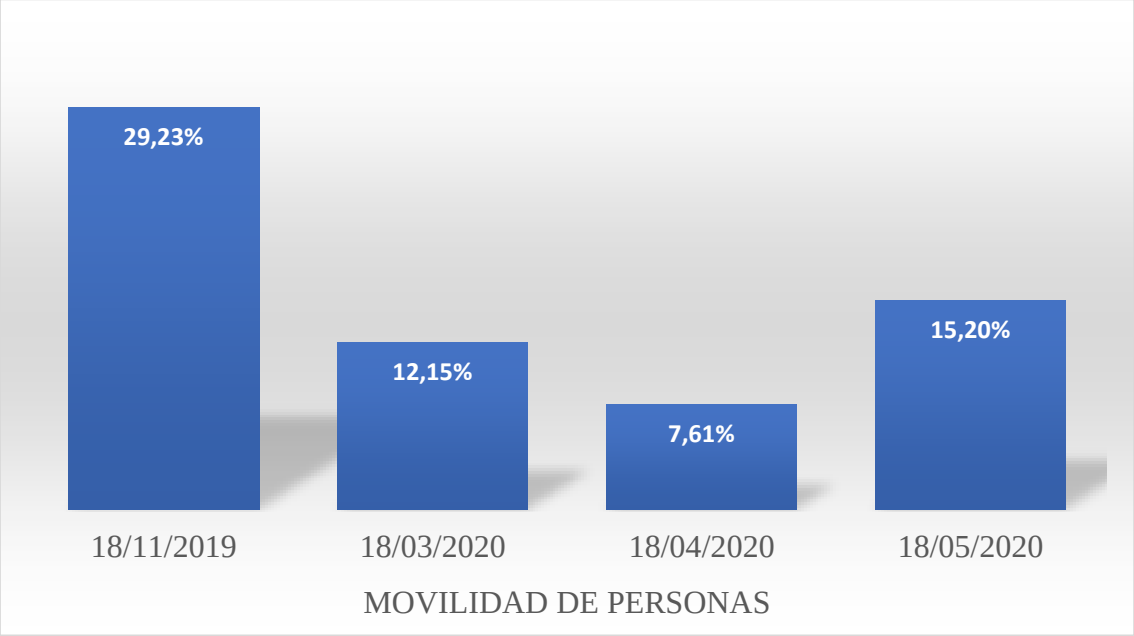
Fuente: elaboración propia a partir de los datos proporcionados por Eurostat[21]

En el análisis que elabora el INE sobre la movilidad de la población durante el estado de alarma, cuyos datos se extraen de la posición de más del 80% de los teléfonos móviles en toda España en estrecha colaboración con los tres principales operadores de telefonía móvil (Orange, Telefonía, Vodafone), se aprecian resultados significativos respecto al desplazamiento de las personas. En primer lugar, el INE toma como primera fecha de referencia el día 18 de noviembre de 2019 y posteriormente pasa directamente al mes de marzo, recogiendo el periodo comprendido entre el día 16 de marzo de 2020 y el 20 de junio de 2020. Los resultados arrojados informan que la movilidad de la población pasa de un 29,3% en noviembre de 2019 a un 7,61% en el mes de abril de 2020, por lo que queda patente los efectos de las restricciones como consecuencia de la pandemia, datos que resultan significativos, puesto que las personas se desplazan menos en el mundo físico. Para una mejor comprensión se indican los datos en la figura 7.

[21] https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=sts_trtu_m&lang=en

Figura 7

Gráfico de Movilidad de la Población en España durante el Estado de Alarma.



Fuente: elaboración propia a partir de los datos facilitados por el INE[22].

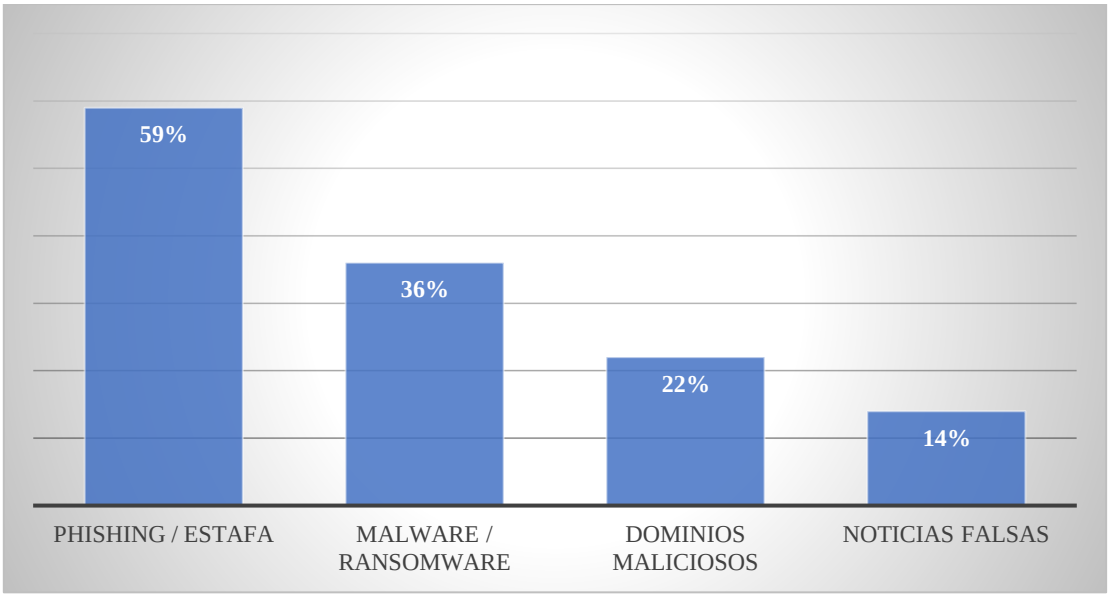
Del mismo modo, se pronuncia el estudio de Ghirelli et al., (2021), cuyo documento recoge los indicadores de movilidad proporcionados por Google para España que muestra como la movilidad se redujo de forma drástica en el mes de marzo, comienza a incrementarse en el mes de mayo y alcanza parámetros más normales en el mes de junio. Este trabajo apunta que la caída de la actividad económica se debe a la reducción de movilidad. Por otra parte, de acuerdo con el estudio realizado por Miró Llinares (2021) sobre el cibercrimen y la COVID-19, organismos como Apple y Google sostienen una reducción de movilidad en los medios de transporte, así como, un descenso de desplazamientos entre zonas residenciales y zonas de comercios y ocio durante los primeros meses de pandemia. En el mismo sentido, el estudio de Kemp et al. (2021) sobre la cibercriminalidad y el fraude cibernético en Reino Unido, recoge mediante gráficos los datos recabados por Google, expresando una reducción de movilidad en el lugar de trabajo, comercio, zonas residenciales y estaciones de tránsito, coincidiendo con el periodo de más restricciones. Estos dos últimos trabajos relacionan la reducción de movilidad con el incremento de la cibercriminalidad.

[22] https://www.ine.es/covid/covid_movilidad.htm

En otro orden, durante la pandemia la Interpol (2020) ha detectado en Europa multitud de dominios maliciosos con la palabra “COVID”, ataques “ransomware” dirigidos a las instituciones esenciales, réplicas de páginas web pertenecientes a organismos gubernamentales y un aumento de “phishing”. Las principales amenazas que se hallan en el ciberespacio se encuentran relacionadas con la pandemia, realizando la Interpol la siguiente clasificación: phishing/estafa (59%), “malware/ransomware” (36%), dominios maliciosos (22%) y noticias falsas (14%), datos que se reflejan en la figura 8.

Figura 8

Gráfico sobre las Principales Amenazas Detectadas en el Ciberespacio.



Fuente: elaboración propia a partir de los datos publicados por la Interpol[23].

El Centro Criptológico Nacional anuncia en su informe de “ciberamenzas y tendencias 2020” que muchos de los aspectos de riesgo se encuentran relacionados con la pandemia por la COVID-19, debido a la situación excepcional por la que está atravesando la sociedad[24]. Las medidas de confinamiento promueven que los ciudadanos teletrabajen desde sus casas con sus equipos informáticos domésticos, hecho que provoca el incremento de la exposición en Internet, la vulnerabilidad de las empresas y situación que aprovechan los ciberdelincuentes para sustraer datos con fines delictivos. Además,

[23] COVID-19 Cybercrime Analysis Report- August 2020.pdf
[24] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html

alerta de los ataques que pretenden acceder a la infraestructura de las empresas, de modo que aumentan los riesgos como consecuencia del teletrabajo y siguen creciendo los ataques a sistemas públicamente expuestos como, por ejemplo, aplicaciones de videoconferencias. De este modo alertan riesgos de posibles ataques contra las farmacéuticas, laboratorios de investigación dedicados a la COVID-19 durante el año 2020.

El VIII Informe de Cibercriminalidad (López et al., 2020) refleja que en el año 2020 se gestionan más de 133.155 incidentes de ciberseguridad en España, siendo los más frecuentes de tipo "malware" con un 35% seguidos de los fraudes con un 32%. Los operadores críticos detectan un incremento del 5,25%, destacando el "malware" motivado por el aumento de las actividades en el ciberespacio como consecuencia de las medidas restrictivas de la pandemia. El sector estratégico resalta los incidentes cometidos en el sector tributario y financiero con un 52.50%[25]. En resumen, el cibercrimen tiene la pretensión de sacar provecho de la situación por la que atraviesa la sociedad.

