**TRABAJO FIN DE GRADO EN DERECHO**

**CURSO 2020/2021**


Biblioteca
UNIVERSITAS Miguel Hernández

# "ESTAFAS EN EL COMERCIO ELECTRÓNICO"

Alumno: Iziar Sánchez Zaragoza

Tutor: Jose Antonio Espinosa Bernal

**INDICE**

## 1. Introducción

El ciberdelito o también lo que es conocido como cibercrimen, es un término genérico, el cual hace referencia a la actividad delictiva de las acciones en Internet o relacionadas, llevada a cabo mediante equipos infórmaticos o a través de Internet. Asimismo, puede hacer uso de diferentes métodos y herramientas, como pueden ser el *phishing* (robar información de alguien), *ciberbullying* (acceso a través de la red), el *grooming* (conocer a menores con fines sexuales), normalmente con el objetivo de robar información personal o de realizar actividades fraudulentas. La característica principal de este tipo de delitos es que para ser perpetrados es necesario acceder a redes de información o medios informáticos.

Los responsables pueden ser personas aisladas, grupos organizados o facciones con patrimonio estatal, suelen ser personas con un alto conocimiento de informática, aunque hoy en día cualquier persona puede acceder a un ordenador y a internet, accediendo a redes sociales o mandar correos a particulares, debido al avance de las nuevas tecnologías y como se han implantado en la sociedad como un elemento común. Los ciberdelincuentes compran y venden *malware* en línea (normalmente en la red oscura) y comercian sus servicios que prueban la robustez de un virus, paneles de inteligencia empresarial que controlan la implementación de *malware* y soporte técnico.

Por otro lado, podemos decir que la ciberdelincuencia está increíblemente organizada y profesionalizada. La profesionalización y proliferación de la ciberdelincuencia supone un coste anual enorme de daños que sufren personas, empresas o incluso gobiernos, se trata de una de las actividades ilegales más lucrativas.

A medida que internet evoluciona y los dispositivos inteligentes ganan popularidad, los ciberdelincuentes disfrutan de una superficie de ataque mucho mayor: más oportunidades para romper las medidas de seguridad, lograr acceso no autorizado y cometer delitos.

Por lo tanto, podemos decir que el ciberdelito es en la actualidad una de las amenazas más preocupantes a la hora de navegar en Internet. Cada vez más usuarios están conectados a Internet a través de equipos portátiles, smartphones y tablets, y es por ello una de las actividades ilegales más rentables. Así, los ciberdelitos son ya el 10% de las infracciones penales conocidas en nuestro país en el año 2020. Los fraudes en Internet se convierten, con 192.375 denuncias, en el segundo delito más común, solo tras los hurtos. También podemos destacar, que durante el confinamiento la policía detectó un incremento de estos delitos de hasta un 70%.

### 1.1. Evolución de las estafas a través de Internet

Los primeros casos de la delincuencia cibernética se cometieron antes de que internet llegara a existir e implicara robo de datos. La evolución e historia del cibercrimen o ciberdelito coinciden con la evolución de internet. Así, los primeros crímenes fueron simples hackeos para robar información de las redes locales, pero a medida que internet se estableció más, también lo hicieron los ataques.

La primera gran ola de delitos cibernéticos llegó con la proliferación del correo electrónico a finales de los años 80, lo cual permitió que una gran cantidad de fraudes y/o *malware* se enviaran a las bandejas de entrada. Un ejemplo a destacar es la estafa del mítico príncipe nigeriano, en el cual desde los albores de la Red, uno de los primeros "*spam*" o correos basura que llegaba era los del Príncipe Nigeriano, ese heredero al trono tan rico como el Príncipe de Zamunda que tenía problemas y nos preguntaba vía mail si podía usar su cuenta para mover sumas millonarias de dinero. Conocido como la

estafa nigeriana, timo nigeriano o timo 419, su nombre viene del número del artículo del código penal de Nigeria que viola, ya que buena parte de estas estafas provienen de ese país. Esta estafa consiste en ilusionar a la víctima con una fortuna inexistente y persuadirla para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna.

La siguiente gran ola en la línea del tiempo de la historia del ciberdelito llegó en los años 90, con el avance de los navegadores web. En ese momento, había una multitud para elegir, mucho más que hoy, y la mayoría eran vulnerables a los virus, los cuales eran enviados a través de conexiones a internet siempre que se visitaban sitios web cuestionables.

Pero ahora bien, el ciberdelito empezó realmente a despegar a principios del año 2000, cuando las redes sociales cobraron vida. La gente ponía toda la información en una base de datos del perfil, ello creó una inundación de información personal y el aumento del robo de identidad. Los delincuentes utilizaban la información de varias maneras, incluyendo el acceso a cuentas bancarias, la creación de tarjetas de crédito y otros fraudes financieros.

El primer caso en el que se comete un delito a través de una red de ordenadores es imposible saberlo, pero si que podemos conocer el primer gran ataque a una red digital y luego usar eso como punto de referencia en la evolución de los delitos cibernéticos. Así, en 1971, John Draper, un manipulador telefónico (término usado para describir a programadores de ordenadores obsesionados con las redes telefónicas). Este manipulador descubre que un silbido dado como premio en casas de Captain Crunch producía los mismos tonos que los ordenadores del conmutador de la época. Él construyó una “casa azul” con el silbido que le permitía hacer llamadas de larga distancia gratuitas y luego publicó instrucciones de como hacerlo. Los casos de fraude telefónico aumentaron significativamente. También podemos destacar que en el año 2007, los casos de hackeo, robo de datos e infecciones de *malware* se disparan. El número de registros robados y máquinas infectadas aumentan en millones.

Este tipo de crímenes son muy prominentes y ellos se debe a que el crimen se esconde justo debajo de la superficie de internet. La razón por la que es capaz de propagarse de la manera en que lo hace se reduce a una serie de factores. En primer lugar, los criminales pueden esconderse fácilmente detrás de sus terminales, lejos de los reguladores, operando con impunidad, utilizando *softwares* de última generación y técnicas de redes para enmascarar sus ubicaciones y evitar cualquier mirada indiscreta. En segundo lugar, internet proporciona un acceso fácil. Y por último, no tienes que ser un programador, sino que basta con saber donde comprar uno.

Ahora bien, en cuanto a la evolución de las estafas a través de internet en nuestro Código Penal, podemos decir que en el Código Penal actual de 1995, el delito de estafa informática queda regulado en el artículo 238.2.a), el cual nos dice lo siguiente: "se consideran reos de estafa 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. No obstante, antes del Código Penal de 1995 la mayoría de los delitos referentes a la informática resultaban atípicos y extraños para los Tribunales.

Por último, cabe destacar que España es el líder mundial en engaños, estafas y fraudes en internet. Esta es una de las conclusiones del Índice de Civismo Digital (ICD) "Civismo, seguridad e interacciones online-2020", elaborado anualmente por Microsoft y que incluye a España por primera vez. En este sentido, España se ha situado en un 44% en cuanto a engaños, estafas y fraudes en internet, lo que lo sitúa 13 puntos por encima de la media mundial. Un 36% asegura haber recibido un contacto no deseado en Internet y un 26% se declara víctima de "sexting" o envío y recepción de mensajes (vídeos, imágenes…) con contenido sexual a través del móvil u otro dispositivo. Por otro lado, en España uno de cada seis encuestados (21%) ha percibido que el civismo en internet empeoró durante el confinamiento en los meses de abril y mayo. Entre las causas, se atribuyen a que internet se ha usado para desahogarse y exteriorizar frustraciones. Otro 26%, creen que ella

civismo mejoró por el sometimiento de comunidad ante uno de los peores momentos de la pandemia[1].

## 2. Tipos de fraudes en el comercio electrónico:

Admitida la denominación de cibercrimen en la actualidad referida a la delincuencia informática, la doctrina ha tratado de sistematizar de muy diversas maneras los numerosos comportamientos ilícitos surgidos en el ciberespacio transnacional, popular y en constante revolución. Así, el fraude en Internet se basa en la utilización maliciosa de tres elementos sobre los que se construye el engaño: ingeniería social, *spam* y *malware.* La presencia de estos elementos varía según el tipo de fraude y son utilizados de manera complementaria. La ingeniería social es la herramienta más utilizada para llevar a cabo estafas, fraudes y timos, convencer a los internautas para que reenvíen un correo a su lista de direcciones y que éste contenga código malicioso es un ejemplo muy habitual en la práctica. Otra de las técnicas consiste en el envío de correo masivo y no deseado, conocido como *spam,* ésta constituye el mejor y más barato mecanismo de difusión. Y por último, el *malware, ya puede ser en forma de virus, gusanos, troyanos o de* keyloggers, entre otros, éstos interceptan los datos que el usuario intercambia con una determinada entidad o las pulsaciones de su teclado. Asimismo, en cuanto a las modalidades de cibercrimen podemos encontrar la siguiente clasificación: cibercrímenes económicos (*malware* intrusivo, *spam*, *phishing*, entre otros), cibercrímenes sociales (*spoofing*, *sexting*) y por último, cibercrímenes políticos (ciberespionaje terrorista, ciberguerra). A continuación veremos algunas de las principales fórmulas de fraude utilizadas en el medio de internet, para con ello, más adelante ver si son susceptibles de castigo penal, según estén tipificadas o no en el Código Penal.

### 2.1. Obtención de los datos o claves de acceso (*spyware* y *phishing*)

[1] Óscar López-Fonseca ( 7 de junio de 2020) Delitos Informáticos. Los ciberdelitos son ya el 10% de las infracciones penales conocidas. El país.

