La estafa informática en el Código Penal Argentino

María Milagros Roibón

Correo electrónico: milagrosroibon@gmail.com

I.- Nociones generales sobre los delitos informáticos y las pérdidas económicas que generan

En la página web de las Naciones Unidas se explica que el delito informático consiste en "*una forma emergente de la delincuencia transnacional y uno de los de más rápido crecimiento. A medida que Internet se ha convertido en una parte casi esencial de nuestras vidas, suministrando información y comunicación en todo el mundo, los delincuentes le han sacado provecho. Con unos dos mil millones de usuarios en todo el mundo, el ciberespacio es el lugar ideal para los delincuentes, ya que pueden permanecer en el anonimato y tener acceso a todo tipo de información personal que, a sabiendas o inconscientemente, guardamos en línea. Las amenazas a la seguridad en Internet se han disparado de forma espectacular en los últimos años, y el delito cibernético afecta ahora a más de 431 millones de víctimas adultas a nivel mundial.*

El delito cibernético existe en muchas formas, siendo los más comunes los relacionados con la identidad. Esto ocurre por phishing (engañar a los usuarios de Internet para que den sus datos personales), el malware (software instalado involuntariamente que recoge información personal) y hacking (acceso ilegal a la computadora de alguien de forma remota). Los delincuentes tienden a utilizar estos métodos para robar información de tarjetas de crédito y dinero. Por otra parte, Internet también se ha convertido en un lugar para los delitos relacionados con los derechos de autor y derechos de propiedad intelectual; y también delitos como la pornografía infantil y material de abuso.

El delito cibernético ha ido creciendo más fácilmente a medida que avanza la tecnología y los autores ya no requieren grandes habilidades o técnicas para ser una amenaza. Por ejemplo, las herramientas de software que permiten al usuario localizar

puertos abiertos o anular la protección de contraseña se pueden comprar fácilmente en línea. Lo que no ha crecido fácilmente, por desgracia, es la capacidad para encontrar a los responsables. Con el anonimato que ofrece el ciberespacio, es difícil para las fuerzas del orden identificar y localizar a los delincuentes. Lo que se sabe, sin embargo, es que más de tres cuartas partes de la delincuencia cibernética están hoy vinculadas a la actividad de la delincuencia organizada".

En ese sentido, la empresa Welive Security sostiene que, en la actualidad, el cibercrimen funciona como un servicio. Los criminales ofrecen sus productos o infraestructura en el mercado negro a cambio de un precio. Existe un proceso de comercialización y distribución del software y de los productos y servicios que los cibercriminales ofrecen en esta industria. Si bien "*el escenario del cibercrimen es bastante heterogéneo. Por un lado, muchos jóvenes con una ética cuestionable deciden incursionar en este mundo en busca de obtener rédito económico, pero sobre todo para ser reconocidos entre sus pares. Es probable que muchos de estos jóvenes, dada su inexperiencia, comiencen realizando ataques que requieran poca complejidad o sofisticación y busquen aprovecharse del uso de viejas técnicas que aún siguen funcionando. Pero sería un error creer que estos jóvenes representan a todo lo que uno puede encontrar en el universo de los actores maliciosos… la industria del cibercrimen presenta características como las de una empresa de software… es muy probable que algunos grupos organizados de cibercriminales cuenten con una oficina, que tengan sus empleados, que exista un proceso de comercialización y distribución del software y de los productos y servicios que se ofrecen. En el caso de los grupos organizados, existen aquellos que cuentan con respaldos gubernamentales y que… utilizan herramientas más complejas para lograr sus objetivos, ya que cuentan con un presupuesto más generoso*".