El Portal Estadístico de Criminalidad (SEC) recoge las conductas que implican la comisión de delitos informáticos, hallándose en una continua progresión puesto que existe diversidad de comportamientos ilícitos. Los datos demuestran que la cibercriminalidad ha evolucionado de tal manera que han surgido diversas modalidades ilícitas que ponen en riesgo los intereses jurídicamente protegidos, siendo por tanto preciso la intervención del derecho penal, de modo que su evolución se ve relacionada con el desarrollo social. Para la correcta comprensión del fenómeno sobre el fraude a través de medios informáticos, se expone los datos recogidos de criminalidad y, en especial, de cibercriminalidad, con el objeto de observar su evolución y comprobar si existía datos que evidencian las consecuencias motivadas por las medidas de confinamiento tras la pandemia por la COVID-19. Pero antes de abordar los datos publicados por el SEC, ha de tenerse en cuenta que las series se encuentran alteradas a partir del año 2015, debido a la aportación de datos por los Mossos d'Esquadra y la Ertzitza, así como, al incluirse nuevos hechos delictivos con motivo de la reforma del Código Penal. Sin embargo, no todas las series incluyen los datos de todos los cuerpos policiales, puesto que la Ertzaintza

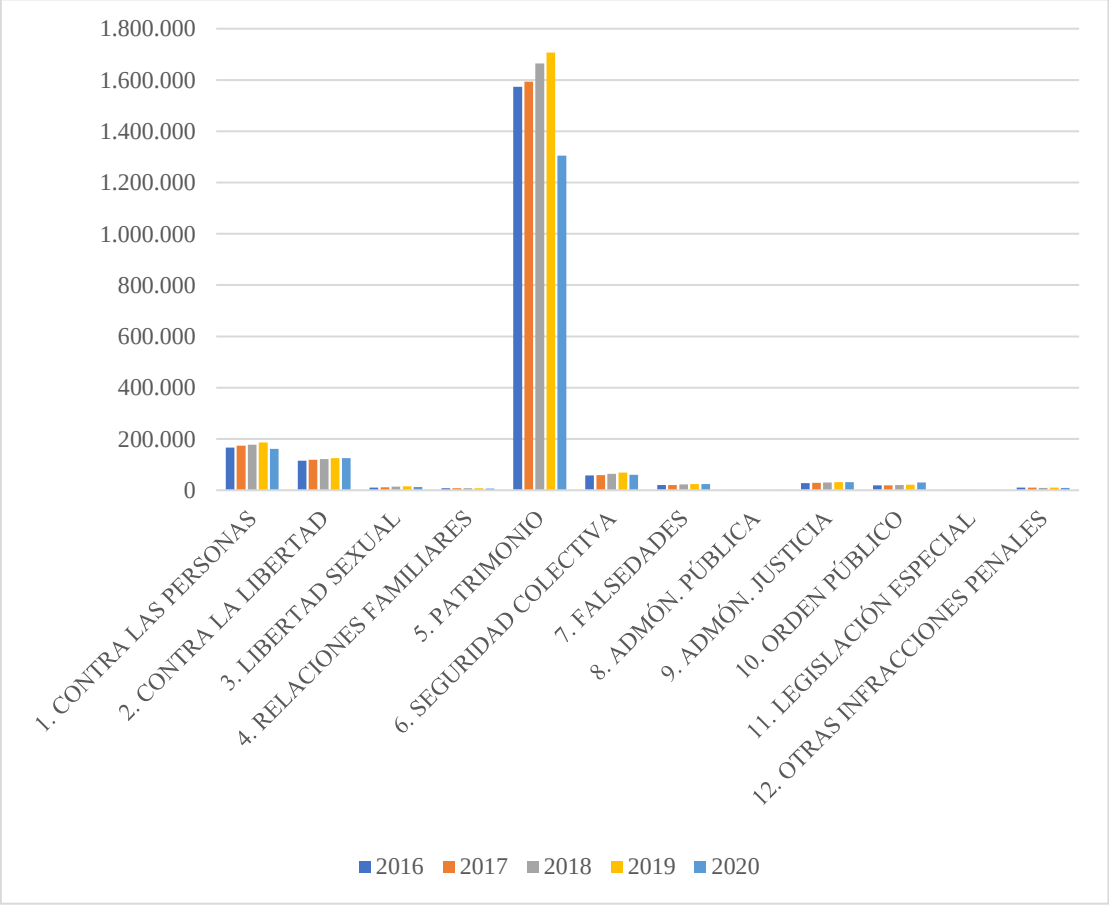
[25] Véase el VIII Informe sobre Cibercriminalidad en España, 2020, cuyo documento recopila los datos estadísticos sobre la cibercriminalidad, los usos de las tecnologías, Internet y los nuevos riesgos como consecuencia de la Covid-19 http://www.interior.gob.es/web/archivos-y-documentacion/informe-sobre-la-cibercriminalidad-en-espana

no facilita datos sobre hechos esclarecidos y victimización. Aun así, se considera adecuado recurrir a los datos estadísticos, ya que es un buen modo de aproximarse a la realidad, y su observación puede ayudar a prevenir ciertas conductas delictivas. Además, cabe añadir que se tomaron en cuenta diferentes periodos anuales para tener una orientación adecuada de su evolución y en especial el periodo comprendido entre el año 2016 y 2020.

En primer lugar, en cuanto a los datos registrados de criminalidad "hechos conocidos", se destaca el grupo penal más cometido "delitos contra el patrimonio", grupo que incluye la estafa. En el año 2020 se puede apreciar un descenso pronunciado del 12% respecto al año 2016 y más de un 19% respecto al año 2019, como muestra la figura 9 y 10.

Figura 9

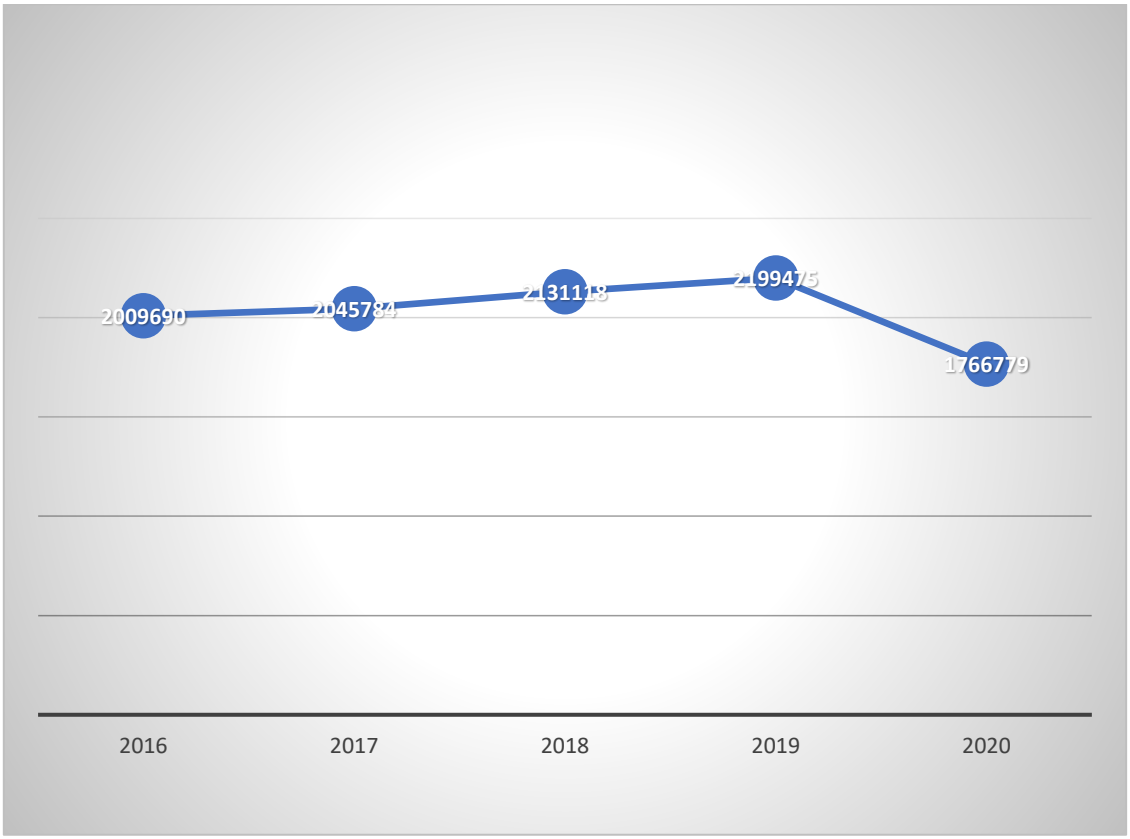
Gráfico sobre la Incidencia de los Delitos contra el Patrimonio en España.



Fuente: elaboración propia a partir de los datos publicados por el SEC.

Figura 10

Gráfico sobre el descenso de la Criminalidad en España en tiempos de COVID-19.



Fuente: elaboración propia a partir de los datos publicados por el SEC[26].

En cambio, los delitos informáticos experimentan una evolución contraria a la definida por los datos de criminalidad. Es decir, se aprecia un aumento considerable año tras año, ascendiendo de forma exponencial en el año 2020 con respecto al año anterior, periodo coincidente con la pandemia. Se destaca el fraude informático como grupo penal más cometido en el ciberespacio, como se refleja en la tabla 11. Asimismo, en el año 2020 se registraron un total de 287.963 hechos conocidos, lo que supone un 31,9% más con respecto al año anterior y el 86,9% corresponde al fraude informático /estafas. Se expresa la tendencia del fraude informático en la figura 12.

[26] Series de Criminalidad en España: https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/portal/datos.html?type=pcaxis&path=/Datos1/&file=pcaxis

Tabla 11

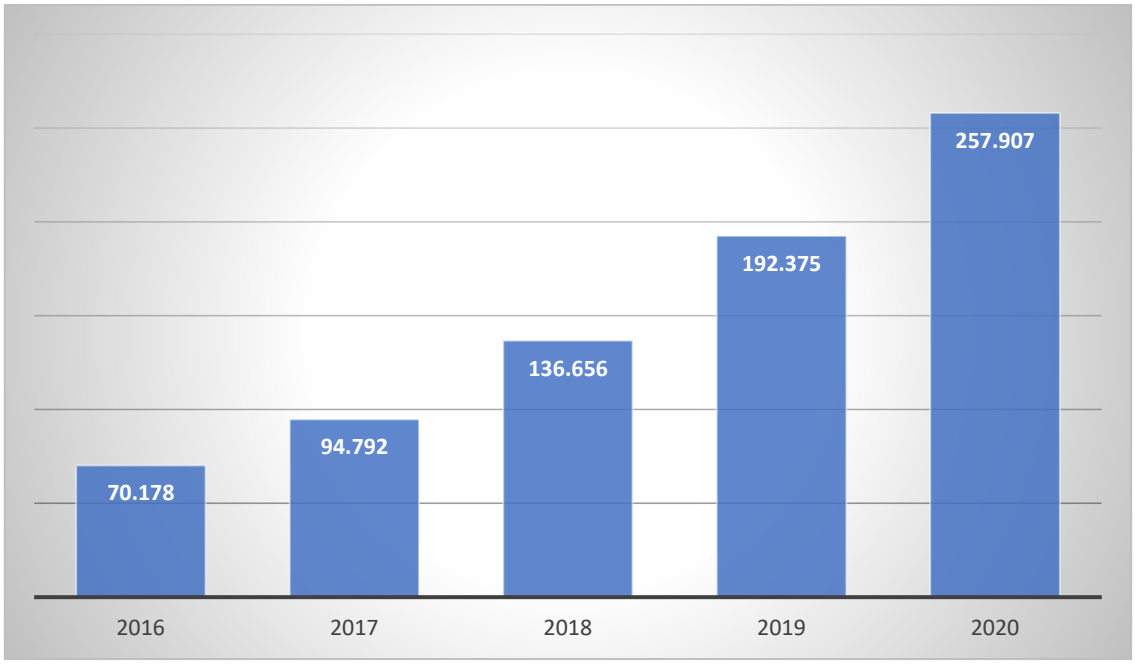
Aumento acelerado de la cibercriminalidad.