Dentro de este apartado incluimos números y claves de tarjetas de crédito o débito

### 2.1.1. Sustracción de las claves de acceso sin el conocimiento de la víctima (*spyware*).

Mediante esta fórmula se lleva a cabo la sustracción de datos que permiten la suplantación de personalidad de la víctima, así se pueden obtener claves bancarias, claves de acceso a páginas o servicios o datos de tarjetas de crédito para posteriormente poder ser utilizados para conseguir ventajas económicas en favor del autor de la sustracción o de terceros. Esta fórmula implica normalmente el acceso al sistema operativo de la víctima a través de la red, que puede tener lugar a través de diversas vías. En la actualidad, estos datos suelen obtenerse a través de *spyware* o archivos espía, éstos se trata de aplicaciones que se consiguen introducir en el ordenador de la víctima, y el envío a un lugar exterior de datos del sistema donde estén instalados es su objetivo, mediante la utilización subrepticia de la conexión a la red, todo ello sin el conocimiento del usuario. Lo más habitual en la práctica son los troyanos[2] que se descargan en internet y su instalación se lleva a cabo mediante controles ActiveX[3] procedentes de fuentes poco fiables o inseguras. Ahora bien, los más frecuentes son los *keyloggers*[4], pero también encontramos otros más complejos en los cuales acceden a dicha información sin necesidad de que el usuario teclee nada, mediante la apertura de puertos y accediendo a la información cuando el usuario ingresa en un enlace determinado. Por lo

---

[2] En informática, se denomina caballo de Troya, o troyano, a un *malware* que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

[3] Los controles ActiveX son pequeñas aplicaciones que permiten a los sitios web proporcionar contenido, como vídeos y juegos. También te permite interactuar con contenido como barras de herramientas y tableros de cotizaciones mientras navegas por internet.

[4] Un *keylogger* es una clase de software o un dispositivo *hardware* específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet

tanto, a través de estas fórmulas el defraudador se hace con información personal, como claves de acceso o datos bancarios, los cuales se utilizarán más tarde para realizar transferencias a su favor o en favor de terceros[5].

### 2.1.2. Obtención fraudulenta de las claves. *Phishing*.

En este caso, es la propia víctima la que, sin saberlo, hace llegar al defraudador los datos necesarios para realizar las transacciones. Se define por el grupo mundial *antiphishing*[6] como el mecanismo criminal que emplea ingeniería social y subterfugios técnicos para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias.

En la actualidad, un ataque de *phishing* incluye tres componentes clave: el mensaje, la interacción y el robo. En el primero de los componentes, el mensaje, las víctimas reciben un reclamo a través de un medio electrónico, que en la mayoría de las casos se trata de un correo electrónico, remitido por el delincuente, pero a su vez, también puede ser un SMS o VoIP[7]. Poniendo en práctica diferentes estrategias de engaño, se consigue que el usuario siga un enlace a una URL inserta en un correo electrónico, proporcione determinada información sensible respondiendo a un correo o instale un *malware.* Podemos encontrar como ejemplo aquellos mensajes en los que se requieren actualizaciones de seguridad o falsas actualizaciones, entre otros. Asimismo, en otros casos, el mensaje contiene una proposición relacionada con futuras ganancias o beneficios, que busca aprovechar el ánimo de lucro de la víctima.

---

[5] FERNÁNDEZ TERUELO, J.G. *Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red.* Revista de Derecho Penal y Criminología, 2007. Pág. 218 y ss.

[6] La protección *antiphishing* le mantiene a salvo de todo tipo de ataques relacionados con el robo de datos privados tales como contraseñas, datos bancarios, etc.

[7] El término VoIP significa Voz sobre Protocolo de Internet, y se trata de un método con el que se puede hacer llamadas de voz a través de la red. Ahora bien, con la VoIP no se depende de la señal de las antenas o del cable de teléfono, sino que se depende de la cobertura de internet que tengas para poder transmitir las llamadas

El segundo componente que encontramos es la interacción. Una vez recibido el mensaje por el usuario se requiere que la propia víctima acuda a la web que se ha creado de forma idéntica a la de una organización de confianza, como puede ser un banco. Para ello, registran nombres de dominio parecidos a los de la identidad elegida, así como también utilizan logos e imágenes de las empresas u organismos a los que suplantan, generando una falsa seguridad en la víctima.

Por último, encontramos la utilización efectiva de la información robada. El delincuente, en algunos casos, utiliza la directamente los datos de la víctima suplantando su identidad, pero normalmente, el *phisher* no explota por sí mismo la información obtenida, sino que la vende a terceros. Un ejemplo que podemos señalar es las cuentas de usuario para juegos masivos *online* o la venta de números de tarjetas de crédito.

Ahora bien, las diferentes modalidades de *phishing* se encuentran en constante mutación y refinamiento a medida que mejoran las medidas de seguridad y protección de organismos, entidades y usuarios[8]

### 2.2. *Dialers (conexiones fraudulentas telefónicas).*

Los *dialers son programas que se instalan en el ordenador y que, llaman a números de tarificación adicional[9] sin que el usuario lo sepa. Se suelen instalar mediante un fichero ejecutable (.exe) o mediante la descarga de un control ActiveX. En la mayoría delas ocasiones no se informa de que van a instalar un programa en el disco duro y/o hacer modificaciones en el sistema, con lo que confundirán a usuarios con pocos conocimientos en la materia.*

[8] MIRÓ LLINARES, F. *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, pág. 72-79.*

[9] Un número de teléfono de tarificación adicional es todo aquel número de teléfono cuyo coste es superior al de una llamada a un abonado a la red telefónica. El beneficio obtenido de las llamadas se reparte entre la operadora de telefonía y la empresa que es llamada.

*Ahora bien, desde un punto jurídico, estos programas únicamente serán lícitos cuando advierta de modo claro y nítido, de los cambios que van a hacer en el sistema y los costes en que incurre el usuario al utilizarlos*[10]

### 2.3. Fraudes en operaciones de comercio electrónico.

Estos fraudes están sujetos a la entrega de la cosa (por parte del vendedor) o en el pago del precio ( por parte del comprador). Las fórmulas habituales de fraude consisten en el envío o en la entrega de un bien que no reúne las características de las que se presume, o incluso en la falta de envío o entrega del mismo, utilizando como formas de pago el pago anticipado o contra reembolso. En este caso, la mayoría de los supuestos fraudulentos se basan en la ausencia de pago y suplantación de la personalidad del comprador real (desde el punto de vista del adquirente), haciendo soportar los cargos del mismo a una tercera persona que desconoce la operación[11]

### 2.4. Envío de mails fraudulentos.

En estos casos, el correo electrónico es un simple medio de contacto con la víctima para llevar a cabo diversos fraudes[12]. Un ejemplo sería la estafa nigeriana, a la cual hemos hecho mención anteriormente, así como también podemos encontrar premios ganados, en los que primero hay que

---

[10] FERNÁNDEZ TERUELO, J.G. *Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red.* Revista de Derecho Penal y Criminología, 2007. Pág. 222.

[11] Podemos destacar el *phishing car* que es una variación del *phishing, en la que la venta de un coche es el gancho para encañar al comprador, al cual se le pide una señal por dicho coche que nunca se efectuará.*

[12] El Instituto Nacional de Ciberseguridad (Incibe) ha alertado de que se ha detectado una campaña de envíos de correos electrónicos fraudulentos que suplantan la identidad del servicio de Correos pidiendo que el usuario pague 2,99 euros por costes de envío de un paquete. Así, el objetivo es redirigir a la víctima a una página que simula ser la web legítima de Correos, pero que en realidad no lo es (*phishing) y solicitar dicho pago.* Efe León (13/11/2020). El Incibe alerta de una campaña de e-mails fraudulentos que suplantan a correos. La Vanguardia.

desembolsar una determinada cantidad de dinero para posteriormente obtener dicho premio[13].

### 3. Respuesta penal.

La categoría del cibercrimen o cibercriminalidad define un ámbito de riesgo que derivaba de la tecnología informática, común a muchos bienes jurídicos cuya tutela parecía requerir una modificación de los tipos penales existentes, para así poder adaptarse a las nuevas realidades informáticas. Por lo tanto, podríamos decir, que el riesgo de la actividad informática, era y es, lo común a infracciones penales como puede ser el *hacking*[14], el sabotaje o daños informáticos, entre otros; se trata pues, de tipologías de conducta específica que la doctrina penal considera merecedoras de respuesta penal y por ello, se analiza su posible absorción en los tipos penales tradicionales o reforma de los mismos, así como la creación de tipos nuevos[15].

En las últimas décadas, se ha abordado la regulación de Internet, por lo que el Derecho Penal no ha permanecido al margen, ya que todo lo que es ilegal en el mundo real, lo es también en el mundo virtual. Intervenir en Internet no legaliza, así como tampoco exime a ninguna conducta de su encaje en el Ordenamiento jurídico. Ahora bien, hay una cierta problemática a la hora de la dificultad que encontramos al exigir responsabilidades a los autores de dichas conductas. Los delincuentes han encontrado un campo especialmente abandonado para la comisión de delitos, lo que exige una respuesta penal específica a estas conductas.

---

[13] FERNÁNDEZ TERUELO, J.G. *Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red.* Revista de Derecho Penal y Criminología, 2007. Pág. 224.

[14] el *hacking* consiste en la detección de vulnerabilidad de seguridad, y también engloba la explotación de las mismas.

[15] MIRÓ LLINARES, F. *El cibercrimen.* Fenomenología y criminología de la delincuencia en el ciberespacio, pág. 34 y ss.