A su vez, el informe titulado "Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe", publicado por la Organización de Estados Americanos (OEA), revela que el 92 por ciento de los bancos de la región fueron víctimas de ciberataques en 2018 y que, en el 2017, a estas organizaciones el responder a estas amenazas y recuperarse de ciberataques les costó 809 millones de dólares. En julio del 2018 la empresa IBM publicó un estudio en el que se encuestaron a 500 empresas en 15 países. En él, se calculó que los

costos asociados a “megaviolaciones” (rango entre uno y 50 millones de registros perdidos) les cuestan a estas compañías entre 40 y 350 millones de dólares, respectivamente. Según esta investigación, la violación de datos aumentó 6,4 por ciento en comparación con 2017 y llegó a los 3,86 millones de dólares.

Igualmente, la empresa Panda Security S.L. manifestó que la cantidad de ciberataques perpetrados aumentó en forma asombrosa. Estiman que en el 2018 hubo casi dos veces más incidentes de ciberseguridad en empresas comparado con el año anterior. La empresa detectó unas 159.000 brechas de datos impulsadas por ransomware (programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción) o por nuevos métodos de ataque, siendo escalofriantes las consecuencias económicas de estos incidentes. Se espera que el coste global del cibercrimen supere los 2 billones de dólares en 2019.

En síntesis, las pérdidas económicas causadas por el cibercrimen resultan abrumadoras, con tendencia a incrementarse en el corto y mediano plazo, siendo los países en desarrollo los más afectados por este tipo de criminalidad. Las Naciones Unidas consideran que estos países *“carecen de la capacidad para combatir los ciberataques y otras formas de la delincuencia cibernética. Por lo tanto, no es sorprendente que las tasas de victimización sean mayores en los países con menores niveles de desarrollo. Los delincuentes también explotan las lagunas jurídicas y las débiles medidas de seguridad de los países para perpetrar delitos cibernéticos. La falta de cooperación entre los países desarrollados y en desarrollo también puede resultar en "refugios seguros" para aquellos que cometen delitos cibernéticos”*. Un estudio difundido en agosto de 2018 en Panamá por la compañía rusa Kaspersky Lab registró 746.000 ciberataques en los últimos 12 meses en Latinoamérica, un incremento del 60 por ciento con respecto al período anterior, en un promedio de 9 ataques por segundo en la región. Según los expertos, los países y las empresas latinoamericanos constituyen un blanco fácil para las organizaciones cibercriminales, ya que muchas compañías son reactivas y no proactivas en lo que hace a las políticas y medidas de prevención frente a los ataques informáticos.

Las Naciones Unidas también señalan que “*la delincuencia cibernética ha crecido rápidamente convirtiéndose en un negocio que puede superar $ 3.000.000.000.000 al año.*

Sin una normativa adecuada y una capacidad insuficiente en muchos países, la lucha contra la delincuencia cibernética es difícil. Se necesita un esfuerzo mundial para proporcionar una mejor protección y regulaciones más firmes porque los delincuentes cibernéticos hasta ahora se han escondido dentro de vacíos legales en los países con menos reglamentación Los autores y sus víctimas pueden ser localizados en cualquier lugar, pero los efectos se ven a través de las sociedades, destacando la necesidad de una respuesta internacional urgente y enérgica".

II.- <u>Definición y clasificación de los delitos informáticos</u>:

1.- En la actualidad no existe un conceso sobre lo que se conoce como delitos informáticos. Sin embargo, Gustavo Sain manifiesta que cuando *"se habla de este tipo de criminalidad, el significado más utilizado… es aquel que los describe como conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo. En el primer caso, si una persona intimida o intenta chantajear a otra persona vía correo electrónico, el dispositivo informático actúa como medio para cometer el hecho ilícito, siendo el delito de amenaza el hecho ilícito en sí. En el segundo caso, el dispositivo informático es el objeto o blanco del crimen, donde una persona puede enviar un virus a la computadora de un tercero y así dañarla o inutilizarla o alterar su funcionamiento. En este último caso, la figura delictiva podría encuadrarse dentro del daño en tanto delito contra la propiedad, considerando el dispositivo informático como un bien tangible, tanto, así como la información que puede almacenar. En ese sentido, los delitos informáticos son entendidos en base al lugar que ocupa la tecnología para la comisión del delito, más que a la naturaleza delictiva del acto mismo… De las diferentes definiciones existentes en delitos informáticos… la mayoría utiliza cuatro criterios de clasificación.*