HECHOS CONOCIDOS	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
ACCESO E INTERCEPTACIÓN ILÍCITA	1.492	1.701	1.805	1.851	2.893	3.243	3.150	3.384	4.004	4.653
AMENAZAS Y COACCIONES	9.839	9.207	9.064	9.559	10.607	12.036	11.812	12.800	12.782	14.066
CONTRA EL HONOR	1.941	1.891	1.963	2.212	2.205	1.546	1.561	1.448	1.422	1.550
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	222	144	172	183	172	129	121	232	197	125
DELITOS SEXUALES	755	715	768	974	1.306	1.231	1.392	1.581	1.774	1.783
FALSIFICACIÓN INFORMÁTICA	1.860	1.625	1.608	1.874	2.644	3.017	3.280	3.436	4.275	6.289
FRAUDE INFORMÁTICO	21.075	27.231	26.664	32.842	62.038	70.178	94.792	136.656	192.375	257.907
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	228	298	359	440	1.193	1.336	1.291	1.192	1.473	1.590
TOTAL	37.412	42.812	42.403	49.935	83.058	92.716	117.399	160.729	218.302	287.963

Fuente: elaboración propia a partir de los datos publicados por el SEC.

Figura 12

Gráfico sobre el aumento del fraude informático.

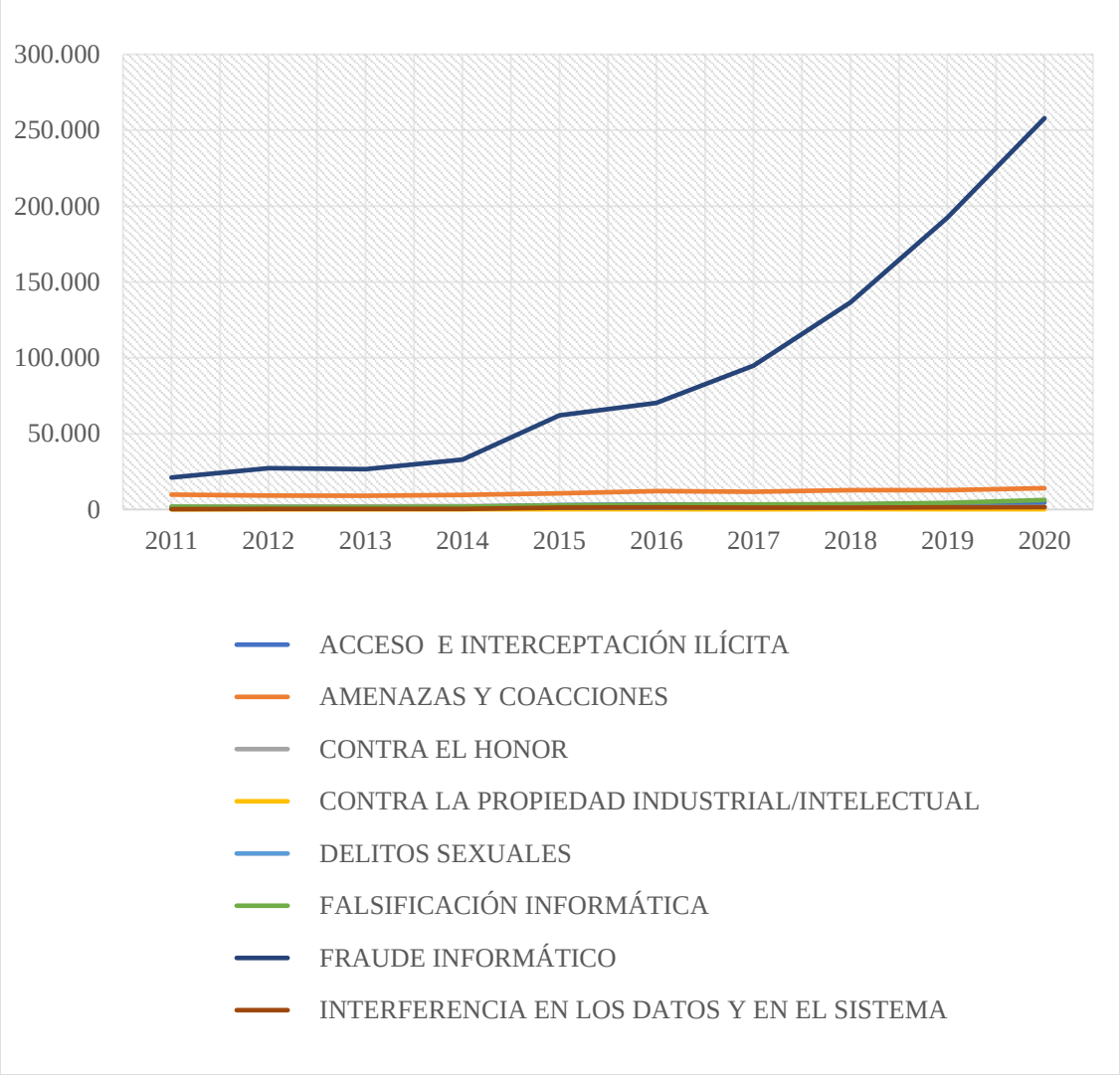


Fuente: elaboración propia a partir de los datos facilitados por el SEC.

En la tendencia general de la cibercriminalidad se aprecia un ascenso destacable en el grupo penal “fraude informático”, donde muestra claramente que es la conducta delictiva prevalente en el ciberespacio respecto al resto de conductas, asumiendo el mayor peso de la ciberdelincuencia, como se puede observar en la figura 13.

Figura 13

Gráfico sobre la Evolución Significativa del Fraude Informático Respecto al Resto de Ciberdelitos.



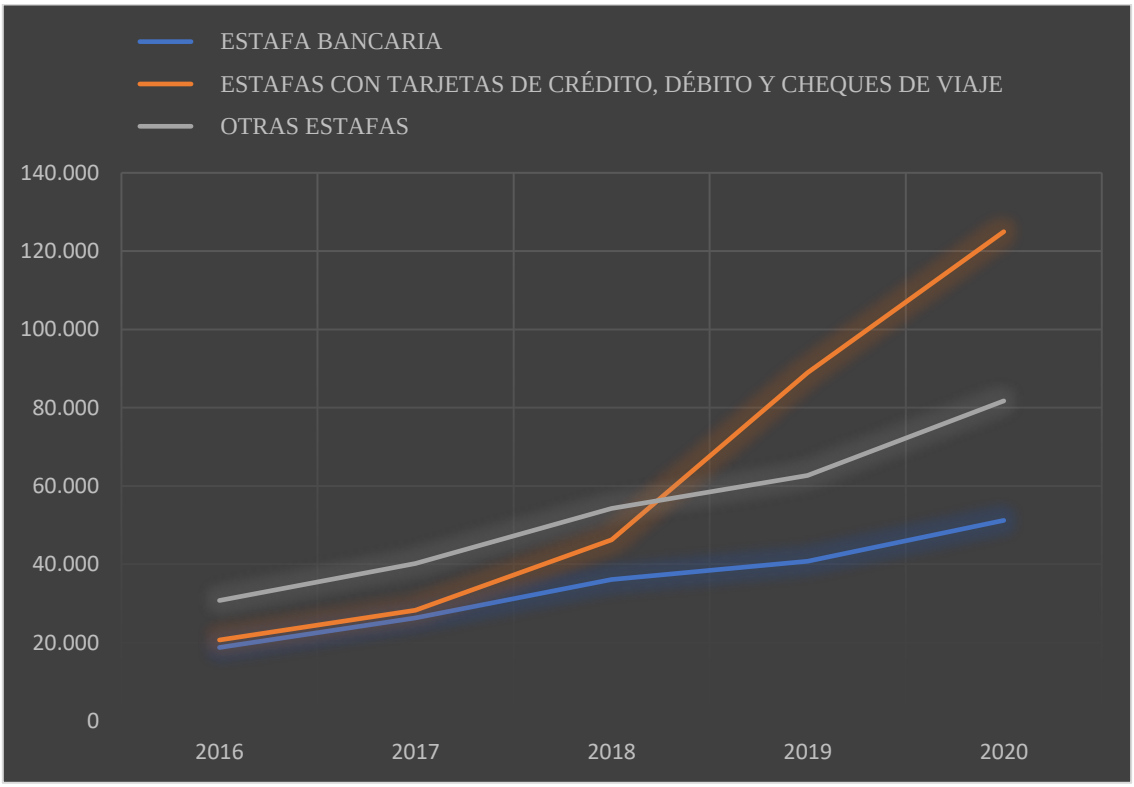
Fuente: elaboración propia a partir de los datos publicados por el SEC[27].

[27] Datos expuestos sobre Cibercriminalidad a lo largo de este apartado: https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/portal/datos.html?type=pcaxis&path=/Datos5/&file=pcaxi

En la figura 14 se aprecia la distribución de las diversas estafas que contempla el SEC como fraude informático, resultando la conducta más cometida en los últimos años la estafa con tarjetas de crédito, débito y cheques de viaje.

Figura 14

Gráfico sobre la Evolución de los Tipos de Estafas que Comprende el Fraude Informático.

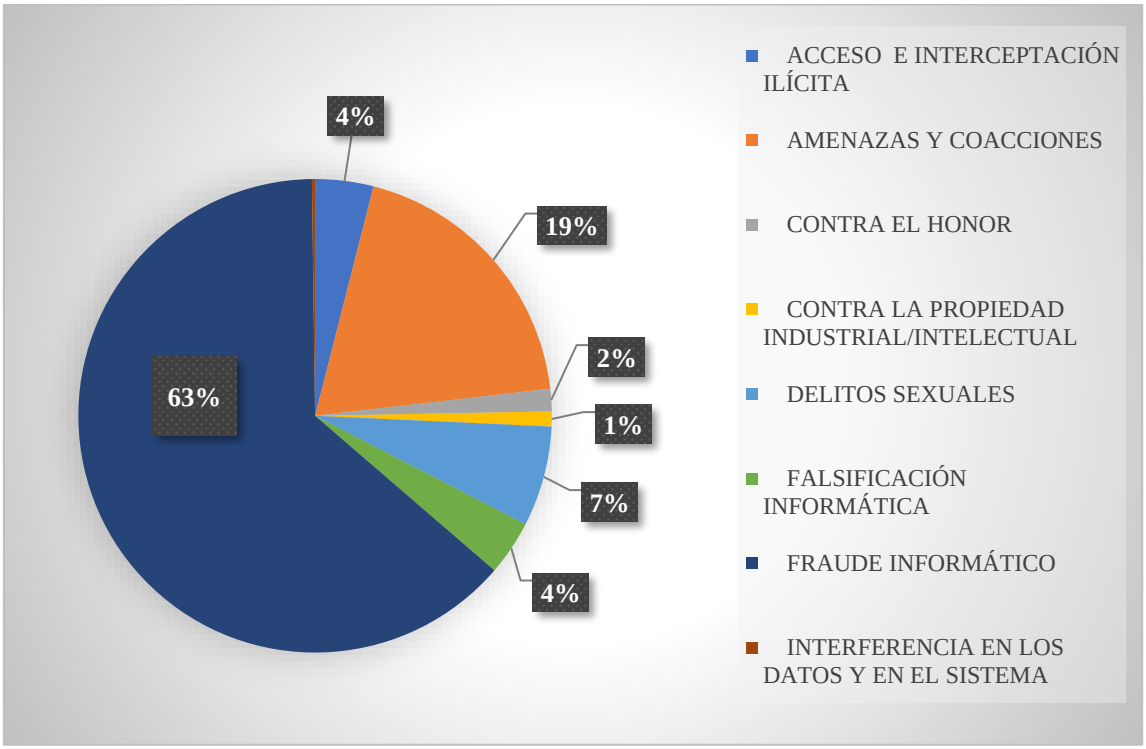


Fuente: elaboración propia a partir de los datos publicados por el SEC.