Por lo tanto, podemos decir, que el el Derecho Penal debe responder ante estas amenazas haciendo uso de sus técnicas e instrumentos , todo ello sin olvidar sus principios estructurales, en especial el principio de ultima ratio.[16]

### 3.1.- Tipo básico de estafa, definición y elementos.

El delito de estafa se encuentra regulado en nuestro Código Penal bajo la rúbrica "Delitos contra el patrimonio y contra el orden socioeconómico". Así, se trata de un delito contra el patrimonio, siendo el patrimonio de la persona, según la mayoría de la doctrina, el bien jurídico protegido.

A continuación, vamos a detallar los elementos esenciales, tanto objetivos como subjetivos, del tipo básico de estafa que se encuentra regulado en el art. 248.1 CP. Los objetivos son aquellos que caracterizan objetivamente el supuesto de hecho de la norma penal y serían los siguientes:

1.- El engaño. Un engaño precedente o concurrente plasmado en algún artificio. Dicho engaño ha de ser bastante para la consecución de los fines propuestos, así como con suficiente entidad para provocar el traspaso patrimonial.

Para ARROYO DE LAS HERAS, el requisito fundamental del delito de estafa es el engaño como elemento objetivo, siendo su elemento más significativo, esencial y definitorio.[17]

---

[16] MOISÉS BARRIO, A. (Letrado del Consejo de Estado. Profesor de Derecho Público, ICADE, Madrid. Abogado). *La ciberdelincuencia en el Derecho Español.* Revista Cortes Generales, pág. 276 y ss.

[17] ARROYO DE LAS HERAS, A. *Los delitos de estafa y falsedad documental, 2005, pág. 22.*

2.- Producción de un error esencial en el sujeto pasivo (víctima), desconocedor de lo que constituía la realidad. Por lo tanto, el error puede consistir tanto en un desconocimiento de la realidad como en un conocimiento deformado de la misma por parte de la víctima como bien acabamos de decir, siempre y cuando dicho error sea consecuencia del engaño perpetrado por el sujeto activo, lo que lleva a la víctima a realizar un acto de disposición patrimonial.[18]

3.- Acto de disposición patrimonial, con el siguiente perjuicio para el sujeto pasivo (víctima). Dicho acto es una consecuencia directa del estado de error en el que se encuentra la víctima del delito, dicho error se ha producido por un engaño del sujeto activo, el cual ha conseguido el fin propuesto, el acto de disposición patrimonial.

El acto de disposición patrimonial puede radicar tanto en llevar a cabo una acción (entregar una cantidad de dinero), como en no hacer una cosa (la renuncia de la Hacienda al percibo de un tributo que le era debido, producida por entender erróneamente que le había sido satisfecho). Así, la STS 436/2019, de 12 de Diciembre, establece que"…acto de disposición patrimonial, con el consiguiente y correlativo perjuicio para el disponente, es decir, que la lesión del bien jurídico tuteado, el daño patrimonial, será producto de una actuación directa del propio afectado, consecuencia del error experimentado y, en definitiva, del engaño desencadenante de los diversos estadios del tipo"[19]

También encontramos en el art. 248 CP que el tipo de estafa no requiere que quien realiza el acto de disposición patrimonial y el perjudicado sean la misma persona. Ahora bien, la doctrina ha resaltado que no es preciso que el disponente tenga facultad jurídica para realizar el acto de disposición, como no la tiene el sirviente que entrega una cosa a quien finge ser recadero de su propietario. Pero, por su parte, CHOCLÁN MONTALVO estima necesario que el

[18] ARROYO DE LAS HERAS, A. *Los delitos de estafa y falsedad documental, 2005, pág. 30.*

[19] Sentencia Penal Nº 436/2019, Audiencia Provincial de Tenerife, Sección 5, Rec 64/2019 de 12 de Diciembre de 2019.

disponente sí que tenga disposición jurídica sobre el elemento patrimonial.[20] Además, el acto de disposición, calificable de estafa, existe pese a la ilicitud de la posesión originaria de la cosa, por lo tanto, no es ilógico castigar al ladrón por su robo y al que de ellos obtiene con el engaño la entrega de tales objetos, por estafa.

4.- Perjuicio. Perjuicio que ha de aparecer vinculado causalmente a la acción engañosa (nexo causal o naturalístico). Y materializarse en el mismo el riesgo ilícito que para el patrimonio de la víctima supone la acción engañosa del sujeto activo (relación de riesgo o segundo juicio de imputación objetiva). Por lo tanto, el perjuicio es la consecuencia final del estado de engaño en el que se encuentra ese sujeto pasivo, por el cual realiza un acto de disposición patrimonial y como consecuencia, sufre el perjuicio patrimonial.

Por otro lado, vamos a ver los elementos subjetivos del tipo básico del delito de estafa:

1.- Ánimo de lucro.

El ánimo de lucro, consiste en la intención de obtener un enriquecimiento de índole patrimonial, dentro del mismo, encontramos también la evitación de un gasto. El art. 248 CP lo considera un elemento esencial para poder calificar la acción del delito de estafa. Así, encontramos en la STS 1232/2002, de 2 de julio, como elemento subjetivo del injusto o dolo en el sujeto activo de la acción, según la jurisprudencia y lo doctrina aparece integrado por el elemento intelectivo de conocer que se esta engañando y perjudicando a otro y el volitivo de obtener una ventaja o provecho[21]. Este elemento subjetivo del dolo ha de inferirse de los hechos realizados y de los beneficios obtenidos como resultado de la acción.

---

[20] CHOCLÁN MONTALVO, J.A. *El delito de estafa, pág. 189 y ss.*

[21] Sentencia Penal Nº1232/2002, Tribunal Supremo, Sala Segunda de lo Penal de 2 de Julio de 2003.

2.-Dolo.

El dolo se trata de la voluntad deliberada de cometer un delito, a sabiendas de su carácter delictivo y del daño que puede causar. El dolo del autor del delito de estafa está encaminado al enriquecimiento injusto, es decir, al propósito de enriquecerse él mismo o a una tercera persona como consecuencia del engaño a la víctima que le ha llevado a realizar el acto de disposición patrimonial. Por lo tanto, podemos decir que basta el ánimo de engañar (*animus decipendi),* sin necesidad del ánimo de dañar (*animus nocendi).*

*Consecuentemente, encontramos el dolo subsequens, en el que la STS 2609/2019, de 24 de julio, nos dice: "…*cuando el autor simula un propósito serio de contratar cuando, en realidad, solo pretende aprovecharse del cumplimiento de las prestaciones a que se obliga la otra parte, ocultando a ésta su decidida intención de incumplir sus propias obligaciones contractuales, aprovechándose el infractor de la confianza y la buena fe del perjudicado con claro y terminante ánimo inicial de incumplir lo convenido, por lo tanto, encontramos un ilícito afán de lucro propio, despegando así unas actuaciones que desde que se conciben y planifican prescinden de toda idea de cumplimiento de las contraprestaciones asumidas en el seno del negocio jurídico bilateral, lo que da lugar a la antijuricidad de la acción y a la lesión del bien jurídico protegido por el tipo"[22]

### 3.2. Elementos del fraude informático.

Después de analizar los elementos del tipo básico del delito de estafa, vamos a señalar los elementos del fraude informático. En ocasiones, nos podemos encontrar con determinados supuestos en los cuales no está claro que existan todos los elementos, como pueden ser los casos típicos de *spyware así* como también los de *phishing, ya que en ambos no se da típica*

[22] Sentencia Penal Nº2609/2019, Tribunal Supremo, Sala de lo Penal, Madrid de 24 de julio de 2019.

*relación de engaño* y es aquí cuando debemos remitirnos a la figura de la estafa económica.

A todo esto, hay que añadir, que las normas penales actuales han incluido nuevos tipos de fraudes o estafas informáticas, los cuales se realizan a través de programas que tiene por fin medios delictivos, así como la manipulación informática de datos para cometer determinados delitos. Así, el fraude tradicionalmente conocido como estafa, se ha multiplicado exponencialmente con muchas formas de cometerlo, no coincidiendo en ocasiones con el concepto tradicional de estafa y yendo mas allá del mismo. Es por ello, que debido a la insuficiencia de la estafa común para resolver algunos supuestos en los que el engaño y error definitorios de este delito están ausentes, el legislador de 1995 creó la llamada estafa informática, que es un nuevo modelo de la estafa común y se encuentra regulada en el artículo 248.2 del Código Penal. La previsión de esta nueva modalidad tiene su razón de ser en la insuficiencia del modelo clásico de estafa para hacer frente los supuestos de manipulaciones informáticas, en los que no se encuentran presentes ni el engaño ni el error, que como bien es sabido, son elementos esenciales de la estafa común.

Es decir, podemos utilizar la figura de la estafa económica en aquellos supuestos que no estén comprendidos en el tipo penal de estafa. A continuación, vamos a analizar los cuatro elementos que integran un frute informático:

1.- Manipulación informática. Ésta se trata de la alteración, introducción, borrado o supresión indebida de datos informáticos, especialmente datos de identidad, y la interferencia ilegítima en el funcionamiento de un programa o sistemas informáticos, cuyo resultado sea la transferencia no consentida de un activo patrimonial en perjuicio de tercero. Por tanto, podemos incluir en dicho término la introducción de datos falsos, así como la manipulación de los mismos, la introducción indebida de datos reales, y también las interferencias que puedan afectar al propio sistema.

2.- La transferencia de un activo patrimonial. La transferencia de un activo patrimonial consiste en el traspaso fáctico de un activo[23]. Así, cuando el afectado ha caído en el error se produce un acto de disposición patrimonial en beneficio del sujeto activo y en perjuicio de la víctima. Pero algo muy importante que debemos resaltar y que lo distingue del delito de estafa que hemos visto anteriormente es que es la propia víctima quien lo realiza. De no ser así, podríamos encontrarnos ante supuestos de administración desleal.