El primero de ellos es <u>legal</u>, en tanto que aquellos hechos indebidos relacionados con dispositivos informáticos pueden ser considerados delito informático, siempre y cuando dichas conductas se encuentren <u>penadas por la ley</u> o, en su defecto, sean susceptibles de tipificación…

Otro criterio utilizado es el técnico. En ese sentido, algunas definiciones refieren comportamientos que involucran computadoras, mientras que otros lo hacen respecto a todo tipo de dispositivos informáticos, es decir cualquier equipamiento capaz de realizar tareas en forma automática…

El tercer criterio de clasificación es el entorno, donde algunos limitan este tipo de conductas a los hechos ilícitos e ilegales que se manifiestan en Internet…

Por último, algunas definiciones consideran que los delitos informáticos son aquellos que requieren la aplicación de técnicas y herramientas informáticas en el proceso de investigación para la resolución condicionante de un caso judicial. Esta clasificación no resulta aplicable en términos criminológicos, en tanto que la implementación de pericias forenses de tipo informático se realiza en la actualidad en la multiplicidad de casos no vinculados con el uso de dispositivos informáticos como medio para cometer el ilícito o fin del delito…

Esta ambigüedad que posee el alcance conceptual de los delitos informáticos se ve reflejada en los diferentes nombres que adquieren diferentes unidades policiales, fiscalías especializadas u organismos públicos abocados al tratamiento de los mismos. Así, denominaciones como "delitos informáticos", "cibercrimen", "delitos tecnológicos", "crímenes cibernéticos", "delitos telemáticos", "crímenes electrónicos", "delitos de alta tecnología" o "crímenes por computadora" son frecuentes en estos tipos de oficinas" (Gustavo Sain – Horacio Azzolin, "Delitos informáticos. Investigación criminal, marco legal y peritaje", Editorial IB de f, 2018, páginas 8 a 11).

Hernán C. Waker, Diego Rojo Delaux y Francisco Curi definen a los delitos informáticos "*como aquellas conductas disvaliosas socialmente y reprochables desde el punto de vista penal, que, concretadas mediante instrumentos y sistemas informáticos y virtuales, pueden tener como objeto la violación de cualquiera de los bienes jurídicos tuteladas por la ley, en un momento dado"* ("Derecho Informático", Tomo 4, Directora: Faustina Zarich, Editorial Juris, 2005, página 134).

Con más apego a la teoría penal general, Anzit Guerrero, Tato y Profumo, definen al delito informático como "*toda acción (acción u omisión) culpable realizada por un ser*

humano, tipificado por la ley, que se realiza en el entorno informático, y está sancionado con una pena… El elemento informático puede intervenir como medio o como objeto. Interviene como medio cuando se utilizan elementos informáticos para realizar la acción delictiva; por ejemplo, utilizar una computadora para falsificar dinero. Interviene como objeto cuando la acción delictiva tiene como fin el daño a un sistema informático; por ejemplo, cuando un virus borra información de una computadora" ("El Derecho Informático – Aspectos Fundamentales", ed. Cátedra Jurídica", páginas 145 y 146).

Según la página web Wikipedia, un delito informático es *"toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet… La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático".*

En síntesis, la delincuencia informática comprende un amplio tipo de actividades ilícitas que **tienen en común el medio electrónico en el que tienen lugar o del que se valen.**

2.- En cuanto a la clasificación de los delitos informáticos, transcribiré al Dr. Diego Migliorisi, quien considera que los mismos se dividen en dos grandes grupos.

"Por un lado, los delitos históricamente tipificados en el Código Penal Argentino, cuya configuración se realiza utilizando medios informáticos y, por supuesto, Internet. Es decir que su existencia data de tiempos anteriores a la creación de Internet y la informática, y solamente se incorpora un nuevo medio para configurarlos.