Según las series de investigaciones / detenciones contempladas en el módulo de cibercriminalidad, las Fuerzas y Cuerpos de Seguridad efectúan un total de 11.280 detenciones/ investigaciones en el año 2020, mayormente por conductas de fraude informático, delitos de amenazas y coacciones, lo que significa un ascenso del 26,5% respecto al año 2019. Respecto a las investigaciones y detenciones por fraude informático se registran un total de 7.159 casos, lo que se traduce a un ascenso del 44,7% respecto al año anterior. El fraude informático es la conducta ilícita con mayor incidencia dentro de este grupo, puesto que representa en el año 2020 más del 63% respecto al resto de grupos penales, como se refleja en la figura 15.

Figura 15

Gráfico sobre las Investigaciones Detenciones Efectuadas en el Año 2020 Correspondientes al Cibercriminalidad.

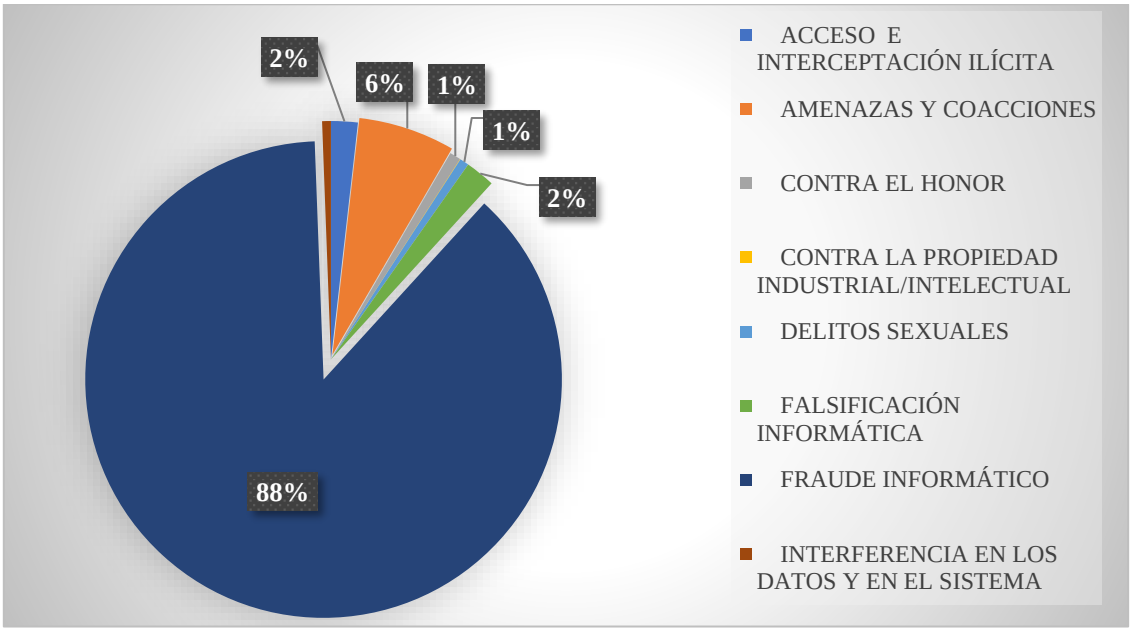


Fuente: elaboración propia a partir de los datos publicados por el SEC.

En los datos ofrecidos por las series de victimización se registran un total de 215.507 casos en el año 2020, lo que significa un 29,7% más que el año 2019, siendo en su mayoría víctimas por fraude informático, amenazas y coacciones. Respecto al grupo penal "fraude informático" se consignan un total de 188.852 casos en el mismo año, lo que se traduce a un incremento del 32,4% respecto al año anterior y representa casi el 88% del total de la victimización registrada, por lo que se puede decir que la principal conducta ilícita que sufren las víctimas son los fraudes informáticos / estafas como se indica en la figura 16. Cabe recordar que las serie no se encuentra completa puesto que la Ertzaintza no facilita datos de victimización, pero se considera la representación que mejor se aproxima de la realidad. Por otra parte, en cuanto al porcentaje que asume cada estafa de fraude informático sobre el total del resto de conductas, resultando significativo puesto que la estafa menos cometida "estafas bancarias" supera en un 3% al total del resto de conductas ciberdelictivas, como se puede observar en la figura 17.

Figura 16

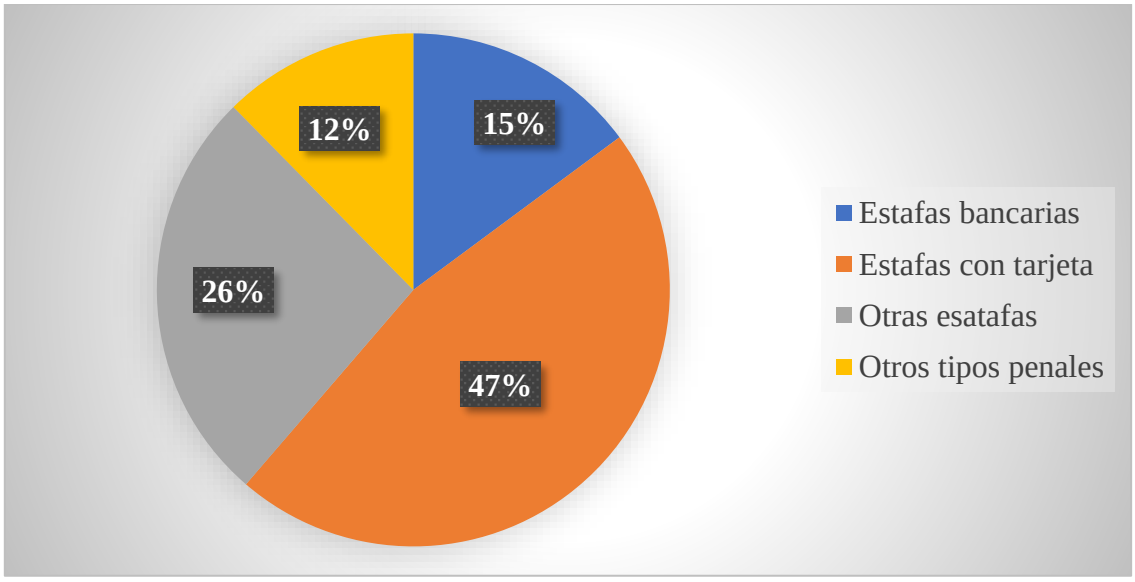
Gráfico de Victimización Registrada en el Año 2020 por Delitos Informáticos.



Fuente: elaboración propia a partir de los datos publicados en el SEC.

Figura 17

Gráfico sobre el Porcentaje que Ocupa las Conductas de Fraude Informático Respecto al Resto de Conductas Registradas en el Cibercrimen.



Fuente: elaboración propia a partir de los datos publicados por el SEC.

En definitiva, mientras que el crimen descendió un total de 432.696 casos en el año 2020, es decir, más de un 19% menos respecto al año anterior, el cibercrimen aumentó 69.661 nuevos casos, lo que se traduce a un 31,9% más respecto al año anterior. Esto se traduce a que el cibercrimen pasó de significar un 4,6% en el año 2016 a un 16,3% en el año 2020 sobre el total de las infracciones penales, lo que quiere decir que los delitos informáticos se están abriendo camino en la criminalidad como se puede observar en la tabla 18 y la figura 19.

Tabla 18

Hechos Conocidos de Cibercriminalidad y Total de Hechos Conocidos de Criminalidad.

HECHOS CONOCIDOS	2016	2017	2018	2019	2020
CIBERCRIMINALIDAD	92.716	117.399	160.729	218.302	287.963
TOTAL CRIMINALIDAD	2.009.690	2.045.784	2.131.118	2.199.475	1.766.779

Fuente: elaboración propia a partir de los datos publicados por el SEC.

Figura 19

Gráfico sobre la Evolución de la Cibercriminalidad Dentro de la Criminalidad.

Fuente: elaboración propia a partir de los datos publicados por el SEC.

El porcentaje que representa el fraude informático (estafa) respecto del número total de estafas registradas en la serie de criminalidad módulo “hechos conocidos” pasa de significar un 39% en el año 2016 a un 71,5% en el año 2020, lo que se traduce a un incremento exponencial de la estafa a través de medios informáticos sobre el total de estafas registradas, dato significativo que se aprecian en la tabla 20 y en la figura 21.

Tabla 20

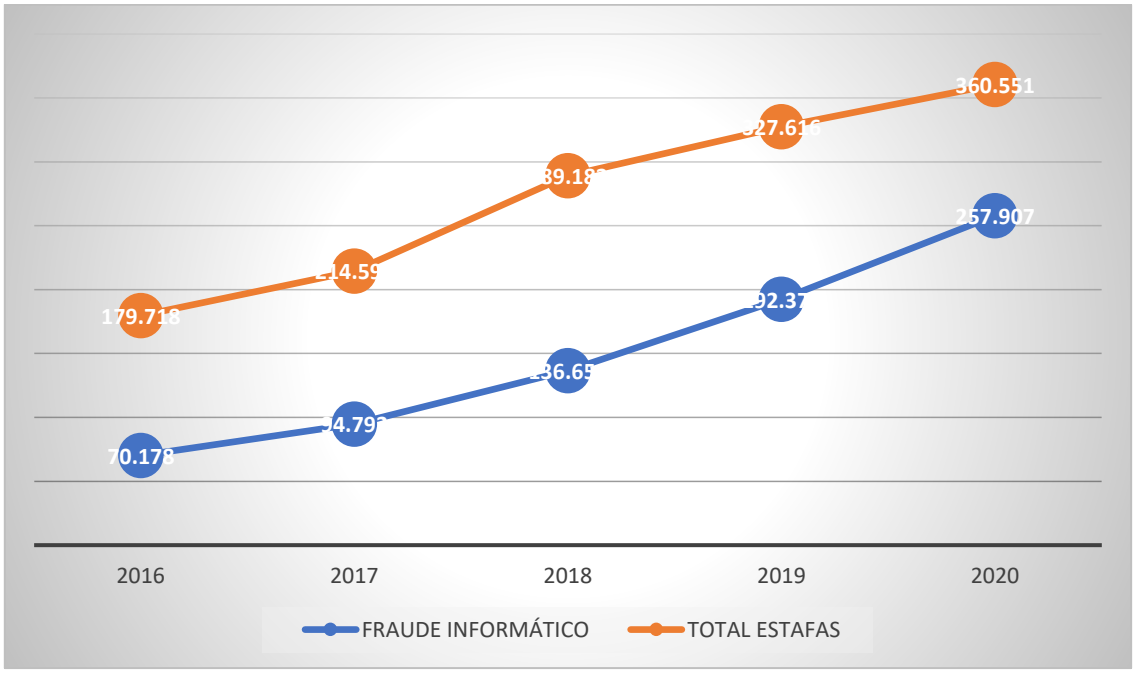
Fraude Informático Registrado en el Módulo de Cibercriminalidad y el Número Total de Estafas Registrados en el Módulo de Criminalidad.