3.- Ánimo de lucro. Como bien hemos dicho anteriormente el ánimo de lucro es el elemento subjetivo el injusto que consiste en el propósito o intención del delincuente de conseguir un beneficio o ventaja económica.

4.- Por último, el actor del fraude informático deberá actuar en perjuicio de tercero o sujeto objeto del engaño, el cual sufre un daño en su activo patrimonial, dando así lugar por lo tanto a la consumación del delito.

Biblioteca UNIVERSITAS Miguel Hernández

## 4. Problemas derivados de la ausencia de medidas preventivas y nuevas soluciones técnicas.

A medida que los avances tecnológicos y la utilización de los mismos ha ido avanzando, también ha ido aumentando la cantidad de información que se ha puesto a disposición de la sociedad mundial, en las diferentes áreas del conocimiento, permitiendo procesar esa información que llega a los gobiernos, instituciones y a las personas. Así, el empleo de estos medios tecnológicos han facilitado, por así decirlo, que los sujetos dedicados a cometer ilícitos en contra el patrimonio puedan acceder a distintas maneras de vulneración de la información, como por ejemplo podemos destacar la clonación de tarjetas

[23] El traspaso fáctico de un activo se trata de una operación de transferencia de un elemento patrimonial valorable económicamente que pasa del patrimonio originario a otro, no teniendo necesariamente que producirse por medios electrónicos o telemáticos.

bancarias, a través de la manipulación de los programas pertinentes. Por lo tanto, podemos decir, que las legislaciones deben adecuarse a los avances tecnológicos informáticos, replanteándose la manera en la que se persiguen y se juzgan este tipo de delitos.

Como bien sabemos, la estafa es uno de los delitos más clásicos cometidos contra el patrimonio, siendo su principal componente un elemento intencional, ánimo de lucro de una conducta que se compone de tres elementos, engaño, error y disposición patrimonial, mencionados anteriormente. Por ello, se sanciona a la persona que provoca una disposición patrimonial ajena a través de un engaño, el cual tiene que ser suficiente y así generar el error, que es lo que lleva al acto de disposición.

A lo largo del tiempo, han ido surgiendo nuevas modalidades de comisión de los tradicionales delitos, siendo hoy en día más compleja su persecución, ya que las legislaciones en ocasiones no tienen las herramientas necesarias para hacer frente a esta formas actuales de llevar a cabo dicho delitos mediante los sistemas o redes informáticas e incluso, pudiendo llegar a quedar impunes.

El fraude informático es una de las tipologías del cibercrimen, en el cual se da la defraudación por medios informáticos, es decir, la utilización del sistema informático como medio para transferir patrimonio a favor del sujeto activo. Pero, muchas veces, las legislaciones se muestran lentas ante los cambios, y más en concreto, los que van sucediendo en esta nueva era informática, así como también, dichas legislaciones se han visto obligadas a tener que crear o adecuar sus sistemas a la realidad mundial, y por ello, el Derecho Penal no se puede quedar al margen y debe adecuarse a los tiempos. En este sentido, podemos decir que el delito de estafa informática tiene como fin una norma de control social tendiente a establecer y garantizar reglas básicas de convivencia, en el campo de las relaciones sociales patrimoniales que se desarrolla mediante la utilización de sistemas informáticos. Así, GALAN MUÑOZ, ALFONSO, nos da una visión del derecho penal, que podríamos

denominar funcionalista, y nos dice que las normas penales serían meros instrumentos destinados a establecer los parámetros por lo que debe discurrir la vida social, creyendo sus penas, por principal función la de restablecer su propia vigencia como normas sociales, cuando se hubiese visto autorizada por las conductas efectuadas por alguno de sus destinatarios[24]

### 4.1. Medidas preventivas frente a los fraudes en operaciones de comercio electrónico (garantías jurídicas).

Hoy en día, el método de pago más seguro para comprar por internet es la tarjeta de crédito, por ello, vamos a hacer mención al artículo 46 de la Ley de Ordenación del Comercio minorista (LOCM, ley 7/1996, de 15 de enero, modificada por la Ley 47/2002, de 19 de diciembre), el cual nos habla del pago mediante tarjeta y prevé expresamente que cuando el importe de una compra hubiese sido cargada fraudulenta o indebidamente utilizando el número de una tarjeta de pago, su titular podrá exigir la inmediata anulación de cargo. Por lo tanto, el fundamento de dicho artículo es la protección del titular de la tarjeta cuya cuenta se haya hecho indebidamente el cargo del precio de una compraventa a distancia, bien debido a un error o al uso fraudulento de la tarjeta por un tercero.

Por otro lado, también vamos a hacer mención al artículo 44 LOCM, que concede un derecho de desistimiento[25] al consumidor, concediéndole al comprador un plazo mínimo de siete días hábiles para poner fin a la relación contractual de forma unilateral sin penalización alguna.

Otro caso que se da muy a menudo en la práctica, es la pérdida o sustracción de la tarjeta. Cuando esto ocurre y se utiliza la tarjeta

---

[24] GALÁN MUÑOZ, A. *El fraude y la estafa mediante sistemas informáticos, análisis del artículo 248.2 del Código Penal Español, 2005, pág. 183.*

[25] El derecho de desistimiento de un contrato, servicio o compra consiste en que el consumidor puede dejarlos sin efecto, notificándoselo así al empresario en el plazo establecido, sin necesidad de justificar su decisión y sin penalización de ninguna clase para el consumidor.

fraudulentamente para realizar transacciones en internet, con carácter general, va a ser el banco quien deba de resarcir al titular de la tarjeta de los gastos ocasionados por ese uso fraudulento por parte de terceros. Pero ahora bien, la pérdida o la sustracción de la tarjeta de crédito y su apropiación por un tercero que hace uso de la misma provocando un daño que debe ser asumido por uno de los sujetos sistemáticos se encuentra prevista en las cláusulas de los contratos que componen el sistema de tarjeta de crédito. Se trata de una situación factible en el empleo normal de dicho documento de pago y por ello está específicamente prevista en los referidos negocios jurídicos que establecen obligaciones a cargo de cada uno de los sujetos del sistema con la finalidad de prevenir el uso de la tarjeta de crédito por quien se ha apropiado ilegítimamente de la misma. De acuerdo a dichas previsiones contractuales, el titular de la tarjeta debe custodiar en forma diligente su tarjeta y en el caso de extravío o sustracción, deberá comunicar en forma inmediata a la entidad emisora del hecho; el establecimiento adherido debe verificar la regularidad del pago que se realiza por medio de la tarjeta de crédito; la entidad emisora debe bloquear el posible uso de la tarjeta y comprobar la regularidad de la nota de cargo; el titular debe controlar el extracto de pagos enviados por el emisor. Por lo tanto, como regla general, la transmisión del riesgo por el uso no autorizado de una tarjeta de crédito se produce al comunicar el titular a la entidad emisora de dicha situación de riesgo para la tarjeta y así, su voluntad de bloquear la operatividad de la misma. Una vez comunicado, el usuario no responderá por los cargos derivados por la utilización de la tarjeta denunciada. Si las operaciones se producen una vez denunciada la situación, el titular no esta obligado a reembolsar la cantidad a la entidad emisora ya que es ésta quien debe asumir las consecuencias de la falta de diligencia por no haber operado el bloqueo que impida el uso indebido. Ahora bien, el problema viene cuando el uso indebido sobre dicha tarjeta se produce antes de la comunicación del titular de la misma sobre esa situación a la entidad emisora, ya que por lo general, respondería el titular de la misma[26]

[26] Gete-Alonso y Calera, Mª del C. *Las tarjetas de Crédito, pág. 115.*

Así, encontramos ciertas claves para reducir el fraude en el comercio electrónico, entre las que podemos destacar:

1.- La clave está en los datos. Para abordar el problema a la hora de distinguir una transacción correcta de una fraudulenta, es fundamental identificar todos los datos de los consumidores y compartirlos con las herramientas de prevención de fraude.

2.- Automatizar al máximo las decisiones. La automatización puede llevar a disminuir la deuda mala y acortar el plazo medio en el que se cobran las facturas y los días de retraso que se producen sobre los plazos pactados inicialmente, reduciendo la exposición a cuentas de alto-riesgo porque cualquier señal de riesgo se detecta por adelantado.

3.- Monitorizar la tasa de transacciones denegadas. El propósito es alcanzar el equilibrio entre la prevención del fraude y no espantar a los clientes auténticos con todas las medidas de seguridad.

4.- Análisis por países y métodos de pago. Identificar los métodos de pago en cada país, como también las preferencias de pago es esencial, ya que los comportamientos varían de un país a otro.

5.- Listas de transacciones positivas y negativas. La elaboración de listas, tanto de transacciones válidas como denegadas, puede resultar útil para detectar de manera rápida y efectiva los intentos de fraude o compra legítima.

6.- Implementación del estándar 3-D Secure 2.0. Se ha implantado para los comercios dos medidas de identificación para cada transacción, con la entrada en vigor de PSD2[27]. Por lo tanto, la integración del estándar 3-D *Secure 2.0* lo que permite es la flexibilizaron de este aspecto a través del

[27] PSD2 (*Payment Services Directive)* es la Directiva Europea que regula los servicios de pago (por ejemplo, transferencias, domiciliaciones, pagos con tarjetas, entre otras). Permite además que terceras empresas (*Third Party Providers* o TPP), también intervengan en los pagos. Esto es lo que se conoce como *open banking.*

intercambio de datos contextuales entre el banco y el comercio, evitando la necesidad de que cada comprador se autentifique activamente cada vez que compra con una contraseña.

7.- Utilizar las últimas tecnologías . Como por ejemplo: redes neuronales[28], mapas de comportamiento[29] y autentificación biométrica[30], entre otros.