A este grupo lo llamaremos ***ciberdelitos tipificados o delitos tradicionales del Código Pernal que se configuran a través de Internet****.*

Por otro lado, al segundo grupo lo denominaremos ***ciberdelitos propiamente informáticos****, puesto que son aquellos que surgieron con la tecnología, es decir con el nacimiento de la informática e Internet. También este grupo está integrado por delitos que están tipificados en el Código Penal, pero que han mutado sus efectos al ciberespacio, como el fraude informático y el daño informático, para citar algunos ejemplos".* (Migliorisi, Crímenes en la web. Los delitos del siglo XXI. Editorial del Nuevo Extremo, año 2014, página 37).

III.- La estafa informática en el Código Penal argentino

La ley 26.388 (sancionada el 4/6/2008) incorporó al Código Penal argentino un conjunto de ilícitos que se consideran "delitos informáticos". Además, modificó algunos tipos existentes para incorporar nuevas modalidades de comisión a través de los medios electrónicos. Es así que se agregó el inciso 16 al artículo 173, el que establece que: "*El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o a la trasmisión de datos*".

Jorge Eduardo Buompadre expresa que esta nueva modalidad constituye una figura especializada en relación a la estafa prevista en el art. 172, por el medio empleado (un sistema informático), aunque con anterioridad ya se había contemplado la posibilidad de defraudar con tarjetas de compra, débito o crédito sustraídas o extraviadas incluso si se lo hacía mediante operaciones automatizadas (art. 173, inciso 15, incorporado por la Ley 25.390). (Buompadre. Manual de Derecho Penal. Parte especial. 3ª reimpresión. Editorial Astrea, año 2017, página 476).

Pablo A. Palazzi considera que esta inclusión al código de fondo *"buscar incorporar ciertas situaciones patrimoniales abusivas relacionadas con la informática como una modalidad de defraudación, para superar el problema que presentaba en nuestro derecho y en el comparado respecto de la imposibilidad de estafar o engañar a una máquina u ordenador"*. (Palazzi. Los Delitos informáticos en el Código Penal. Anàlisis de la ley 26.388, Editorial Abeledo Perrot, año 2009, página 169). Buompadre señala que con esta nueva disposición legal "*desaparecen las hipótesis de atipicidad que se daban por no concurrir en el caso concreto la secuencia tradicional de la estafa (ardid o engaño, error, disposición patrimonial perjudicial), en especial el engaño a otro a que hace referencia el art. 172 del Cód., que… requiere para su determinación el engaño a otra persona física*" (obra citada, página 476).

La propiedad o el patrimonio de la víctima constituyen el bien protegido por esta figura, como sucede en la defraudación. Por otro lado, el Dr. Marcelo Riquert en su blog sobre delincuencia informática (riquertdelincuenciainformatica.blogspot.com) expresa que "*Matiza, por su lado, Mariluz Gutiérrez Francés diciendo que se siente inclinada a reconocer que las defraudaciones por medios informáticos lesionan algo más que el*

patrimonio en cuanto hay un interés social valioso y digno de protección, de carácter macrosocial, cuál sería la confianza en el funcionamiento de los sistemas informatizados... Acompañan la noción de "pluriofensividad" en las conductas de fraude informático propuesta por la profesora de Salamanca los autores chilenos Magliona Markovicth y López Medel, sosteniendo que en cada una de las modalidades se produce una doble afectación: la de un interés económico micro o macrosocial (individual o colectivo, como la Hacienda Pública) y la de un interés macrosocial vinculado al desempeño mismo de los sistemas informáticos, es decir, de la confianza en su correcto funcionamiento".

