El avance de una cibercriminalidad financiera

The advance of financial cybercrime

Ubaldo Matías Garcete Piris[1]
Universidad Americana. Asunción, Paraguay.

RESUMEN
Ciertamente, el aspecto gnoseológico de las actividades ilícitas suscita nuevos métodos que vinculan a diversos injustos a partir de los lineamientos establecidos por las organizaciones criminales que, a menudo recurren al lavado de activos para ocultar el origen de sus fondos ilícitos, y ante ello, ejecutan acciones que dificultan a los sistemas de control en el ámbito económico. Para ello, ocupa interés la expansión tecnológica que incide en el entorno socio - económico, en donde la alteración monetaria en contra de la verdad financiera y de la confianza comercial se encuentran enlazadas bajo fenómenos de la sociedad de riesgo, que resultan de una interacción delictiva a través de los diversos sistemas informáticos (transaccionales). Es por tanto, que, la importancia de la presente investigación radica en el entorno del acto de la ciberdelincuencia, puesto que, el agente (activo) se aprovecha del desconocimiento de personas que realizan "transferencias" con fondos monetarios. Así, la ciberdelincuencia financiera ocupa cuidado, ante la acción ilegal que se da por vías informáticas o por el objetivo de destruir y dañar ordenadores, medios electrónicos y redes de Internet. Por tanto, hemos de analizar una parte de la dogmática que determina nuevos paradigmas de conductas en contra del sentido legal dentro del sector económico - financiero.

Palabras clave: Actividades, injustos, organizaciones, internet, económico

[1] GARCETE PIRIS, Ubaldo Matías. Docente Investigador de la Carrera de Derecho de la Universidad Americana. Asunción, Paraguay.

ABSTRACT

Certainly, the epistemological aspect of illicit activities raises new methods that link various wrongdoers based on the guidelines established by criminal organizations that often resort to money laundering to hide the origin of their illicit funds, and in response to this, execute actions that hinder control systems in the economic sphere. To this end, the technological expansion that affects the socio-economic environment is of interest, where monetary alteration against financial truth and commercial trust are linked under risk society phenomena, which result from a criminal interaction. Through the various computer systems (transactional). Therefore, the importance of this investigation lies in the environment of the act of cybercrime, since the (active) agent takes advantage of the ignorance of people who make "transfers" with monetary funds. Thus, financial cybercrime requires caution, given the illegal action that occurs through computer channels or with the objective of destroying and damaging computers, electronic media and Internet networks. Therefore, we must analyze a part of the dogmatics that determines new paradigms of conduct against the legal meaning within the economic-financial sector.

Keywords: Activities, unfair, organizations, internet, economic.

> *"Las nuevas tecnologías de la comunicación pondrían en contacto a los cibercriminales y al resto de usuarios en el entorno del ciberespacio (ambiente social virtual y asociación con cibercriminales), de lo que resultaría un proceso de contaminación criminógena"* (Skinner & Fream, 1997).

El sentido gnoseológico de la estafa mediante sistemas informáticos

El fenómeno delictivo de la estafa se ha perfeccionado a lo largo de los años conforme al avance tecnológico, y ante ello, se ha desarrollado una necesidad de implementar "medidas preventivas" como acción de control de riesgos en las relaciones

financieras, protegiendo el bien patrimonial (de terceros), de toda conducta que se vincule a la programación indebida o de los correspondientes datos falsos en el circuito económico.

Asimismo, tenemos por extensión del término criminalidad informática o "cibercrimen" que trasciende un mayor alcance, puesto que, en el se incluyen delitos como el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos utilizando ordenadores y redes como medio para realizarlos[2].

Consecuentemente, estos hechos se realizan en diversas localidades (a nivel internacional) para no llamar la atención del sistema de control, y se ve facilitado ante el inminente vínculo del comercio con el internet. No obstante, resulta indudable determinar con (objetividad) el grado de responsabilidad de las personas que participan en el círculo delictivo, pues bien, se podría apreciar una interacción con potenciales "encubridores" o participes necesarios dentro de la ejecución técnica.