8.- Estrategia antifraude a medida. Una vez definidas las necesidades y capacidad del negocio para hacer frente al fraude, ha de buscarse la solución antifraude más adecuada[31]

Es fundamental garantizar la seguridad del consumidor online mediante una correcta utilización de los datos ya que el fraude puede llegar a suponer hasta un 3% de la facturación de un ecommerce.

### 4.2. Medidas preventivas generales. De la actividad cotidiana a la prevención (situacional) del cibercrimen.

Desde el punto de vista del usuario, la adquisición de una cultura de seguridad en internet es imprescindible, del mismo modo que se sigue en otros ámbitos de la vida cotidiana, ya que uno de los motivos de que sea internet donde se llevan a cabo más fraudes es la vulnerabilidad que muestran muchos equipos de usuario, que carecen de las medidas de protección adecuadas. Por ello, es importante que se lleven a cabo las mismas medidas

---

[28] Una red neuronal es un modelo simplificado que emula el modo en que el cerebro humano procesa la información. Funciona simultaeando un número elevado de unidades de procesamiento interconectadas que parecen versiones abstractas de neuronas.

[29] El mapa de comportamiento pretende precisamente clasificar a las personas en cuatro cuadrantes de cómo pensamos y de cómo actuamos.

[30] La autentificaron biométrica es simplemente el proceso de verificar la identidad de un sujeto utilizando las características únicas de su cuerpo, y luego iniciar sesión en un servicio, una aplicación, un dispositivo, etc.

[31] Seguridad. Claves para reducir el fraude en el comercio electrónico, 15 Marzo 2019.

de precaución y desconfianza que se adoptan en la vida diaria en cuanto a adoptar claves, contraseñas o datos que puedan ser utilizados en el acceso a información personal, o realizarse actividades fraudulentas mediante los mismos.

Ahora bien, también vamos a mencionar la importancia de la víctima en el evento del cibercrimen. Es la propia víctima la que tiene esa gran capacidad para dejar fuera del ámbito de riesgo aquello que no quiere que se vea afectado por el mismo, es decir, va a determinar esos márgenes genéricos del ámbito de riesgo al que va a estar sometida al incorporar determinados bienes y esferas de su personalidad al ciberespacio, con esto queremos decir, que los bienes de la víctima o su patrimonio no se verán afectados si la misma no entra al ciberespacio. Asimismo, la víctima es casi la única que puede incorporar guardianes para su autoprotección, como puede ser un *software* adecuado frente a virus[32].

La conducta de la víctima determina el riesgo criminal al que estará sometida y lo hará directamente desde el momento en el que entra al ciberespacio, en ese espacio de riesgo nuevo, así como también ese tipo de actividades que va a realizar en Internet, si bien pueden ser sociales, personales o económicas, y por último, esos lugares que visita, los documentos que descarga y sobre todo, los medios tecnológicos que va a incorporar a su sistema informático como auto-guardianes para proteger sus datos[33]

Por lo tanto, lo que se pretende es mejorar su protección en términos de prevención situacional, aumentando el esfuerzo necesario para la realización del delito.

Especialmente nos vamos a centrar en las actividades sociales y económicas. En ambas vamos a presenciar una conducta de quien recibe el

[32] MIRÓ LLINARES, F. *El cibercrimen,* op.cit. pág.191.

[33] MIRÓ LLINARES, F. *El cibercrimen,* op.cit. pig. 192-194

ataque, es decir, de la víctima, ya que sin ella el ataque no se hubiere producido. Por un lado, dicha conducta puede ser activa, como el envío de datos personales a un desconocido o la utilización de un método de pago no seguro en Internet. Pero, por otro lado, también puede ser pasiva, como carecer de esos medios de protección de los que tanto hablamos. Reconocemos por consiguiente la excepcional importancia de la conducta de la víctima en relación con la cibercriminalidad[34]

Lógicamente, además de la víctima encontramos otros elementos relevantes en cuanto a la prevención del cibercrimen. En este caso, nos referimos a la posibilidad de incorporar sistemas de protección ajenos a la víctima que velen por la seguridad en el ciberespacio. Existen prácticas de vigilancia de la criminalidad en el ciberespacio, con la transmisión de contenidos ilícitos, a nivel institucional-estatal como por parte de las ONG, que pretenden denunciar las conductas que cometen los cibercrímenes[35]

Por último, vamos a mencionar algunas medidas específicas en cuanto a la protección del *phishing,* entre las que encontramos una correcta información, conociendo que las entidades financieras o asimiladas nunca piden las claves de acceso por correo. También la protección específica frente al *spyware,* ya que este suele actuar escondido y en un segundo plano. En general, el usuario percibe la esencia de este tipo de programas cuando el escáner del antivirus o el cortafuegos disparan la alarma. Si esto no sucediera, porque el escáner antivirus no esta actualizado o incluso instalado, la infección se hace notar cuando el ordenador trabaja de una forma inusualmente lenta.

### 4.3. Nuevas medidas o soluciones tecnológicas.

Los efectos de las nuevas tecnologías han hecho que la sociedad y la realidad se transformen y con ella la concepción que hasta ahora teníamos. Ocasionalmente, las TICs se consideraban como un nuevo medio para la

[34] MIRÓ LLINARES, F. *El cibercrimen, op.cit. pág. 195*

[35] MIRÓ LLINARES, F. *El cibercrimen, op.cit. pág.197.y ss.*

comisión de delitos clásicos, así como otras veces, han surgido con esta nueva realidad nuevas figuras delictivas, hasta ahora desconocidas para la sociedad. Por lo tanto, esta nueva realidad ha dado lugar a toda una gran categoría de nuevos delitos, conocidos como delitos informáticos, que tienen en común las nuevas tecnologías. Podemos destacar la vacuna contra el COVID-19 como cebo, la consolidación del teletrabajo y el comportamiento de los usuarios como alguno de esos nuevos delitos informáticos que marcarán el cibercrimen durante el 2021 y que trataremos más profundamente en el siguiente punto.

Ahora bien, el cifrado es el elemento esencial para la seguridad de datos y es la mejor forma de impedir que roben la información de un sistema informático con fines fraudulentos, se utiliza en Internet para asegurar la inviolabilidad de la información personal enviada entre navegadores y servidores, dicha información puede tratarse desde datos de pago hasta información personal. Vamos a destacar el certificado SSL (*Secure Sockets Layer),* la tecnología estándar para mantener segura una conexión a Internet, es decir, para garantizar esa seguridad entre dos sistemas y evitar que se lean o modifiquen de forma maliciosa cualquier dato que se transfiera. Lo que nos va a garantizar es que esos datos que se transfieren entre usuarios y sitios web o entre dos sistemas sean imposibles de leer, utilizando algoritmos de cifrado[36]. Por otro lado, el protocolo TLS (*Transport Layer Security)* es solo una versión actualizada, así como más segura de SSL.

Por lo tanto, tenemos que tener en cuenta que nos encontramos ante un medio en constante evolución, y por ello, debemos recurrir a una investigación permanente en materia de control y seguridad, adoptando estas nuevas medidas o soluciones tecnológicas.

[36] En criptografía, el cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave para transformar un mensaje, sin atender a su estructura lingúistuca o significado, de tal manera que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta.

## 5. Perfiles de delincuentes en el ciberespacio.

En el espacio físico nos podemos encontrar con múltiples perfiles de criminal, del mismo modo en el ciberespacio no podemos hacer referencia a una caracterización general del cibercriminal, refiriéndonos a éste como cualquier sujeto que delinque utilizando el ciberespacio como parte esencial del delito. El cibercriminal puede abarcar todos los estratos de edad y todas las clases sociales como veremos a continuación.

Ahora bien, debido a los escasos enjuiciamientos de los ciberdelitos no es sencillo llevar a cabo estudios que nos permitan analizar los caracteres generales de las personas que perpetran esos cibercrímenes.

En primer lugar, vamos a hablar de los *hackers.* La idea de *hacker* ha ido evolucionando con el tiempo, por lo tanto, no encontramos una única figura de *hacker.* Lo podemos definir como aquella persona con conocimientos informáticos que realiza alguna actividad ilícita, o no autorizada, en el ciberespacio. Asimismo, frente al concepto genérico de *hacker,* podemos utilizar otro concepto más estricto, denominado samurai informático, que se entiende por aquel experto en informática, apasionado de Internet y de las nuevas tecnologías. Para este último, el acceso a un sistema informático no es un medio para lograr algo sino un reto tecnológico que mejora el propio sistema.

Por otro lado, nos referimos al término *cracker,* entendiéndose como aquella persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos. Dicho término se empezó a usar por los mismos *hackers* para diferenciarlos de aquellos que superaban las barreras de acceso por el mero hecho de hacerlo. En muchos casos, los *crackers* no son más que meros *hackers* sin salidas profesionales o económicas a su actividad y la consiguen a través de esa ilegalidad.

Por último, encontramos los *scriptkiddies.* Éstos buscan aprovecharse de la vulnerabilidad ajena y dañar. Normalmente se trata de jóvenes, que no tienen más que conocimientos básicos, valiéndose de programas y aplicaciones sencillas para perpetrar dichos daños.

Ahora bien, atendiendo a las especialidades del perfil del cibercriminal derivadas de la modalidad de cibercrimen realizado podemos distinguir entre: el cibercriminal económido, los *ciberhacktivistas,* ciberterroristas y cibercriminales políticos y el cibercriminal social.