1.- Acción típica: La acción típica de la estafa informática consiste en defraudar a otro "*mediante cualquier técnica de manipulación informática".* La manipulación debe alterar el funcionamiento del sistema informático o de telecomunicaciones. Migliorisi explica que *"No es cualquier manipulación informática, sino solo la que es apta para producir dicho efecto*" (obra mencionada, página 119). Esta acción típica genérica convierte -según Palazzi- a la figura bajo análisis en "*una suerte de tipo penal abierto en relación con cualquier abuso informático"* (obra citada, página 180).

En ese sentido, Buompadre sostiene que aun sin ardid o engaño, "*el legislador ha presupuesto, mediante una cláusula general, que el uso de una técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o trasmisión de datos, realizados para causar un perjuicio económico a un tercero, es una forma de estafa que se castiga conforme a la escala penal prevista para los diferentes tipos de fraude tipificados en el art. 173"* (obra mencionada, página 477).

Ahora bien, ¿qué modalidades puede asumir la conducta típica de este delito? Las mismas pueden ser diversas. Por ejemplo, la alteración de registros informáticos, la obtención de un servicio de telecomunicaciones sin haberlo abonado previamente, el fraude informático mediante interceptación de conexiones, el phishing (que es una variante de estafa informática que consiste en la captación de datos bancarios y de tarjetas de crédito de clientes, aunque su objeto también puede ser la obtención de claves u otro tipo de información), la estafa por *typosquatting* (en este supuesto, el delincuente se aprovecha del error de tipeo de la víctima, la que lo llevará a una falsa página web con una denominación muy parecida a la que quería llegar. En este caso, la víctima ingresa a una página estéticamente idéntica a la que realmente

quería entrar, sin darse cuenta que se trata de una página falsa. Una vez dentro de la página, el usuario ingresará los datos que utiliza para acceder al portal de su tarjeta de crédito, su banco, etc. Luego estos datos se remitirán al ciberdelincuente), etc. Explicar cada una de estas modalidades supera ampliamente el objeto del presente artículo.

Buompadre expresa que el tipo penal "*requiere el uso de un sistema informático como instrumento o medio a través del cual se produce el hecho lesivo del patrimonio ajeno. Se trata de un tipo de acción, por lo que la acción por omisión no parece posible; la referencia a cualquier técnica de manipulación informática impide toda consideración al respecto*" (obra referenciada, página 477).

2.- Medios típicos: Buompadre aclara que el medio comisivo del tipo penal exige "*el empleo de una técnica de manipulación informática, esto eso, cualquier modificación del resultado de un proceso automatizado de datos, sea que se produzca a través de la introducción de nuevos datos o de la alteración de los existentes en el computador, en cualquiera de las fases de su procesamiento o tratamiento informático"* (obra mencionada, página 477).

Según la Wikipedia:

2.a. - un sistema informático se trata de un "*sistema que permite almacenar y procesar información; es el conjunto de partes interrelacionadas: hardware, software y personal informático. El hardware incluye computadoras o cualquier tipo de dispositivo electrónico, que consisten en procesadores, memoria, sistemas de almacenamiento externo, etc. El software incluye al sistema operativo, firmware y aplicaciones, siendo especialmente importante los sistemas de gestión de bases de datos*", y

2.b.- la trasmisión de datos consiste en "*la transferencia física de datos (un flujo digital de bits) por un canal de comunicación punto a punto o punto a multipunto. Ejemplos de estos canales son cables de par trenzado, fibra óptica, los canales de comunicación inalámbrica y medios de almacenamiento. Los datos se representan como una señal electromagnética, una señal de tensión eléctrica, ondas radioeléctricas, microondas o infrarrojos*".

Por ende, no cualquier manipulación informática es apta para que se configure la estafa informática, sino aquella que altere el normal funcionamiento del sistema informático o de comunicaciones, como el caso de que la anormalidad funcional se origine en fallas del sistema preexistentes y no provocadas. En este supuesto, estaríamos ante un caso de atipicidad. Según Palazzi, los casos de ingeniería social (es decir el conjunto de actividades o engaños que los atacantes usan para obtener información o bienes de las organizaciones a través de la manipulación de los usuarios legítimos) no se encuentran incluidos dentro de esta figura penal (obra citada, páginas 182 y 183).