En dicho sentido, también se puede dimensionar al fenómeno de "money-mules" que se ha introducido como una acción (negativa), que busca camuflaje en aquello permitido, pues, la captación de las personas (mulas) se realiza a través de correos o mensajes de textos, bajo la oferta de trabajos con importantes comisiones. Así, el trabajo que se "ofrece" conlleva una función de recepción de cantidad de dinero y posterior envió a otras cuentas; y con ello, la promoción de comisiones.

Ciertamente, el injusto penal (técnico) se evidencia de la interconexión de los verbos rectores que deducen la acción fraudulenta, que acompañan los aspectos volitivos y cognitivos por parte del sujeto infractor. Es, por tanto, que la acción también se subsume en un "fraude informático", que se desarrolla desde una planeación ilícita, y que congenia con los actos preparatorios para el efecto delincuencial, concretándose con el acto ejecutivo propio del tipo legal.

En doctrina, el despliegue de conductas que deducen el fraude económico a través de "sistemas informáticos" también se reconocen como phishing y pharming, y se evidencian en ciertos hechos fácticos vinculados a operaciones bancarias donde se incluyen manipulaciones y/o alteraciones de datos de sistemas informáticos. En ocasiones, (también) se han utilizado "troyanos", que resultan de una difusión en internet, que llegan a los

[2] Urueña Centeno, F. J. (2015, 16 de enero). Ciberataques, la mayor amenaza actual. Instituto Español de Estudios Estratégicos (IEEE) http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09- 2015_AmenazaCiberataques_Fco.Uruena.pdf

correos electrónicos, y que, una vez infectados los ordenadores, el virus detecta los accesos a los formularios bancarios e inicia el despliegue del perjuicio patrimonial.

La finalidad de esta conducta es la utilización del correo electrónico para el envío de publicidad no solicitada, donde el *phishing* y el *pharming* permiten a los creadores del *spam* la indagación de los hábitos de consumo o intereses personales del usuario, creando con ello perfiles para la remisión masiva de información de productos de mercado, aunque la técnica más masificada para ello es todavía el uso de malware, generalmente, cookies o troyanos en las páginas "web".[3]

En cuanto al sistema jurídico nacional (paraguayo), debemos recordar que por Ley N° 4.439/11 de fecha 03 de octubre de 2011 se han modificado y ampliado varios artículos de la Ley N° 1.160/97 "Código Penal Paraguayo" de fecha 26 de noviembre de 1997, modificado parcialmente por la Ley N° 3.440/08 del 16 de julio de 2008. Así, el art. 188° tipifica la conducta de: "Estafa mediante sistemas informáticos", infiriendo en una acción promovida a partir de la "intención" por parte del sujeto infractor, de obtener un beneficio patrimonial indebido, creando un nexo causal sobre el resultado de un procesamiento de "datos" mediante una programación incorrecta; el uso de datos falsos o incompletos; el uso indebido de datos; o, la utilización de otra maniobra no autorizada; causando un perjuicio al patrimonio de otro.

Ante lo expuesto, la acción delictiva establece un marco penal de seis meses a cinco años o la sanción multa, asimismo, la normativa instaura la prosecución en los casos de "tentativa". No obstante, la norma advierte que, si el que preparare un hecho punible señalado en el modelo de conducta (art. 188° inciso 1º), mediante la producción, obtención, venta, almacenamiento u otorgamiento a terceros de programas de computación destinados a la realización de tales hechos, podrá ser sancionado con una pena privativa de libertad de hasta tres años o con multa.