La mayoría de los crímenes que se llevan a cabo en el ciberespacio se realizan con intención económica. Los *hackers* económicos son aquellos que desarrollan virus y modalidades de *malware,* naturalmente como forma de impulsar vulnerabilidad en los sistemas informáticos o de crear *backdoors*[37] para acceder a redes o sistemas. Actualmente, son las bandas organizadas las que más ejecutan este tipo de delitos. También encontramos dentro de esta categoría el *insider* que pertenece o trabaja para la empresa víctima del delito, así según el autor Zunzunegui "El *insider trading* es la negociación en el mercado de valores haciendo un uso indebido de información privilegiada. Los iniciados son jugadores de ventaja que negocian sin asumir el riesgo de mercado. Llamamos iniciados a los que poseen la información privilegiada, habitualmente los administradores de las sociedades cotizadas y quienes les prestan servicios de inversión o de asesoría". Casi todas las infracciones informáticas de datos de la empresa se llevan a cabo por los mismos trabajadores de las empresas víctimas.

Por lo tanto, podemos afirmar que el cibercrimen se ha convertido en un crimen cometido por el crimen organizado a nivel transnacional, siendo el ciberespacio el terreno de actuación más valioso para las bandas organizadas.

[37] En informática un *backdoor* se trata de un tipo de virus diseñado para dar acceso a usuarios maliciosos al control de un equipo afectado de manera remota.

Asimismo, también podemos hablar de aquellos delitos en Internet que se llevan a cabo con un objetivo político o ideológico. En los últimos años, los Estados han ido criminalizando las conductas que los *hacktivistas* realizan, como por ejemplo, la difusión de mensajes de libertad, que a priori no supone ningún tipo de conducta delictiva. Así, las conducta que se consideren como graves, cualesquiera que sea su objetivo o propósito, resultará delictiva a partir de la reforma de 2010.

Además, podemos añadir, que tanto el *ciberhacktivismo* como el ciberterrorismo acostumbran a organizarse en grupos más o menos organizados. Como ejemplo del ciberterrismo destacamos el terrorismo yihadista, muy presente en los últimos años. Éstos a través del ciberespacio difieren mensajes de odio y de incitación a la violencia, pretendiendo siempre crear una sensación de terror con la que chantajear a la opinión y voluntad de los gobiernos y sociedades hostiles a sus doctrinas.

Volviendo al *ciberhacktivismo,* uno de los grupos que más relevancia mediática ha obtenido ha sido Anonymous, instruido por *hackers* que se manifiestan en acciones de protesta a favor de la libertad de expresión, del acceso a la información, de la independencia de Internet y en contra de diversas organizaciones. Así, estos revelan información confidencial de gobiernos y algunas empresas privadas que afectan a la sociedad en general tras haber hackeado previamente sus páginas web. Este grupo internacional de *hackers* anónimos nació como diversión en el año 2003 pero cuando verdaderamente su nombre se dio a conocer en todo el mundo fue cuando se destapó el escándalo de *Wikileaks*[38]*.* El propósito de que la verdad quería ser libre atrajo la atención de Anonymous para apoyar dicha causa.

Por último, vamos a hablar del cibercrimen social. Esta categoría es la que presenta una tipología más variada que puede abarcar desde aquellos que actúan con un propósito sexual, hasta aquel que expone su agresividad en el

[38] *Wikileaks* es una organización mediática internacional sin ánimo de lucro que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público.

ciberespacio o que acosa a otra persona. En este caso, podemos encontrar tantos potenciales perfiles de autores como modalidades delictivas. A continuación vamos a ver los ciberdelitos sociales mas destacados:

- El *cybergrooming.* El *grooming* es un fenómeno de engaño en el que un adulto se pone en contacto a través de la red con un menor de edad, haciéndose pasar normalmente por un adolescente con el objetivo de abusar sexualmente de él o ella. Ahora bien, con el tiempo ha ido evolucionando ese perfil del sujeto que lo hace, pudiendo encontrar una modalidad más variada en sus autores. Así, estudios psicológicos y criminológicos concluyen que desde una perspectiva preventiva-especial es más peligroso el abusador sexual clásico o tradicional que el perfil del agresor en el ciberespacio, además este último tiene una menor impulsividad y mayor autocontrol que el primero.

- El *stalking.* El *cyberstalker* se trata del uso de Internet u otros medios electrónicos para perseguir o acosar a un individuo, grupo u organización. Puede incluir falsas acusaciones, difamación, calumnias y difamación. Estas conductas suelen tratarse de envíos de correos electrónicos que puedan obtener imágenes obscenas o amenazas, hacerse pasar por la víctima en redes sociales, etc.

La reforma de nuestro Código Penal por Ley Orgánica 1/2015 de 30 de marzo incluye los nuevos delitos de *Stalking y Sexting,* tratándose de un reflejo de la adaptación del Código Penal a las nuevas circunstancias sociales. En el art. 172 ter CP se regula el *stalking,* acoso, acecho o hostigamiento. Debe destacarse la relevancia de las nuevas formas de *stalking* a que ha dado lugar la llegada de Internet, o ciberacoso, esto es, el envío de correos electrónicos constantes y repetitivos, mensajes en redes sociales de carácter amenazante, entradas en páginas web personales o profesionales para difamar o atentar contra la dignidad de su titular, o interceptación del correo electrónico. En estos casos, se trata de conductas que en la gran mayoría de veces se van a quedar amparadas por el anonimato o la suplantación de personalidad, complicando la identificación del verdadero autor.

- El cyberbully. Este término se utiliza para describir cuando un niño o adolescente es amenazado, acosado, molestado, humillado por otro niño o adolescente a través de Internet o cualquier medio de comunicación como teléfonos móviles o tablets. En relación al sexo de los ciberagresores , un gran porcentaje de estudios indican que los chicos están más involucrados en este tipo de delitos. Pero por otro lado, las chicas también emplean este tipo de acoso inderectamente, especialmente a través de los rumores y hablar mal, lo que lo diferencia de los varones que usan mas la fuerza física y las amenazas.

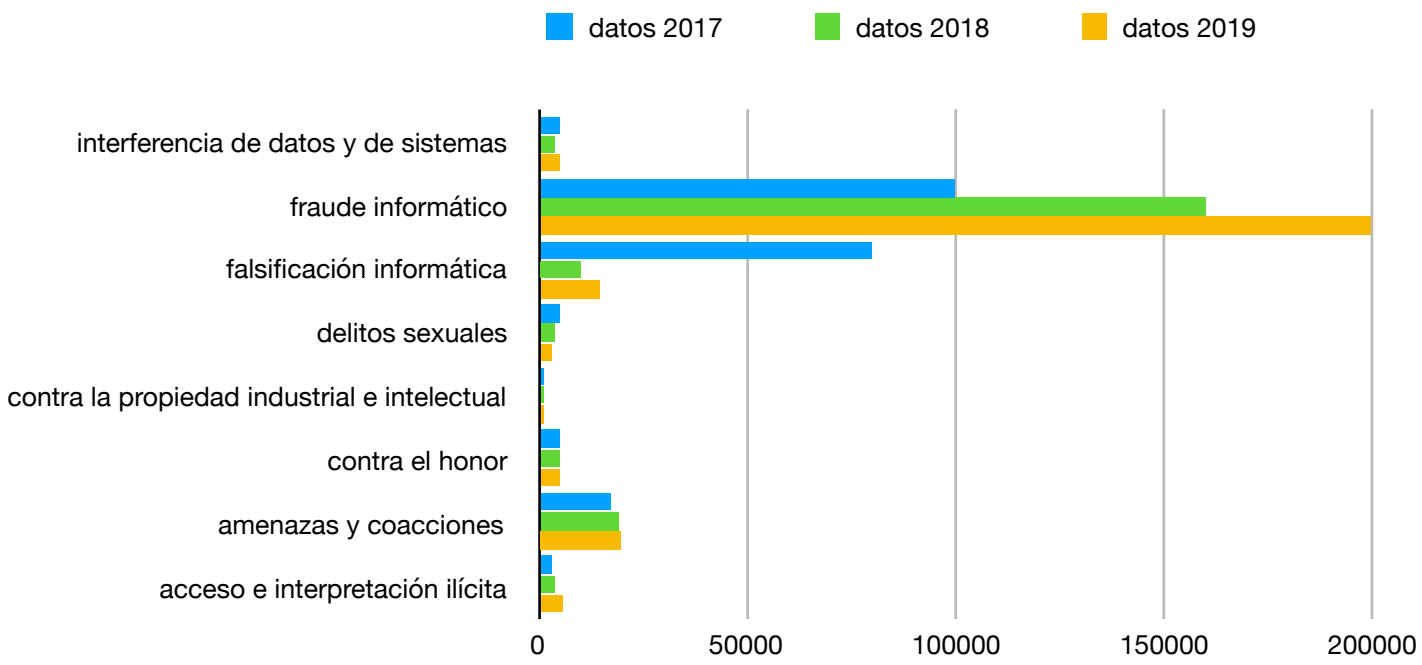
Como hemos visto, encontramos una pluralidad de sujetos involucrados en este tipo de delitos, así como también una gran variedad de modalidades de los mismos[39].

**6. Cibercrimen y COVID-19.**

Durante esta crisis mundial que estamos viviendo, más en concreto, en los meses que hemos pasado en confinamiento por el COVID-19, hemos podido observar que la criminalidad, en términos generales, ha descendido bruscamente, mientras que la ciberdelincuencia ha llegado a máximos históricos, así lo han confirmado considerables medios de comunicación.

Tomando como origen datos del Ministerio de Interior durante los últimos tres años (2017-2019) , según su estudio de cibercriminalidad, podemos afirmar que la Cibercriminalidad ha incrementado exponencialmente en los últimos tres años. Para conseguir una representación visual de dichos datos, vamos a proyectar una gráfica de barras que nos proporciona la diferencia entre delitos.