3.- Sujetos del delito: El sujeto activo de la estafa informática puede ser cualquier persona, sin que importe que se trate o no de alguien autorizado a ingresar al sistema. Es decir que se trata de un tipo penal de titularidad indiferencia. En cambio, el sujeto pasivo -opina Riquert- "*es aquel a quien patrimonialmente se perjudica mediante la manipulación del sistema o transmisión de datos, pudiéndose en muchos casos tratarse no sólo de personas físicas sino de existencia ideal, como compañías financieras, bancarias, bursátiles, aseguradoras, etc.".* En síntesis, el sujeto pasivo es el titular del patrimonio afectado por la estafa informática.

4.- Tipo subjetivo: La doctrina considera que se trata de un delito doloso. Migliorisi enseña que el agente "*debe conocer y querer la realización de los elementos objetivos del tipo penal. Admite la tentativa*" (obra mencionada, página 120). Riquert opina que, en principio, esta figura "*sólo parece compatible con el dolo directo*".

5.- Disposición patrimonial perjudicial: Este tipo de estafa requiere que exista un perjuicio patrimonial y ello se genera mediante la disposición patrimonial. Buompadre enseña que "*la disposición pecuniariamente perjudicial se dará cuando el sujeto pasivo se vea privado de un elemento integrante de su patrimonio por obra de la acción delictiva, cuya disminución resulta evaluable económicamente. Es el "otro" a que hace referencia el precepto legal. Es la persona física que entrega la cosa o presta el servicio, como consecuencia de la manipulación informática (p.ej., las compras de cosas por Internet*". (obra mencionada, página 477).

6.- ¿Cuándo se consuma la estafa informática? Migliorisi explica que "*la consumación se produce con el perjuicio patrimonial derivado del uso por parte del agente*

de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la trasmisión de datos del sujeto pasivo. La tentativa es admisible… es común que cada tanto llegue a la casilla de correo un e-mail de una supuesta tarjeta o banco solicitando validar sus datos remitiéndolo a un link falso, a los efectos de utilizar la información remitida. Esa intención -sin que se configure la acción- podemos afirmar que es una tentativa de fraude informático" (obra referenciada, página 120).

IV.- <u>Consideraciones finales</u>

A pesar de que los delitos informáticos poseen un bajo nivel de denuncia en la Argentina y en otros países, permitir que se incrementen sin castigar a los responsables de los mismos, implican pérdidas millonarias. En la actualidad, los países en vías de desarrollo constituyen el objetivo primordial de los delincuentes informáticos. El avance de la tecnología supone un enorme desafío: no solo para toda la vida en sociedad, sino para impedir que el cibercrimen aumente exponencialmente, amparándose, entre otros factores, en el presunto anonimato que Internet ofrece a sus autores. Los delitos informáticos no sólo causan invaluables daños económicos, sino que tienen entre sus principales víctimas, a los menores de edad, con la consecuente violación de sus derechos humanos (como sucede con los ilícitos referidos a la pornografía infantil, el grooming, etc.). La lucha contra el cibercrimen -por sus características y complejidades- no se reduce a la modificación de los tipos penales existentes o a la creación de nuevos delitos, sino que se necesitan operadores judiciales técnicamente preparados para perseguir uno de los nuevos flagelos delictivos de la modernidad: los delitos cibernéticos.

Por lo expuesto, pienso que la creación de fiscalías especializadas en la investigación del cibercrimen (especialmente en el interior del país) facilitaría que este tipo de causas cobren un gran impulso, mejorando los niveles de la persecución penal en estas investigaciones, las cuales exigen la presencia de personal altamente especializado y capacitado. De esta forma, se contribuiría, entre otras finalidades, a resguardar los derechos de los niños afectados por los delitos informáticos, así como a evitar que se generen enormes pérdidas de dinero y daños para las empresas y para las personas jurídicas radicadas en la República Argentina.