Ahora bien, en el caso señalado, se podrá considerar que, "no será castigado" el que renunciara a la realización del hecho preparado y desviara el peligro de que otros lo sigan preparando, o realicen el hecho; destruyera o inutilizara los medios para el efecto; o, pusiera su existencia y ubicación a conocimiento de una autoridad o los entregare a ella. En tanto, cuando dicho peligro fuera desviado o la consumación del hecho fuera impedida por

[3] Vásquez Ruano, T. (2002). Aproximación jurídica al spam desde la protección de datos de carácter personal. *Revista de Contratación Electrónica*, 33, 3 ss.

otras razones bastará que, respecto a los presupuestos señalados anteriormente, que el autor haya voluntaria y seriamente tratado de lograr este objetivo.

En otro contexto, existen fácticos que, se relacionan al injusto analizado con el "fraude informático" a partir de diversos delitos informáticos o ciberdelitos. En dicho sentido, encontramos "el hacking", que resulta en el acceso indebido a datos o programas de sistemas informáticos. Es que, la estafa por modalidad de sistemas informáticos encuentra su cimiento en la ciberdelincuencia, que congenia la astucia del sujeto infractor y sus conocimientos técnicos para lograr el beneficio patrimonial indebido.

Concretamente, podemos sostener que el delito de fraude informático se encuentra relacionado con la conducta de estafa, en cuanto al perjuicio patrimonial ajeno, y al despliegue de una programación incorrecta (para engañar); el uso de datos falsos o incompletos; el uso indebido de datos; o, la utilización de otra maniobra no autorizada. Por ello, el sistema legal debe precautelar los verbos rectores que se vinculan a las acciones ilícitas dentro de las relaciones económicas, bajo la esfera de una seguridad jurídica - financiera.

El sentido ontológico del carding

Ciertamente, el "carding" resulta en un hecho ilícito que se ejecuta a raíz del copiado de tarjetas (crédito/débito) de la víctima, para luego, utilizar el fondo (patrimonio) disponible para la adquisición de bienes en general. Algunos dogmáticos consideran que ocupa un método de estafa "online" porque se generan varias compras (pequeños montos) que se van acumulando en el tiempo, en perjuicio del titular de la cuenta.

En otra modalidad, los sujetos (activos) infractores logran conseguir la fecha de vencimiento del plástico (tarjeta) y conjuntamente, obtienen el código de seguridad a través de la utilización de programas informáticos (técnicos), que logran la revelación de datos dentro de la tarjeta magnética.

Indudablemente, estos hechos fueron perfeccionándose con la implementación de nuevas tecnologías. En tal sentido, las personas que resultaron ser víctimas de estos hechos, fueron identificando diversas "compras" que no habían realizado, y con ello, divisaron un perjuicio económico en sus estados de cuenta.

El fraude cibernético reconocido como "el carding" se ha desarrollado dentro del régimen financiero, desde el acceso a datos de una tarjeta bancaria, desde hackeos u otras formas de adquisición de datos personales o del código de seguridad (Card Verification Value).

Así, el carding se ejecuta desde dos parámetros; primeramente, los ciberdelincuentes se hacen con los datos de la tarjeta de la víctima. Para ello, suelen implementar el phishing o clonación directa de la tarjeta o de los números de la misma. Seguidamente, con los datos obtenidos, empiezan a generar pequeñas compras en diversos comercios, normalmente, la mayoría de estas compras suelen ser "online" para ocultar la identidad real.

En tanto, resulta loable reconocer aquellos "términos" que se concatenan al acto delictivo (carding), puesto que, estos hechos se suelen realizar por parte de una comunidad de ciberdelincuentes utilizando los parámetros BIN (Bank Identification Number), que son los seis primeros dígitos de la tarjeta bancaria.

Los ciberdelincuentes suelen utilizar una especie de software, que generan combinaciones, puesto que, el carding se identifica por ser un fenómeno criminógeno desarrollado paralelamente al uso de las nuevas tecnologías.

Ante ello, debemos dar cuenta del innegable vinculo del injusto con la utilización de nuevos programas cibernéticos, y en tal sentido, se identifica una modalidad "no presencial" en razón a que estos hechos se cometen a distancia.