	2016	2017	2018	2019	2020
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375	257.907
TOTAL ESTAFAS	**179.718**	**214.595**	**289.182**	**327.616**	**360.551**

Fuente: elaboración propia a partir de los datos publicados por el SEC.

Figura 21

Evolución del Fraude Informático Respeto al Total de Estafas Registradas.



Fuente: elaboración propia con los datos publicados en el SEC

Atendiendo a los datos expuestos, las Fuerzas y Cuerpos de Seguridad registran el fraude informático como la conducta ilícita que más incidencia tiene dentro de la cibercriminalidad, arrojando un resultado de un 86,9% en el año 2020, registrando una cifra del 48,45% en estafas con tarjetas de crédito, débito y cheques de viaje, un 31,7% en otras estafas y un 19,85% en estafas bancarias.

En último lugar, se considera apropiado citar los estudios realizados por Buil et al. (2020; 2021), Kemp et al. (2021) y Miró Llinares (2021), puesto que establecen relación entre el confinamiento social por la COVID-19, la reducción de la movilidad, la modificación de las actividades cotidianas de las personas, el aumento de la cibercriminalidad y la tendencia del fraude online. En ellos se registran los resultados recabados por Action Fraud[28], cuyos datos recoge las tendencias ciberdelictivas en Reino Unido entre los meses previos y durante los meses de confinamiento con motivo de la pandemia. En ellos se puede apreciar un aumento acelerado de la cibercriminalidad en el mes abril, alcanzando su punto álgido en el momento de más restricciones (Kemp et al., 2021). Las conductas que más destacan por su incremento son el hackeo con extorsión, piratería de las redes sociales, correo electrónico y el uso de virus informáticos. Estos delitos son considerados por los autores como ciberdependientes, puesto que sólo se pueden cometer utilizando sistemas informáticos (Buil et al., 2020). Asimismo, en el mes de junio se aprecia que la mayoría de estas conductas ilícitas reducen su incidencia y vuelven a su tendencia normal, alcanzando tasas normales previas al confinamiento (Miro Llinares, 2021).

Respecto a los datos sobre fraude online se puede observar cómo asciende de forma progresiva y permanece en los meses posteriores al confinamiento, por lo que sufre menos variación (Buil et al., 2020). El fraude en línea y estafas / phishing se clasifican dentro de los delitos cibernéticos (no ciberdependientes), refiriéndose a los delitos tradicionales que aumentan gracias a los avances tecnológicos, como sugiere la estadística registrada en los casos por fraudes en línea y estafas phishing (Buil et al., 2020). La modalidad que más destaca dentro de esta conducta es el fraude a través de compras online / subastas y fraude de noviazgo, apreciando un ascenso importante en el mes de abril (Kemp et al., 2021). Sin embargo, no todos los fraudes online aumentan, sino que algunos se ven reducidos con motivo de las circunstancias que rodean la crisis sanitaria,

[28] Centro Nacional sobre Información de Fraude y Delitos Cibernéticos de Reino Unido.

al estar relacionados con actividades del mundo físico, como puede ser la estafa de venta de entradas (Miró Llinares, 2021).

Del mismo modo, Action Fraud registra algunas conductas ilícitas que se llevan a cabo en el espacio físico. Concretamente, recopila la estadística de los delitos sobre violencia, daños, robo y hurto. Los gráficos muestran un descenso destacado durante los meses de más restricciones (Buil et al., 2021). Aunque estos resultados estadísticos coinciden con el periodo de confinamiento, no quiere decir que sea determinante para indicar el cambio de actividades relacionadas con Internet durante la pandemia (Buil et al., 2020).

6. Discusión.

El Instituto Nacional de Estadística (INE) publica los resultados de los estudios realizados a la población española y determina un incremento respecto al año anterior del 0,5% de viviendas con ordenador, un 4% más de equipos conectados a Internet y un 6,9% más de personas que compraron por Internet; datos que evidencian un incremento en la utilización de dispositivos tecnológicos, uso de Internet y compras online. En líneas semejantes se pronuncia "We Are Social", quienes registran en España un aumento de 1,8 millones de usuarios en Internet y 860.000 usuarios más en las redes sociales, resultados que se traducen a un incremento de las Tecnologías de Información y Comunicación durante el periodo de confinamiento. Según Eurostat España se sitúa por encima de la media de la Unión Europea respecto a viviendas con acceso a Internet (López et al., 2020), destaca el descenso del comercio minorista y el aumento acelerado de la venta por Internet, aspecto importante puesto que coincide con el periodo de confinamiento y determina un cambio en las actividades de los ciudadanos.

Por otra parte, el INE realiza un análisis de la movilidad de la población y determina un descenso respecto a meses anteriores, pasando de un 29,3% en noviembre de 2019 a un 7,61% en abril de 2020, aspecto que puede resultar obvio puesto que las medidas de confinamiento prohíben la movilidad general. Este fenómeno también es confirmado por Ghirelli et al. (2021), Kemp et al., (2021) y Miró Llinares (2021), quienes recogen en sus estudios datos que determinan la reducción de movilidad durante los periodos de más restricciones. Así pues, Ghirelli et al. (2021) incluye varios gráficos sobre la movilidad en España de datos procedentes de Google y Banco de España donde

se aprecia un descenso drástico del desplazamiento de personas en el mes de marzo y abril. Del mismo modo, Miró Llinares (2021) incluye varios gráficos con los datos ofrecidos por Apple y Google que indican la reducción de movilidad en los medios de transporte, así como, un descenso de desplazamientos entre zonas residenciales y zonas de comercios y ocio. Igualmente, Kemp et al. (2021) recoge varios gráficos sobre la movilidad de Reino Unido de datos procedentes de Google expresando una reducción de desplazamientos en los lugares de trabajo, comercio, zonas residenciales y estaciones de tránsito. Con estos resultados se puede deducir que existe cierta correlación entre el descenso de la movilidad personal como consecuencia de las medidas de confinamiento y el aumento del uso de las TIC junto con las conexiones a Internet.

Durante la pandemia, organismos como la Interpol (2020) y Europol (2020) se pronuncian e indican que en Europa se han detectado dominios web maliciosos con el nombre de coronavirus o semejantes, un aumento de riesgo contra la ciberseguridad de las empresas al tener que teletrabajar sus empleados y conectarse a la red empresarial desde sus equipos domésticos, así como, un incremento de ataques "ransomware" dirigidos a instituciones que pueden ser más vulnerables por la situación, como es el caso de hospitales o laboratorios. El phishing / estafa se presenta como una de las principales amenazas (59%), seguido del malware/ransomware (36%), dominios maliciosos (22%) y noticias falsas (14%). De igual modo se pronuncia el Centro Criptológico Nacional y anuncia en su informe que muchas de las amenazas se encuentran relacionadas con la pandemia, entre las que destaca un aumento de riesgos para las infraestructuras de las empresas al teletrabajar los empleados desde casa, mayor exposición de los sistemas públicos y organismos dedicados a la investigación de la COVID-19, como es el caso de farmacéuticas y laboratorios. Según el VIII Informe de Cibercriminalidad en España se detectan un incremento de incidentes de ciberseguridad, siendo los más frecuentes de tipo malware (35%) y fraude (32%), como consecuencia del aumento de actividades en el ciberespacio tras la adopción de las medidas restrictivas por la COVID-19.

Atendiendo al trabajo de Miró Llinares (2021), estos peligros se vieron confirmados por diversos estudios, entre los que se pueden desatacar: a) Google mediante sus informes de transparencia detecta un incremento acelerado de suplantación de sitios webs; b) Atlas recoge que el sector sanitario sufrió un 70% más de ataques que el año anterior, posiblemente por la situación de mayor vulnerabilidad que genera la pandemia;

c) Kapersky registra que el número de ataques ascendió de 28,8 millones en febrero a 96,7 millones en marzo, lo que se traduce a un aumento del 236%; d) la OMS detecta un aumento de phishing / spam y ponen de manifiesto que los ciberdelincuentes se hacen pasar por empleados de su organización y; e) también se detecta la venta online falsa de productos sanitarios y mascarillas que nunca llegan. No obstante, la detección de nuevos riesgos no determina el aumento de cibercriminalidad, sino más bien advierte los nuevos peligros. Por ello, hay que acudir a la institución que registra los datos concretos sobre esta modalidad criminal para conocer la evolución concreta en España de los delitos informáticos y aproximarse de alguna manera a la realidad. Así pues, se considera conveniente recurrir a los datos publicados por el Sistema Estadístico de Criminalidad procedentes de las infracciones registradas por las Fuerzas y Cuerpos de Seguridad, cuyos resultados expresan que la ciberdelincuencia en España ha experimentado un fuerte crecimiento coincidente con la pandemia, afectando a todos los ámbitos, tanto públicos como privados.

Los datos manejados por el Ministerio del Interior arrojan una cifra de 287.963 hechos en el año 2020, lo que supone un incremento en la cibercriminalidad del 246,7% en el plazo de 5 años. Dicho de otro modo, ha aumentado su peso dentro del conjunto de la criminalidad, pasando de un 4,6% en el 2016 a un 16,3% en el año 2020 respecto al número total de delitos. La Unión Europea pone de manifiesto que la cibercriminalidad representa 5,5 billones para la economía global, lo que se traduce a la mayor transferencia ilícita de riqueza por encima de la derivada del tráfico de drogas[29]. Respecto al año de pandemia, la criminalidad se ve reducida en más de un 19% mientras que la cibercriminalidad asciende un 31,9%, probablemente por la reducción de oportunidades en el espacio físico y el aumento de oportunidades en el ciberespacio con motivo de la pandemia, puesto que el Gobierno obligó a los ciudadanos a permanecer en sus domicilios sin poder salir, salvo en casos determinados. De esta manera, los datos publicados por el SEC muestran un descenso de la criminalidad por debajo de su pronóstico y un aumento de cibercriminalidad por encima de su tendencia, probablemente como consecuencia de las medidas de confinamiento social tras la pandemia por la COVID-19.