[39]MIRÓ LLINARES, F. , *Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situaciones de ciberdelitos.* Pág. 230-262.




Como podemos ver en dicha gráfica, el fraude informático se dispara, alcanzando cifras muy elevadas, llegando en 2019 a alcanzar los doscientos mil delitos, mientras que en los demás casos, se mantienen más o menos en las mismas cifras.

Esta nueva situación en la que nos encontramos nos ha llevado a pasar mucho menos tiempo en la calle, por lo que nuestra actividad se ha desplazado al ciberespacio. Podemos destacar como ejemplo, un breve estudio de la OCDE (Organización para la Cooperación y el Desarrollo Económico), publicado el mes de mayo de 2019, en el que se muestra un aumento del 60% en el tráfico de los puntos de intercambio de Internet, es decir, la mayoría de las personas se localizaban en internet, bien estudiando, trabajando, realizando videollamadas, etc.[40] Por lo tanto, como bien hemos visto anteriormente, el aumento del uso de internet aumenta exponencialmente las probabilidades de victimización.

[40] Martaviolat (5 agosto 2020), *El incremento del ciber crimen por el COVID-19 ¿es real?, Artículos, Cyber.*

### 6.1. El incremento del cibercrimen por el COVID-19.

El cibercrimen sigue siendo una amenaza mundial, los delincuentes emplean métodos innovadores con el fin de incrementar el volumen y la sofisticación de sus ataques. La pandemia ha sido aprovechada por los delincuentes para atacar a personas vulnerables, los cuales a través del phishing, las estafas en línea y la difusión de noticias falsas incitaban a comprar artículos que, supuestamente, prevendrían o curarían el COVID-19.

El descubrimiento de material de abuso sexual infantil en línea ensayo un fuerte repunte en el punto culminante de la crisis de COVID-19. La tendencia de maltrato infantil sigue aumentando y lo hizo aún más durante la crisis de la pandemia, cuando, entre otras, las restricciones de viaje imposibilitaron que los delincuentes abusaran físicamente de los niños. Un ejemplo que podemos destacar son las aplicaciones de videoconferencia en sistemas de pago, este material no se graba y por lo tanto, se transforma en un reto fundamental para los organismos de represión.

En cuanto a la *web* oscura, en 2019 y a principios de 2020 encontramos una gran inestabilidad ya que no hay un mercado principal claro a lo largo del último año. Aún así, *Tor*[41] sigue siendo la infraestructura preferida, pero ello no quita que los delincuentes hayan comenzado a usar otras plataformas de mercado descentralizadas y centradas en la privacidad para así vender sus productos ilegales. Dichas plataformas han experimentado también un aumento en el último año[42].

---

[41] Tor (Sigla de *The Onion Router* -en español- El Enrutador Cebolla), se trata de un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet, en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revela su identidad, es decir, su dirección IP y, además, mantiene la integridad y el secreto de la información que viaja por ella.

[42] Centro de Documentación Europea de Almería, 07/10/2020. El informe de Europol sobre el cibercrimen en 2020 actualiza las últimas tendencias y el impacto actual del cibercrimen dentro y fuera de la UE.

También podemos destacar el informe elaborado por la Europol[43] en el año 2020, que hace incidencia a la adaptación de los modelos de negocios de los delincuentes, con el propósito de obtener el máximo provecho de la pandemia. Dichos delincuentes ajustan su modus operandi a las nuevas oportunidades que ha dado el coronavirus. La alta demanda de productos de equipos de protección y medicamentos, el aumento de los sistemas informáticos y del teletrabajo son los principales factores que han impulsado estos cambios en la actuación del crimen organizado y el terrorismo.[44].

Podemos sostener que los delincuentes se trasladan de las calles a los ordenadores, por lo tanto es lógico pensar que los delitos en Internet iban a aumentar, ya que si todo queda cerrado y paralizado en las calles, y en consecuencia, todo acontece en Internet, como el trabajo, las compras *online, entre otros,* también es normal pensar que el delito vaya a acontecer allí[45].

La posibilidad de que el mayor uso de Internet supondrá un aumento de la cibercriminalidad se fundamenta en la relación entre cotidianidad, oportunidad y delincuencia: ya que ahora donde más tiempo pasamos es en Internet será también allí donde surjan las nuevas oportunidades que interaccionarán son sus motivaciones delictivas, así como también las víctimas coincidirán en el ciberespacio con aquellos que les atacan[46].

Ahora bien, no se trata de pasar más tiempo en Internet lo que conllevará un aumento de la cibercriminalidad, sino hacer más cosas en Internet y sobre todo, hacer cosas que antes no hacíamos, es lo que llevará a que se perpetren nuevos crímenes a través del mismo. Por otro lado, el

---

[43] La Europol es la agencia de la Unión Europea en materia policial. Su principal objetivo es contribuir a la consecución de una Europa más segura para el beneficio de todos los ciudadanos de la UE.

[44] *El ciber crimen sigue en aumento,* publicado el 12 de octubre, 2020 por Iniseg.

[45] MIRÓ LLINARES, F. , *Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situaciones de ciberdelitos.* Pág. 4.

[46] MIRÓ LLINARES, F. , *Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situaciones de ciberdelitos.* Pág. 5.

término «cibercriminalidad» explica una macrocategoría de maneras delincuenciales expresamente unidas por acontecer en el ciberespacio, es decir, que todas ellas juntas en Internet crean un elemento esencial del evento delictivo[47].

Así, también podemos destacar un informe de Thales, el cual nos dice que los ataques delictivos iniciales tenían principalmente fines económicos, pero conforme avanzaba la pandemia también se observaron actividades de espionaje de grupos respaldados por Estados. La mayoría de los ciberdelitos se llevaban a cabo mediante *webs* o programas que estaban relacionados con la pandemia, como ataques que suplantaban la identidad de autoridades sanitarias a través de correos electrónicos, también encontramos ataques que dirigían a webs falsas relacionadas con ayudas para la pandemia que lo que pretendían era robar la información financiera de las víctimas. Los expertos aconsejan para evitar estos ataques como el *phishing,* capaz de obtener contraseñas o accesos a cuentas bancarias, no abrir archivos adjuntos sospechosos o que provengan de emisores desconocidos, así como únicamente instalar *software* de fuentes fiables[48].

En cuanto a las transacciones económicas que se han disparado a raíz del cambio que hemos experimentado en el día a día con la pandemia, señalan que aquellas personas que han tenido que ajustarse a las nuevas tecnologías y en concreto, a realizar pagos vía Internet, han sido las verdaderas víctimas de aquellos expertos o hackers en la perpetración de delitos informáticos. Y es por ello, que el impacto del cibercrimen en 2020 ha sufrido un aumento, encontrando mas ciberestafas, daños informáticos, ciberacosos y un largo etcétera. Pero también debemos destacar como otro grave problema la piratería para obtener a través de ésta programas informáticos vulnerando la

[47]MIRÓ LLINARES, F. , *Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situaciones de ciberdelitos.* Pág. 5 y ss.

[48] *La ciberdelincuencia saca partido de la COVID-19, 20* mayo 2020, por Inversis.

propiedad intelectual e industrial[49], tratándose de amenazas que pueden afectar a cualquier persona[50].

Por lo tanto, podemos afirmar que los ciberdelitos han aumentado con la pandemia ya que el número de ciberataques es importante debido al «cuasi uso obligatorio de las nuevas tecnologías a partir del mes de marzo»[51] y se predice que lo sigan haciendo.

### 6.2. El COVID y las vacunas como nuevo cebo del cibercrimen.

Como bien veníamos viendo, la COVID-19 ha supuesto un gran impacto en la ciberseguridad de los usuarios durante este último año. Los ciberdelincuentes se han aprovechado de la situación y han empleado, frecuentemente, contenidos relacionados con este nuevo virus como cebo para introducir *malware.* Así, por otro lado, el aumento del teletrabajo del que hemos sido testigos también ha propiciado el aumento de dichos incidentes. Por lo tanto, podemos llegar a la conclusión de que la vacuna contra el Covid-19 como cebo, el teletrabajo y el comportamiento de los usuarios van a ser las tres grandes tendencias del cibercrimen para 2021.

La consolidación del teletrabajo dada la situación actual de la pandemia ha llevado a que los ciberdelincuentes puedan actuar en una superficie más amplia, ya que los ordenadores con los que suelen trabajar las oficinas, por lo general, suelen contar con una mayor protección que los que vamos a utilizar para trabajar en nuestras casas y es por ello, que vamos a ser más vulnerables a la hora de realizar nuestro trabajo en casa.

---

[49] La propiedad intelectual e industrial se refiere a las creaciones de la mente y se trata de un derecho patrimonial de carácter exclusivo y territorial, ya que lo otorgan los Estados por un tiempo determinado para explotar o usar en forma industrial o comercial invenciones o innovaciones,

[50] Silvia Verdugo, *el impacto del cibercrimen aumentó en 2020 con motivo de la pandemia, 11/02/2021, ABCdesevilla.*

[51] VERDUGO, S. Profesora de Derecho Penal del Grado en Derecho del Centro de Estudios Universitarios Cardenal Spínola CEU. "*Retos jurídicos ante la crisis del Covid-19".*

Por otro lado, el comportamiento de los usuarios también va a ser muy relevante en este aumento del cibercrimen. Vamos a destacar un estudio realizado por la organización *Identity Theft Resource Center (ITCR),* la cual considera que los ciberdelincuentes tiene cada vez más en cuenta el comportamiento de los usuarios a la hora de realizar los ciberataques. También hacemos referencia al informe *Cybercrime SOS research de cxLoyalty,* el cual apuntó que más de la mitad de los encuestados, es decir, un 55% aproximadamente, no está seguro de poder impedir un delito cibernético y la mitad, no confía en poder detectarlo. La ciberdelicnuencia ha venido para quedarse, así lo corroboran los datos que hemos visto hasta ahora, y por lo tanto, las empresas deben educar, prevenir y proteger a sus clientes[52].