Misha Glenny, expone que el acceso masivo a números de cuentas ha superado con grandes distancias al hurto diario de tarjetas de crédito de forma personal. Con este ejemplo se evidencia que la modalidad de Carding puede marcar hito no solo en la seguridad personal, sino que puede ser notable en un porcentaje mayor en las organizaciones que se afectan causando pérdidas millonarias en la economía[4].

Consecuentemente, la ejecución delictual merece "conocimientos técnicos" para la implementación del sistema de envío y recepción de datos. Así, se puede apreciar que la

[4] BBC Mundo. Los secretos del cibercrimen organizado para robar tarjetas de crédito. http://www.bbc.com/mundo/noticias/2014/11/141110_tecnologia_crimen_organizado_cibercrimen_tarjetas_credito_ ig

conducta se enlaza con el objeto material (información de la tarjeta), sumado al despliegue de mecanismos para superar el código de seguridad para concretar el ilícito.

Si bien, este fraude financiero se ejecuta "frecuentemente" mediante el internet, no es la única vía de acción, pues, las llamadas telefónicas también forman parte de un parámetro delictual para hacer caer en el error de otorgar datos precisos sobre la tarjeta.

En la dogmática contemporánea podemos encontrar ciertas vertientes que asumen que el delito de estafa informática debe de ser objeto de análisis vinculado con el delito de estafa tradicional. Para dicho parecer, se infiere en el comportamiento del "engaño" a las personas (víctimas) como sucede en el caso de la estafa tradicional.

Ahora bien, el problema radica en adecuar un equivalente a la acción engañosa (declaración falsa) que causa el error y consecuentemente, la disposición patrimonial (en la actuación que se produce sobre un ordenador). Por tanto, otra línea dogmática expone que la adecuación del delito de "carding" (clonación de tarjetas, obtención de información personal y empresarial, ataques a los proveedores de Internet), ocuparía una construcción bajo los lineamientos del tipo legal de apropiación.

Así, el expansionismo penal advierte una calificación de delitos especiales, respecto al nexo causal de una comisión bajo la impronta de utilización de una tarjeta de crédito/débito. Las nuevas conductas ilícitas de uso fraudulento de instrumentos de pago que hayan sido obtenidas por una apropiación indebida, falsificación o manipulación ocupan el "necesario" control de nuevos verbos rectores.

En tal sentido, la forma de obtención de datos (de la tarjeta) puede generarse de diversas maneras, sea por algoritmos para generar números de tarjetas bancarias, esto, a través de softwares específicos que usan los bineros o través del "shoulder surfing"; es decir, la simple acción de mirar disimuladamente el número de la tarjeta cuando se va a pagar y (en dicho instante) memorizar, al igual que el código de verificación.

Así es que, el delito de carding se subsume en aquella acción desplegada por el sujeto infractor que se ajusta al empleo de manera ilegal del código de tarjetas, para luego, generar compras sin el consentimiento del titular (sujeto pasivo).

Por ello, debemos aseverar que la afectación que produce el carding (delito económico) al sistema financiero, se encuentra ligado a la desvirtuación del bien jurídico

colectivo tutelado del orden económico. Como corolario, debemos interactuar con estas nuevas tendencias de fraudes financieros que buscan un beneficio propio a costa de dañar la economía de terceros, creando una inseguridad financiera dentro del orden económico.

Construcción lineal fraudulenta del Ransomware

La debida regulación del sistema económico integral y la confrontación permanente con los nuevos elementos materiales *actus reus* de infracciones fraudulentas, ante la innegable evolución de los medios informáticos, dan cuenta de la referida criminalidad organizada en la punibilidad objetiva de acciones bajo el espectro del ciberespacio, que pretende lograr la desvirtuación del régimen financiero transaccional, sobre la base del camuflaje del movimiento de capitales. Pero, debemos advertir que, en la actualidad se han incrementado aquellos determinados "ciberdelitos" bajo amenazas a partir de un *ransomware* o secuestro de datos dentro de un sistema informático.