[29] https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2021/090321-cibercriminalidad.aspx

En la misma dirección se pronuncian investigaciones como las realizadas por Buil et al. (2020; 2021), Kemp et al. (2021) y Miró Llinares (2021) que evidencian un descenso de la delincuencia en el mundo físico y un aumento de ciberdelincuencia durante los meses de más restricciones por la COVID-19. Los datos estadísticos recabados por Action Fraud[30] reflejan un descenso pronunciado en el espacio físico de los delitos de daños, violencia, robo y hurto (Buil et al., 2021), registrando sus niveles más bajos en el mes de abril. Este hecho cambia en el mes de junio puesto que comienza a recuperar su tendencia. Respecto al ciberespacio, registra un aumento del hackeo con extorsión, piratería de las redes sociales, correo electrónico y el uso de virus informáticos en el ciberespacio, alcanzando su punto álgido en el mes de abril, circunstancia que cambia puesto que en el mes de junio recupera su tendencia habitual. Sin embargo, el fraude online se aprecia como asciende y se mantiene durante el confinamiento, por lo que sufre menos variación que el resto de las conductas ciberdelictivas (Buil et al., 2020). Cabe aclarar que no todos los fraudes online aumenten de la misma manera. El fraude online en subastas se ve incrementado en un 52%, mientras que aquellos fraudes relacionados con el espacio físico se ven reducidos, como es el caso de la estafa de venta de entradas (Miró Llinares, 2021). Estos resultados sugieren que hay un desplazamiento de oportunidades delictivas como consecuencia del cambio de rutinas, al cambiar actividades que antes se llevaban a cabo en el mundo físico y que pasan a realizarse en el mundo virtual. Parece ser que tiene relación la tendencia delictiva con las medidas de confinamiento.

En líneas similares se pronuncian los datos publicados por el SEC respecto al fraude informático / estafas, pues registra un ascenso de 65.532 casos en el año 2020, lo que supone un 34,6% más que el año anterior. De acuerdo con la tabla del módulo de cibercriminalidad, el SEC divide el fraude informático en tres tipos de estafas, registrando en el año 2020 un total de 124.957 casos de estafa con tarjetas de crédito, débito y cheques de viaje, 81.737 casos de otras estafas y 51.213 casos de estafas bancarias, lo que significa un peso del 48,5%, 31,7% y 19,85% respectivamente relativo al grupo de fraude informático conocido ese mismo año. Por tanto, la modalidad de fraude más cometida a través de las TIC son las estafas con tarjetas de crédito, débito y cheques de viajes, incrementándose en el año 2020 un 40,5% respecto al año 2019. Igualmente, se aprecia un incremento en las otras modalidades de estafa respecto al año anterior, resultando un

[30] Centro Nacional sobre Información de Fraude y Delitos Cibernéticos de Reino Unido.

aumento del 30,45% en otras estafas y un ascenso del 25,6% en estafas bancarias. Otro dato destacable es el peso que asume el fraude informático "estafas" respecto a la totalidad de estafas registradas en las series de criminalidad, puesto que pasa de un 39% en el año 2016 a un 71,5% en el año 2020. Estos datos ponen de relieve la evolución del fraude a través de Internet, lo que sugiere cierto desplazamiento en esta conducta concreta.

Después de exponer los datos principales, conviene recordar los aspectos que han servido como base para el estudio del fraude a través de Internet y el desplazamiento de oportunidades, realizando especial hincapié durante la pandemia por la COVID-19, con el fin de aclarar puntos de conexión. Se parte de la base que el desarrollo de las TIC ha conllevado el crecimiento tecnológico de las sociedades (ITU, 2009) e Internet se considera el medio más importante de comunicación personal (Miró Llinares, 2013b), hasta el punto de que se ha popularizado de tal manera que se ha convertido en una parte primordial de las vidas de las personas. En las mismas líneas se pronuncian los datos expuestos por el INE, CIS y We Are Social. Sin embargo, no todo es positivo, dado que puede poner en riesgo algunos derechos jurídicos, como ocurre con el fraude informático (Mayer, 2017). La ciberdelincuencia se presenta como un fenómeno llevado a cabo mediante las TIC y atentan contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos (Convenio sobre la Ciberdelincuencia de Budapest, 2001). De ahí surge la preocupación de los poderes públicos para actualizar los marcos normativos, puesto que hay que proteger los derechos de los ciudadanos en el ciberespacio (Tejero, 2019), inquietud lógica atendiendo a los datos de cibercriminalidad. Esto quiere decir que la evolución tecnológica proporciona ventajas para las sociedades, pero a su vez genera nuevas oportunidades delictivas, convirtiendo el ciberespacio en un medio para cometer el ilícito (Miró Llinares, 2011).

Respecto al fraude informático ocupa un lugar indiscutible en la cibercriminalidad (Miró Llinares, 2013a) y tiene relación con el delito de estafa, pues tiene una evidente connotación patrimonial. Esta afirmación queda sustentada con los datos expuestos por el SEC. Además, guarda un carácter pluriofensivo puesto que afecta al patrimonio de la persona y en términos generales afecta a la funcionalidad informática (Mayer, 2017). La estafa común y la estafa informática se regulan en el mismo artículo, pero en diferentes apartados, puesto que se diferencian en su modo de comisión. Como se ha visto hasta el

momento, puede adquirir diferentes formas (Miró Llinares, 2011). La estafa informática se relaciona con el phishing / pharming (Mayer y Oliver, 2020) y consiste en obtener datos bancarios o de tarjetas de crédito mediante manipulación informática (Sánchez, 2012) para posteriormente realizar una transferencia a su favor en perjuicio de la víctima (Oxman, 2013). La estafa online se encuadra dentro de la estafa común y se obtiene un beneficio a través de la Red (López, 2018) mediando engaño, error de la víctima, ánimo de lucro, intención y disposición patrimonial ajena (Mayer, 2017); es decir, es un delito tradicional que utiliza los avances tecnológicos para su comisión, quedando delimitado dentro de los delitos cibernéticos (Buil et al., 2020). En este sentido, la estafa online y la estafa informática comparten ciertos elementos como la intención, el ánimo de lucro y la disposición patrimonial, pero se diferencian en su modo de comisión, puesto que la estafa informática requiere manipulación informática mientras que la estafa común exige causar engaño o error en la víctima. Por ende, las estafas cometidas a través de Internet tienen diferencias en su modo de comisión, pero comparten ciertas ventajas como: anonimato, dificultades para su identificación y posibilidades de alcanzar mayor número de víctimas (Miró Llinares, 2011).

Otro aspecto que ha influido de alguna manera en la evolución de la cibercriminalidad y del fraude a través de Internet son los efectos provocados por las medidas de confinamiento (Rodríguez, 2021). En este sentido se pronuncian diversos estudios que expresan cierta relación entre el aislamiento social por la COVID-19, el uso de tecnologías y el aumento de la cibercriminalidad (Buil et al., 2020; 2021; Kemp et al., 2021; Miró Llinares, 2021), puesto que las circunstancias que rodean la pandemia conllevaron a que multitud de ciudadanos realizaran actividades a través de la Red que resultaban nuevas y antes no las llevaban a cabo a través del ciberespacio (Miró Llinares, 2021). La estadística sobre la cibercriminalidad sugiere que las estafas en línea / phishing han aumentado con motivo de los avances tecnológicos como indica Buil et al. (2020).

Referente a lo expresado, cabe considerar que multitud de conductas de estafa online no requieren que su autor tenga conocimientos informáticos, sino solo necesita disponer de un dispositivo tecnológico que permita conectarse a Internet y tener ciertas habilidades para perpetrar la conducta ilícita. Como bien se ha reflejado en apartados anteriores, Internet permite contactar cómodamente con personas de cualquier parte del mundo sin tener que entrar en contacto físico con la víctima (Devia, 2017), por lo que su

conducta puede llegar a cualquier lugar sin tener que moverse del sitio. Esta característica junto con otros aspectos que giran a su alrededor dificulta determinar la autoría, por lo que se puede considerar una ventaja más que proporciona este medio al cibercrimen. Asimismo, su carácter expansivo permite que la conducta alcance un mayor número de víctimas (Miró Llinares, 2011), por lo que puede ser otro de los motivos que incite a realizar la acción delictiva a través de Internet. Aunque son aspectos que pueden promover el desplazamiento del estafador tradicional del mundo físico al virtual (modalidades de estafa que no requiere conocimientos técnicos informáticos) no hay que aventurarse a realizar ciertas afirmaciones, puesto que las teorías de la oportunidad no sostienen el desplazamiento de los delitos de un lugar a otro, pero tampoco quiere decir que no se haya producido cierto desplazamiento (Miró Llinares, 2021).

Por otra parte, atendiendo a los estudios y datos manejados, las circunstancias en tiempos de COVID-19 generaron el aumento de las oportunidades para los ciberdelincuentes y un mayor número de víctimas en Internet. Del mismo modo, los resultados sugieren que la estafa se ha desplazado al ciberespacio, teniendo en cuenta la comodidad que ofrece la Red, ya que no es necesario tener conocimientos informáticos, sino que solo es necesario disponer de un dispositivo tecnológico que permita conectarse a Internet y ciertas habilidades para poder llevar a cabo la conducta. Sin embargo, esta probabilidad no es asumible en otros tipos penales, como es el ejemplo de la estafa informática, que sí requiere conocimientos informáticos, al igual que ocurre con otros tipos de ilícitos que solo se pueden perpetrar en el espacio físico. No hay que obviar que las conductas delictivas que se puedan realizar a través del ciberespacio se encuentran limitadas a las posibilidades que ofrece el propio medio (Solari, 2021).

Sin entrar en más valoraciones de momento, el fraude informático "estafa" en España es la conducta ilícita más cometida en el ciberespacio según los datos registrados en los últimos años, significando en el año 2020 un 86,9 % de los casos totales registrados en cibercriminalidad y un 14,6% respecto a los casos totales de criminalidad. Igualmente, se aprecia que un 63% de las investigaciones detenciones y un 88% de los casos de victimización corresponde a este grupo delictivo. Es decir, la mayoría de los datos evidencian el aumento de riesgo en el ciberespacio en tiempos de COVID-19, probablemente por el desplazamiento de oportunidades como consecuencia del cambio de actividades cotidianas del mundo físico al virtual, ya que muchas personas comienzan

a realizar actividades como teletrabajar, compras online, transacciones bancarias, consultas y gestiones a través de webs, entre otras; lo que significa un aumento de riesgos para aquellos usuarios que realizan nuevas actividades sin disponer de los conocimientos adecuados. Vale decir que los riesgos no vienen marcados porque uses más Internet, sino más bien por el tipo de actividad que realices a través de este (Miró Llinares, 2013b). Estas son algunas de las razones que pueden haber promovido el aumento de la cibercriminalidad, puesto que Internet ofrece gran comodidad para perpetrar los injustos y obtener beneficios, desapareciendo por completo las limitaciones espacio-temporales (Miró Llinares, 2011).

7. Conclusión.

El presente trabajo trata de abordar el fraude a través de Internet y su evolución durante los tiempos de COVID-19. Parte de la suposición que las medidas de confinamiento impuestas por el Gobierno con motivo de la pandemia generan un cambio de rutinas en los ciudadanos de manera que muchas actividades pasan del mundo físico al mundo virtual, por lo que provocan un desplazamiento de oportunidades delictivas y, por consiguiente, un aumento de fraude a través de Internet. Pues bien, mediante los resultados obtenidos se trata de despejar algunas de las cuestiones planteadas. Para ello se va a procurar de resolver por separado los factores que inciden en la evolución de este ilícito penal con el objeto de comprender mejor las posibles causas / efectos del fenómeno.