En medio de toda esta gran crisis, encontramos organizaciones cibercriminales interesadas en obtener información sensible sobre la vacuna de la COVID-19, extorsionar a quienes la producen, sabotear su desarrollo o distribución, robar datos sanitarios o sacar partido del boom informativo para estafar a la gente. Ahora bien, algunos de estos ciberataques han trascendido, pero otros ni siquiera se han comunicado, ya que en los asuntos de seguridad cibernética la norma es el secretísimo.

Podemos destacar, que en noviembre de 2020 se hizo público que investigadores del laboratorio británico y de la Universidad de Oxford que estaban participando en el desarrollo de la vacuna recibieron falsas ofertas de trabajo, las cuales incluían *software* malicioso con el objetivo de entrar en sus ordenadores.

Se atribuye al norcoreano Lazarus[53] el ataque contra AstraZeneca y la Universidad de Oxford. Así, Corea del Sur acusó en febrero a Corea del Norte de tratar de hacker allí a Pfizer para robarle información de la vacuna. Se

[52] Eduardo Esparza, VP General Manager de Affinion España.

[53] Se trata de una organización de hackers que se hace llamar Lazarus (o Darkseoul) y que nació en Corea del Norte en el año 2009. Uno de los grupos de espionaje mas conocidos.

piensa que Lazarus estaría también detrás de este incidente, que comprometió a “un Ministerio de Sanidad” y a “una compañía farmacéutica que está desarrollando una vacuna contra el covid-19”.

No obstante, también robaron información sobre la vacuna en Estados Unidos, Reino Unido y Corea del Sur, en este caso fue la norcoreana Velvet Cholima, así su organización hermana Labyringth Cholima intento boicotear varias plantas estadounidenses de producción de vacunas, según la empresa de ciber seguridad *CrowdStrike.*

Ahora bien, centrándonos en nuestro país, el Centro Nacional de Inteligencia (CNI)[54] hizo público que *hackers* provenientes de China habrían sustraído información que estaba relacionada con la vacuna que preparan investigadores españoles. Por ello, la directora de dicha organización, Paz Esteban, alarmó de “una campaña, especialmente virulenta, no solo en España, contra laboratorios que trabajan en la búsqueda una vacuna para la covid-19”. Como consecuencia, las autoridades españolas dieron inicio a un dispositivo especial de vigilancia digital a partir del día 15 de marzo de 2020, coordinado por el Consejo Nacional de Ciberseguridad.

Como hemos podido observar, la mayoría de los incidentes relacionados con la covid-19 son estafas y fraudes informáticos que buscan información sobre patentes de vacunas para poder extorsionar. Los ciberdelincuentes han ido modificando sus ataques conforme ha ido avanzando la pandemia, cuando las muertes cobraron importancia, la información científica que diera lugar a conseguir una vacuna efectiva pasó a ser primordial. Por lo tanto, su objetivo principal es obtener información sensible. Para ello se lleva a cabo el espionaje científico, el cual es silencioso y difícil de atribuir, siendo en ocasiones imposible[55].

---

[54] En Centro nacional de Inteligencia es el servicio de inteligencia de España, creado en 2002. Dicho servicio se integra dentro de la estructura general del Ministerio de Defensa, como un organismo público con autonomía funcional y autonomía jurídica propia, así como plena capacidad de obrar.

[55] MANUEL, G. Pascual, Madrid 23 de marzo 2021, EL PAÍS: Sabotajes, espías y robo de datos: la guerra invisible por la vacuna de la civid que se libra en el ciberespacio.

Por lo tanto, se ha constatado un aumento de campañas masivas que emplean el tema como cebo. Un estudio de la empresa *Check Point* confirma que desde noviembre de 2020 se disparan los dominios que contiene la palabra “vacuna”, además en algunos casos también se incluía la palabra “covid-19” o “corona”. Asimismo, los ciberdelincuentes también han utilizado como herramienta las campañas de *phishing* mediante correo electrónico, adjuntando archivos a través del gancho de la vacuna, que cuando clickeas para acceder instala un programa para robar información.

## 7. Conclusiones.

El cibercrimen engloba todas aquellas actividades ilícitas que ocupan Internet o el ciberespacio como lugar del delito, ya sea el objetivo del delito o la herramienta. Dado a la evolución del mismo, podemos ir desde las descargas ilegales de contenido con derechos de autor, siendo estas consideradas como el núcleo del cibercrimen unos años atrás, hasta robos económicos, filtración de datos, robo de información personal, espionaje y un largo etcétera.

Para poder adaptarse a estas novedosas realidades informáticas arriba mencionadas, se vio necesario una modificación de los tipos penales existentes. Que estos delitos se lleven a cabo mediante Internet no legaliza, así como tampoco exime a ninguna conducta de su encaje en el Ordenamiento Jurídico.

Si bien, el delito de estafa en su tipo básico, se encuentra regulado en su artículo 248 del Código Penal, perteneciente a la sección primera, tratándose de delitos contra el patrimonio y el orden socioeconómico , y nos dice en su apartado primero: “cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno”. Así, nuestro Código Penal, va a introducir en el segundo apartado de dicho artículo la estafa informática,

que también considera 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; los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de estafas previstas en ese artículo; los que utilizando tarjetas de crédito débito, o cheques de viaje, o los datos sobrantes en cualquiera de ellos, realice operaciones de cualquier clase en perjuicio de su titular o de un tercero”. Por lo tanto, podemos observar una ampliación notable en el tipo básico de estafa. No obstante, esto no impide la dificultad a la hora exigir responsabilidades a los autores de dichos delitos.

Por otro lado, la doctrina, en su mayoría, considera que el bien jurídico protegido es el patrimonio en este tipo de delitos, y la ley manifiesta que no se considera consumado dicho delito hasta que no se lleve a cabo el daño patrimonial. Mientras que el bien jurídico protegido en los delitos informáticos es la información. La estafa se lleva a cabo mediante el engaño y los delitos informáticos a través de la manipulación de datos. A mi parecer, los cibercrímenes pueden afectar a varios intereses, ya que en el caso del espionaje puede afectar a la intimidad, y el caso del *spyware* puede ser también el patrimonio de la víctima, entre otros.

Gracias a estos avances y a la posible tipificación de estos delitos en nuestro Código Penal, permite, aunque no fácilmente y contando con una gran ausencia de medidas preventivas, la persecución de estos actos ilícitos que perpetran sus autores utilizando medios tecnológicos. Por lo tanto, corresponde a los Estados garantizar esa seguridad, es decir, velarán para que se cumplan las medidas adecuadas a dicho riesgo, así como también a la hora de prevenir y reducir dichas conductas que afectan a la seguridad ciudadana. En este sentido, todavía nos queda mucho por lo que luchar.

Actualmente nos encontramos en una situación difícil de gestionar debido a la pandemia del COVID-19, y con ello se ha podido observar un

aumento notable de este tipos de delitos, ya que hemos pasado prácticamente de un espacio físico al ciberespacio, así como también un gran porcentaje de la población se ha visto afectado económicamente. Hoy en día todo el mundo tiene acceso a Internet, la mayoría de las personas lo usamos y ni si quiera sabemos donde navegamos, ni donde introducimos los datos de nuestras tarjetas de crédito, así como muchas veces también se mantiene contacto con desconocidos, por lo tanto, los delincuentes se han aprovechado de esta situación y de los más vulnerables.

Cabe decir, que esta también en nuestras manos reducir y prevenir estos tipos de delitos, adoptando para ello las medidas de seguridad adecuadas que estén a nuestra disposición.

## 8. Bibliografía y materiales de referencia.

- FERNÁNDEZ TERUELO, J.G. *Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red.* Revista de Derecho Penal y Criminología, 2007.

- MIRÓ LLINARES, F. *El cibercrimen. Fenomenología y criminología de la* delincuencia *en el ciberespacio, 2012.*

- MOISÉS BARRIO, A. (Letrado del Consejo de Estado. Profesor de Derecho Público, ICADE, Madrid. Abogado). *La ciberdelincuencia en el Derecho Español.* Revista Cortes Generales, pág. 276 y ss.

- ARROYO DE LAS HERAS, A. *Los delitos de estafa y falsedad documental, 2005, pág. 22.*

- CHOCLÁN MONTALVO, J.A. *El delito de estafa, pág. 189 y ss.*

- GALÁN MUÑOZ, A. *El fraude y la estafa mediante sistemas informáticos, análisis del artículo 248.2 del Código Penal Español, 2005, pág. 183.*

- Gete-Alonso y Calera, Mª del C. *Las tarjetas de Crédito, pág. 115.*

- MIRÓ LLINARES, F. , *Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situaciones de ciberdelitos.*

- Silvia Verdugo, *el impacto del cibercrimen aumentó en 2020 con motivo de la pandemia, 11/02/2021, ABCdesevilla.*

- VERDUGO, S. Profesora de Derecho Penal del Grado en Derecho del Centro de Estudios Universitarios Cardenal Spínola CEU. "*Retos jurídicos ante la crisis del Covid-19.*

- *MANUEL, G. Pascual, Madrid 23 de marzo 2021, EL PAÍS: Sabotajes, espías y robo de datos: la guerra invisible por la vacuna de la civid que se libra en el ciberespacio.*

- *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.*

- Ley Orgánica 1/2015 de 30 de marzo, que modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

- Páginas Web de Noticias Jurídicas.

- Buscador de Jurisprudencia del Tribunal Supremo (Poder judicial).