Es que, un sistema informático es "todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento"[5].

En tal sentido, la finanza global se encuentra amenazada ante nuevas tendencias de estafas y sustracciones de fondos, bajo una articulación común (ciberataques). Esto, ocurre a través del gran impacto que se ha comprobado ante la utilización de las denominadas "criptomonedas", que se han transformado en un suceso radical del sistema económico mundial.

Así, las criptomonedas se han vuelto un interesante objeto digital (de especie monetario), que se vincula a las diversas transacciones desde los medios digitales, complementando una nueva forma de pago y/o de intercambio comercial. No obstante, los últimos informes estadísticos han determinado que son altamente volátiles, lo que podría inferir en la inseguridad económica (a falta de mecanismos preventivos idóneos), puesto que, pueden provocar una caída repentina afectando a los usuarios que decidan invertir en dicho elemento económico.

[5] Consejo de Europa. Decisión Marco 2005/222/AI de 24 de febrero de 2005. http://goo.gl/3QNdd

Es que, el método de utilización puede caer en conflicto por alguna avería accidental; al decir, el olvido de la clave de acceso, con lo que se puede acabar en un perjuicio irreversible (tal como ocurriría con la sustracción irregular de dichos objetos digitales).

En dicho contexto, debemos reparar en que la inminente ciberdelincuencia, también ocupa un parámetro de inseguridad para las criptomonedas, pues bien, la sustracción fraudulenta a partir del empleo la minería de criptomonedas maliciosa, nos demuestra la inversión de dispositivos informáticos para la extracción ilícita de dichas monedas digitales.

Por ende, estos actos ilegítimos que se encuentran conectados con la vulneración a los ordenadores, redes, entre otros, nos advierten sobre la actividad de los hackers que ingresan (ilícitamente) a los dispositivos (ajenos), creando algoritmos para conseguir divisas digitales, mediante al acceso indebido a datos que facilitan la adquisición de criptomonedas.

Así, la nueva era digital concibe este tipo de acciones, como los reconocidos "ciberataques", que conforman una serie de amenazas permanentes a las transacciones económicas digitales. Asimismo, estos actos se piensan a raíz de lo que se reconoce como infección de un *malware*, y que se concreta desde diversas modalidades, como el *scam* que sirve para engañar con las famosas "promociones" para solicitar datos precisos.

En tanto, la lista de infecciones *malware* sigue con el reconocido "gusano informático", que se utiliza para afectar a los ordenadores, bloqueando el acceso a las comunicaciones. Igualmente, el *phishing*, que configura una URL falsa para la obtención de datos sensibles, que luego sirven para suplantar la identidad en cuentas digitales.

El *malware* es una expresión ambigua que incluye una amplia lista de programas maliciosos que tienen objetivos variados, que van desde la destrucción de datos alojados en servidores o computadoras personales, pasando por la mera demostración de la vulnerabilidad de los sistemas, hasta el desvío de los servidores DNS con el objeto de redirigir la navegación para la propagación de publicidad, o bien, para introducirse en sistemas de información, a través de la utilización o simulación de datos reales a fin de

hacer creer a la víctima que se está contactando con un usuario real, por ejemplo, una página de una entidad bancaria por Internet u otro servicio de carácter comercial.[6]

Ahora bien, en el caso de las denominadas "Estafas Ponzi", a través de supuestas inversiones que terminaron en engaños, nos ha permitido inferir que, las criptomonedas resultan sumamente ideales para dicho sistema fraudulento, pues, se va optando por atraer a aquellos inversores que buscan aumentar sus beneficios digitales.

En otro tanto, se encuentra el "Pump and dump", medio por el cual los agentes infractores alientan a compras de acciones de empresas de criptomonedas (que no son de renombre), bajo la utilización de informaciones ilusorias.