Los datos sobre el fraude informático en España sugieren que es el delito más prevalente registrado dentro del módulo de cibercriminalidad durante los últimos años. En el año 2020 representa el 86,9% de la cibercriminalidad con respecto al número total de hechos conocidos, lo que quiere decir que es el ciberdelito que con mayor frecuencia se comete en el ciberespacio. Esta aserción se confirma por diferentes estudios. También cabe considerar que las cifras registradas representan una parte de la realidad, puesto que no se pueden conocer todos los casos reales al existir la cifra negra (Montiel, 2016), pero se considera una buena manera de aproximarse a los riesgos sociales.

Los resultados apuntan a que el desarrollo tecnológico y el incremento de la utilización de Internet va paralelo a la evolución social y al uso del ciberespacio, hecho que sugiere un cambio de hábitos en los ciudadanos y un aumento de oportunidades delictivas. Esta combinación de factores parece marcar la tendencia de la

cibercriminalidad, suposición que viene afirmada por diversos estudios, destacando los realizados por Miró Llinares (2021), Buil et al. (2020; 2021) y Kemp et al. (2021).

Las restricciones por la pandemia conllevan a que ciudadanos sin las nociones básicas se expongan en la Red y efectúen actividades que antes no habían realizado (Miró Llinares, 2021). Estas circunstancias sumadas a la situación de incertidumbre colocan a multitud de personas e instituciones en una posición de vulnerabilidad, hecho del que sacan provecho los cibercriminales (Interpol, 2020; Europol, 2020; CCN-CERT, 2020).

Los documentos analizados evidencian un aumento de cibercriminalidad durante el periodo de más restricciones, lo que sugiere que la pandemia trae más oportunidades delictivas al ciberespacio, al igual que se ve reducida posterior al confinamiento, probablemente por el levantamiento de medidas (Buil et al., 2020; 2021; Kemp et al., 2021; Miró Llinares, 2021). A pesar de ello, se aprecia que la conducta del fraude en compras online se mantiene en la Red, posiblemente porque ciertas actividades que antes de la pandemia no se hacían con tal habitualidad, se comienzan a normalizar durante y después del confinamiento (Miró Llinares, 2021).

En cuanto a las cuestiones planteadas sobre si la crisis sanitaria por la COVID-19 ha sido la causa del cambio de rutinas cotidianas, desplazamiento de oportunidades delictivas del mundo físico al virtual, la aceleración de la expansión tecnológica y el uso de Internet, atendiendo a los resultados obtenidos durante la pandemia, se aprecia que las rutinas cotidianas sí se vieron modificadas como consecuencia del confinamiento, puesto que las personas no podían salir a la calle y multitud de actividades se tuvieron que realizar a través de la Red como el teletrabajo o las compras online. Esto no quiere decir que antes de la pandemia no se realizaran dichas actividades, sino que muchas personas comenzaron a realizarlas con motivo de la situación (Miró Llinares, 2021).

Respecto al desplazamiento de oportunidades delictivas, es evidente que el ciberespacio se encuentra limitado a los delitos que se puedan llevar a cabo a través de la Red, puesto que hay conductas ilícitas que resultan imposibles de cometer. No obstante, en relación con los comportamientos que se pueden llevar a cabo, los datos sugieren que puede existir un desplazamiento en determinados ilícitos, como el caso concreto de la estafa a través de Internet, ya que los datos reflejan un ascenso progresivo respecto a años anteriores y un aumento exponencial en tiempos de pandemia. En este sentido se

pronuncia Buil et al. (2020) cuando se refiere a que los delitos de fraude en línea se ven favorecidos por el avance tecnológico, pero es muy precipitado afirmar el desplazamiento, puesto que requiere un estudio pormenorizado del fenómeno. Lo que sí que sugieren los datos revisados es que existe correlación entre actividades cotidianas y oportunidades delictivas.

Referente a la duda de si la pandemia ha acelerado el uso de las TIC, los datos indican que han aumentado durante las medidas de confinamiento, por lo que se entiende que de forma indirecta y debido a las circunstancias que rodean la pandemia sí ha fomentado el uso masivo de las tecnologías y el acceso a Internet, afirmación que se sustentan en los estudios y resultados analizados.

En alusión a la cuestión sobre si las particularidades que rodean la pandemia fue la causa de la aceleración del fraude informático, multitud de instituciones alertaban de los nuevos riesgos como consecuencia de los usos en tiempos de confinamiento y los datos evidencian un aumento de la cibercriminalidad y del fraude informático, por lo que de una manera indirecta se puede considerar un factor acelerador de su evolución pronosticada (Miró Llinares, 2021).

En cuanto al aumento de los fraudes a través de Internet, Action Fraud ponen de manifiesto que no todos los ciberfraudes ascendieron de la misma manera, puesto que detectaron un aumento de fraude online en subastas y un descenso del fraude en entradas para espacios físicos, coincidiendo con el periodo de confinamiento (Miró Llinares, 2021). En este estudio se relacionan las actividades rutinarias con las oportunidades delictivas y parecen marcar las tendencias del crimen.

En este trabajo se cuestiona la relación entre cibercriminalidad y la pandemia, puesto que las medidas de confinamiento trajeron nuevos tiempos a la sociedad que afectaron a diferentes ámbitos de su vida, además de apreciar durante este periodo un aumento de los cibercrímenes. A pesar de ello, se entiende que la crisis sanitaria como tal no tiene una relación directa con la criminalidad, sino que son las circunstancias promovidas por las restricciones las que guardan cierta relación con ella. Dicho de otra manera, son los quehaceres cotidianos de los ciudadanos en tiempos de coronavirus los que guardan relación directa con el incremento de oportunidades delictivas en el

ciberespacio, como bien se puede deducir de los resultados ofrecidos por los diferentes estudios y, por ende, del aumento de la cibercriminalidad.

Por todo lo expuesto, la voluntad del presente ha sido tratar de resolver las cuestiones planteadas mediante la exposición de los resultados que barajan diversas investigaciones. No obstante, hay que recordar que cuenta con limitaciones, puesto que analiza algunos de los muchos trabajos existentes, lo que quiere decir que no se pueden sacar conclusiones definitivas. Teniendo en cuenta este aspecto, se considera que hay cierta aproximación entre el avance tecnológico y los riesgos que asumen las sociedades en el ciberespacio.

Como breves consideraciones respecto al fenómeno tratado, se puede apreciar que las instituciones pretenden poner remedio a los riesgos que se producen en el ciberespacio mediante la regulación normativa y estrategias reactivas. En cambio, su carácter global y transnacional lo convierte en una tarea muy difícil de ejecutar. Hay que tener en cuenta que el mundo de la tecnología evoluciona con tal rapidez que lo que vale hoy no sirve para mañana (Miró Llinares, 2011). Pero esto no significa que los problemas se deban dejar de lado, sino que debe de servir para tomar conciencia de ello, evaluar el problema y escoger la estrategia más adecuada. Solo mediante su estudio constante se puede obtener una buena aproximación a la realidad y solución del problema.

En último lugar y considerada la principal, hay que tener en cuenta que de nada sirve que las instituciones intenten poner remedio al problema de la cibercriminalidad si la población usuaria no es consciente de los riesgos que asume cuando realiza ciertas actividades en Internet, o más bien no quiere adoptar las medidas de prevención advertidas. Como recoge Devia (2017) al principio de su trabajo:

> *"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores (Kevin MITNICK – hacker)".*

Así pues, teniendo en cuenta el eslabón más débil en este entramado fenómeno, conviene plantear futuras políticas sociales que implanten medidas de concienciación y prevención, con el objeto de evitar que los usuarios de las TIC, en cierta medida, puedan

convertirse en víctimas de estos ciberdelitos. En definitiva, como sugieren algunos de los estudios analizados, si no hay oportunidad delictiva a través del medio, difícilmente puede haber delito, por lo que esta reflexión puede servir de base para futuras estrategias de prevención en el ciberespacio.

8. Referencias bibliográficas.

Aguilar Cárceles, M. M. (2015). Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. *Revista Criminalidad*. *Vol. 57* (1), 121-135.

Alas Rojas, D. L. (2015). La estafa en las prestaciones ilícitas: Fundamentos para su atipicidad. *Derecho y Cambio Social*, *12* (39), 18.

Álvarez Vizcaya, M. (2001). Consideraciones político-criminales sobre la delincuencia informática: el papel del derecho penal en la red. *Cuadernos de Derecho Judicial*, Nº 10, 255-280.

Baena Paz, G. (2017). *Metodología de la Investigación*. *Ed. 3.* Grupo Editorial Patria.

Balmaceda Hoyos, G. (2011). El delito de estafa informática en el derecho europeo continental. *Revista de derecho y ciencias penales: Ciencias Sociales y Políticas*, (17), 111-150.

Bicarregui Garay, J. (2008). El fraude on-line: Nuevo escenario, vieja picaresca. *Boletín de Estudios Económicos*, *63*(194), 311.

Brantingham, P.J, y Brantingham, P.L. (1993a). Nodes, Paths and Edges. Considerations on the Complexity of Crime and the Physical Environment. *Journal of Environmental Psychology*, *13* (1), 3-28.

Brantingham, P. J. & Brantingham, P. L. (1993b), Environment, Routine and Situation. Toward a Pattern Theory of Crime. *Advances in Criminological Theory, 5* (2), 259-294.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.

Buil-Gil, D., Moneva, A., Kemp, S., Díaz-Castaño, N., & Miró-Llinares, F. (2020). Recorded cybercrime and fraud trends in UK during COVID-19.

Cámara Arroyo, S. (2020). La Cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*, (60), 470-512.

Centro Criptológico Nacional. (2020). *Ciberamenazas y tendencias*. *Análisis de las ciberamenazas nacionales e internacionales de su evolución y tendencias futuras*. CCN-CERT IA-13/20. Ministerio de Defensa. Gobierno de España.

Centro de Investigaciones Sociológicas. Barómetro de marzo de 2015. Estudio Nº 3057. Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática. Gobierno de España.

Cereceda, J., Sánchez, F., Herrera, D., Martínez, F., Rubio, M., Gil, V., Santiago, A., Gómez, M. (2019). *Estudio sobre la Cibercriminalidad en España*. VII Informe sobre la Cibercriminalidad. Ministerio del Interior. Gobierno de España.

Cerezo Domínguez, A. I., & García Cornejo, R. (2020). La ciberdelincuencia en España: Un estudio basado en las estadísticas policiales, (34), 91-106.

Chiriguayo Lozano, S. J. (2015). Comercio electrónico: Importancia de la seguridad en las transacciones electrónicas, amenazas y soluciones a implementar. *Revista Empresarial*, *9*(35), 8-14.