Ciertamente, los medios para ejecutar ilícitos económicos en el contexto de las criptomonedas van en desarrollo. Por tanto, en la actualidad se puede destacar al sistema de los "intercambios falsos" que se promueve a través del envio de correos electrónicos ante la promesa de acceso o incremento del dinero virtual almacenado en bolsas de criptomonedas, con lo que se capta al usuario que termina invirtiendo una primera cuota, pero, no obtiene ninguna transacción a favor. Consecuentemente, se percibe la amplia gama de aplicaciones impostoras, muy manipuladas para la falsificación de aplicaciones de criptomonedas, lo que ocasiona que el usuario pueda llegar a perder sus datos financieros.

En ocasiones, los comunicados de prensa "falsos" también contribuyen como medio de engaño, puesto que, se puede llegar a inducir al engaño a los periodistas para que refieran una información falsa, y, una vez publicado el comunicado, facilitan los esquemas de pump and dump. Asimismo, hemos destacado que existen casos de *ransomware* a través de móviles u otros dispositivos, puesto que, los ciberdelincuentes manejan esta vía para pedir el rescate de datos a través del pago de criptomonedas.

Por último, se puede inferir en la conducta reconocida como *Fake Wallets*, que es utilizada por los agentes infractores para hacerse pasar por una cartera virtual a partir de una aplicación falsa, utilizando (inclusive) el logo original, así, estos programas logran que los usuarios paguen con criptomonedas, causando un perjuicio patrimonial. Es por ello, que el debido cuidado debe operar bajo mecanismos de control suficientes (programas de

[6] Pardo Albiach, J. Ciberacoso: "cyberbullying", "grooming", redes sociales y otros peligros, en González, Javier (coordinador), en Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet (Valencia, Tirant lo Blanch, 2010), pp. 66 ss.

cumplimientos idóneos) que logren impedir que las criptomonedas sean funcionales al financiamiento de la criminalidad organizada o a la expansión de la inseguridad económica.

El parámetro engañoso del Scam financiero

Debemos subrayar que existen nuevos "mecanismos" indebidos que anhelan consolidar "fraudes" financieros, pues bien, estos resultan a partir de las conductas (técnicas) de agentes que tienen la "intención" de maniobrar toda información y/o dato de índole económico, bajo el propósito (adicional) de lograr obtener beneficios patrimoniales inverosímiles. Ciertamente, todos estos sucesos conllevan (directamente) a un perjuicio monetario en diversas personas que soportan el régimen financiero - económico.

En tanto, estos injustos se tornan visibles (también) en el ámbito societario, ante las diversas acciones intencionadas que acometen contra los estados financieros de terceros para crear el fraude ante lineamientos de falsificación y/o manipulación técnica de registros e identidad contable.

Dicho lo anterior, la actividad irregular conlleva (innegablemente) el sentido subjetivo del "designio" de engañar como postulado del acto fraudulento, mientras que, la irregularidad (propiamente) se traduce en la infracción antijurídica, por contraponerse a las diversas disposiciones legales, administrativas y/o contractuales.

En consecuencia, hemos de mencionar aquel panorama dogmático que la Unión Europea ha distinguido, infiriendo sobre la distinción entre el sentido ontológico de "fraude" y el de "irregularidad", soportando de manera lógica, que la determinación en postura de refutación, radica en el elemento objetivo de "engañar" a un tercero.

Así tenemos que, la configuración (previa) de la percepción de fraude y los "métodos" actuales de manipulación, nos revelan el complejo vértice del *imposter scam* o estafa de impostor, en donde el agente del injusto se hace pasar por otro, estableciendo un híbrido entre el *phishing*, *smishing* o *vishing* y las pirámides de valor.