Cockburn, W., & Hurtado, M. (2021). Perspectiva europea sobre los riesgos laborales en el ámbito del teletrabajo. *Archivos de Prevención de Riesgos Laborales*, *24*(2), 95-98.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach, *American Sociological Review*, 588-608.

Constitución Española de 1978. *Boletín Oficial del Estado* núm. 311, de 29 de diciembre de 1978. España.

Convenio sobre la Ciberdelincuencia celebrado en Budapest el 23 de noviembre de 2001. Serie de Tratados Europeos Nº 185, 1-26.

Cornish, D. & Clarke, R. V. (1986). The reasoning criminal: Rational choice perspectives on offending. NuevaYork: Springer-Verlag.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime prevention studies*, *16*, 41-96.

Crespo-Pazmiño, D. (2019). Ciberseguridad y Derechos Humanos: respuestas estatales e individuales a las revelaciones de espionaje de Snowden. *Comentario Internacional. Revista del Centro Andino de Estudios Internacionales*, (19), 77-98.

Devia González, E. A. (2017). El delito informático: Estafa informática del artículo 248.2 del código penal. (Tesis Doctoral), Universidad de Sevilla.

Espinosa Sánchez, J. F. (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red. *La Razón histórica: revista hispanoamericana de historia de las ideas políticas y sociales*, (44), 153-173.

Europol (2020). Catching the virus cybercrime, desinformation and the COVID-19 pandemic.

Eurostat (2020). Venta de comercio minorista en España. Primer semestre. Oficina Estadística de la Unión Europea.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. Police research series, *paper*, *98*(1-36), 10.

Fernández Delpech, H. (2014). Manual de derecho informático. *Abeledo Perrot. Buenos Aires*. *37* (1), 91-41.

Fernández Teruelo, J. G. (2007). Respuesta Penal frente a fraudes cometidos en Internet: estafa, estafas informáticas y los nudos de la red. *Revista de Derecho Penal y Criminología*, (19), 217-243.

Ghirelli, C., Gil Martín, M., Hurtado López, S., & Urtasun Amann, A. (2021). Relación entre las medidas de contención de la pandemia, la movilidad y la actividad económica. *Documentos Ocasionales/Banco de España, 2109*.

González-Rivera, J. A., & Álvarez-Alatorre, Y. (2020). COVID-19, infodemia y un buen café. *Revista Caribeña de Psicología*, *Vol. 4* (2) 81-87.

Hernández Sampieri, R., Fernández Collado, C. & Baptista Lucio, M. (2014). Metodología de la Investigación Sexta Edición.

Instituto Nacional de Estadística (2020a). *Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares.* Organismo adscrito al Ministerio de Asuntos Económicos y Transformación Digital. Secretaría de Estado de Economía y Apoyo a la Empresa.

Instituto Nacional de Estadística (2020b). *Análisis de la movilidad personal nacional durante la crisis sanitaria por la COVID-19*. Organismo adscrito al Ministerio de Asuntos Económicos y Transformación Digital. Secretaría de Estado de Economía y Apoyo a la Empresa.

Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Boletín Oficial del Estado Nº 226, de 17 de septiembre de 2010, 78847-78896. Referencia: BOE-A-2010-14221.

Interpol (2020). *Cybercrime: COVID-19 Impact*. Secretaria General de la Interpol (agosto), 1-20.

Izquierdo Sánchez, C. (2016). *Engaño y silencio: bases para un tratamiento unitario de la comisión activa y omisiva del delito de estafa* (Tesis Doctoral, Universitat Pompeu Fabra).

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, *37*(4), 480-501.

Kemp, S., & Moneva, A. (2020). Fraude online vs. offline: factores predictores de victimización y su impacto. *InDret: revista para el análisis del derecho, (1)* 424-444.

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Boletín Oficial del Estado Nº 233, de 29 de septiembre de 2015, 87106-87117. Referencia: BOE-A-2015-10389.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado Nº 281, de 24 de noviembre de 1995. Referencia: BOE-A-1995-25444.

Leyton Jiménez, J.F. (2014). Los elementos típicos del delito de estafa en la doctrina y jurisprudencia contemporáneas. *Revista Ars Boni et Aequi*. *10* (2*)* 123-161.

López, J., Sánchez, F., Martínez, F., Rubio, M., Gil, V., Santiago, A., Gómez, M., (2020) *Estudio sobre la cibercriminalidad en España.* VIII Informe sobre la Cibercriminalidad. Ministerio del Interior. Gobierno de España.

López Pesquera, B. (2018). El delito de estafa cometido a través de las redes sociales: problemas de investigación y enjuiciamiento. *IDP: Revista de Internet, Derecho y Politica*, *27*.

Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista chilena de derecho*, *44*(1), 261-285.

Mayer Lux, L., & Oliver Calderón, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista chilena de derecho y tecnología*, *9*(1), 151-184.

Méndez, L., & Pérez, F. (2020). El grooming como factor de impacto en tiempo de pandemia. *Diario La Ley*, (9752), 4.

Miró Llinares, F. (2011). La oportunidad criminal en el ciberespacio. *Revista Electrónica de Ciencia Penal y Criminología*, *7*, 1-07.

Miró Llinares, F. (2013a). La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing. *Revista Electrónica de Ciencia Penal y Criminología*, (15), 12.

Miró Llinares, F. (2013b). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista española de investigación criminológica*, *11*, 1-35.

Miró Llinares, F. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. *IDP: revista d'Internet, dret i política*, (32).

Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the yahoo boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, *14*(1), 300-315.

Montiel Juan, I. (2016). Cibercriminalitat social juvenil: la xifra negra. *IDP: revista d'Internet, dret i política*, (22).

Moreno-Fleitas, O. E. (2020). La divulgación de la información en la encrucijada de la crisis del COVID-19 en Paraguay. Reacciones y trasmisión de datos falsos y científicos a través de las redes sociales y los medios masivos. Paraguay: *Revista Sociedad Científica*, *25* (1), 58-85.

Naciones Unidas para la Tecnología de la Información y la Comunicación (2009). *El ciberdelito: guía para los países del organismo internacional de las Recursos jurídicos contra el ciberdelito.* Unión Internacional de telecomunicaciones (ITU).

Núñez Pérez, F.V. & Carhuancho Zaldaña, B. (2020). Ciberdelincuencia en tiempos de Covid-19: ¿la vulneración a derechos constitucionales? *Lumen. Vol. 16* (1), 93-100.

Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo Nacional de Ciberseguridad. Boletín Oficial del Estado Nº 20, 23 de enero de 2018, 8186-8190. Referencia: BOE-A2018-799.

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del" phishing" y el" pharming". *Revista de derecho (Valparaíso)*, (41), 211-262.

Pérez San-José, P., Gutiérrez, C., Fuente, S., Álvarez, E., García, L. (2012). Guía para usuarios: identidad digital y reputación online. Instituto Nacional de Tecnologías de la Comunicación. Ed. Julio de 2012.

Pérez Zúñiga, R., Mercado Lozano, P., Martínez García, M., Mena Hernández, E., & Partida Ibarra, J. A. (2018). La sociedad del conocimiento y la sociedad de la información como la piedra angular en la innovación tecnológica educativa. *RIDE. Revista Iberoamericana para la Investigación y el Desarrollo Educativo, 8*(16), 847-870.

Picotti, L. (2013). La tutela penale della persona e le nuove tecnologie dell'informazione. *Tutela penale della persona e nuove tecnologie*, 29-75.

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad *URVIO: Revista Latinoamericana De Estudios De Seguridad*, (20), 80-93.

Posada Maya, R. (2017). EL cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Revista Nuevo Foro Penal, Vol. 13*, Nº 88, enero-junio 2017, pp. 72-112. Universidad EAFIT, Medellín.

Ramón, J., Cerezo, A., García, E., Gassó, A., Giménez, A., Gómez, E., Miró Llinares, F., Mueller, K., Varona, G. (2020). Impacto del COVID-19 en distintas formas delictivas. Fundación para la investigación aplicada en la delincuencia de la seguridad. FIADYS.

Real Academia Española. Diccionario de la lengua española.

Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria provocada por la COVID-19. Boletín Oficial del Estado Nº 67, de 14 de marzo de 2020, 25390-25400. Referencia: BOE-A-2020-3692.

Recasens, A. (2007). La seguridad y sus políticas. Atelier.

Rodríguez Mesa, M. J. (2021). La Covid-19. Un campo de experimentación para el enfoque criminológico de la oportunidad delictiva. *Revista de estudios Jurídicos y Criminológicos*, *4*, 15-21, Universidad de Cádiz.

Rovira del Canto, E. Delincuencia informática y fraudes informáticos, Editorial Comares, Granada, España, 2002.

Sain, G. (2018). Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet. *Revista Erreius*. Ed. 1. Buenos Aires, Argentina.

Sánchez Medero, G. (2012). Ciberespacio y el crimen organizado: los nuevos desafíos del siglo XXI. *Revista Enfoques, Vol. X* (16), 71-87.

Schlack Muñoz, A. (2008). El concepto de patrimonio y su contenido en el delito de estafa. *Revista chilena de derecho*, *35*(2), 261-292.

Sistema Estadístico de Criminalidad. Series de datos sobre criminalidad y cibercriminalidad. Secretaría de Estado y Seguridad. Ministerio del Interior. Gobierno de España.

Solari-Merlo, M. N. (2021). Actividades cotidianas en redes sociales Estudio del comportamiento habitual y las medidas protección de los usuarios de Facebook, Instagram y Twitter. *Revista De Derecho Penal Y Criminología*, (25).

Soto Solano, M. (2012). El crimen on-line. Una mirada a la responsabilidad del proveedor de servicio de Internet. *Justicia Juris, 8* (1), pág. 75-83.

Tejero, E. L. (2019). Dificultades jurídicas ante las conductas delictivas contra y a través de medios informáticos y electrónicos. *Revista de Pensamiento Estratégico y Seguridad CISDE*, *4*(2), 39-54.

Tiedemann, K. (2000). Derecho penal económico: introducción y panorama en derecho penal y nuevas formas de criminalidad. *Idemsa, Lima*, 16.

Tribunal Supremo. Sala Segunda de lo Penal. Sentencia de 19 de abril de 1991.

Tribunal Supremo. Sala Segunda de lo Penal. Sentencia nº187, 8 de febrero de 2002.

Tribunal Supremo. Sala Segunda de los Penal. Sentencia nº 2175, 20 de noviembre de 2001.

Tribunal Supremos. Sala Segunda de los Penal. Sentencia nº 465, 1 de junio de 2012.

Vílchez Limay, R.C. La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional. *Ars Iuris Salmanticensis*, *Vol.8*, 21-25, Ediciones Universidad de Salamanca.

We Are Social (2020). Informe global sobre las tendencias tecnologías y el uso que hacen las personas. Agencia Creativa Especializada en Tendencias Tecnológicas y el Uso que hacen las Personas.

Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, *56*(1), 21-48.