Ante ello, surge el plan técnico, motivado por lo ilícito, y configurado bajo parámetros de una "estafa". También, determinada bajo la llamada "hoax". Pues bien, esta nueva estrategia fraudulenta se utiliza a menudo para concretar los timos relacionados a inversiones con "criptomonedas" o monedas virtuales.

Así, según Roubini[7], «la industria mundial de servicios financieros viene atravesando una revolución, pero la fuerza motriz no son las aplicaciones sobrevaloradas de bitcóin. Es una revolución creada en base a inteligencia artificial, big data y la "internet de las cosas"».

Igualmente, debemos percibir que la técnica denota un engaño "online"; es decir, a través de medios (técnicos) informáticos, que comúnmente se canaliza en mensajes, simulando la procedencia de "empresas" de reconocimiento. Asimismo, los agentes se ocupan de engañar a las personas que buscan un trabajo legítimo, en tal sentido, lo único que se les solicita realizar, es la "labor" consistente en generar transacciones de dinero con sus propios usuarios financieros, y con ello, se propone (al engañado) un porcentaje en concepto de remuneración. En tanto, también se puede formalizar a través de identidades falsas, sea de personas físicas y/o jurídicas, que solicitan la actualización de la información financiera del sujeto manipulado.

Ahora bien, en el caso de que una empresa sea víctima de un incidente informático, éste afectará a la reputación corporativa que entrañará una pérdida de confianza de los mercados y por ello una reducción de las expectativas y de la confianza de los accionistas[8].

Por lo que, una vez que las personas resulten captadas, estos estafadores (en línea) inician el cometido de apropiarse de los datos, y proceden a imitar la interfaz de sus víctimas, para proceder a emitir transacciones. Ante ello, el sistema internacional ha abordado la protección de los intereses financieros en la lucha contra el fraude en redes.

Conforme a lo antepuesto, "ontológicamente" trasciende el *fraus* o *fraudis* que implica la respectiva acción contraria a la verdad, que termina causando un hecho antijurídico en contra de toda disposición legal (vigente). En tal sentido, la aproximación gnoseológica del fraude (informático) se ejemplifica ante una nueva especie de conducta delictiva a raíz de la evolución del ciberespacio.

[7] Roubini, N. (2018). *Las promesas rotas de blockchain*. https://es.weforum.org/agenda/2018/01/las-promesas-rotas-deblockchain/

[8] Deloitte Advisory, SL. (2013). *Ciberseguridad es su negocio*. https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk complian ce/Deloitte_ES_GRC_Ciberseguridad.pdf

Es así, que, con respecto a la tipología del fraude informático, en atención al referido oficio ilícito del *Scam*, notamos ciertos parámetros rectores que podrían advertirse bajo la naturaleza jurídica de nuestra legislación penal (paraguaya), puesto que, se determinarían en aquellos parámetros que se destacan en el art. 188° modif. por la Ley Nº 4.439/11, al referirse a la "Estafa mediante sistemas informáticos", bajo el modelo de conducta por parte de la persona que, con la "intención" de obtener para sí o para un tercero un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante: 1. Una programación incorrecta; 2. El uso de datos falsos o incompletos; 3. El uso indebido de datos; o, 4. La utilización de otra maniobra no autorizada; y con ello causara un perjuicio al patrimonio de otro, lo que, podría conllevar una sanción de pena privativa de libertad de hasta cinco años o con multa.

Dicho lo anterior, continua (la referida disposición normativa) señalando que, el que preparare un hecho punible señalado anteriormente, mediante la producción, obtención, venta, almacenamiento u otorgamiento a terceros de programas de computación destinados a la realización de tales hechos, será castigado con pena privativa de libertad de hasta tres años o con multa.

Es que, la planeación de los ataques es el primer punto diferencial, ya que los ataques cibernéticos están planeados con mucho tiempo de antelación, mientras que las crisis financieras no están programadas. La complejidad también diferencia los riesgos cibernéticos de los financieros, ya que los primeros forman parte de un sistema altamente complejo, mientras que los segundos son estudiados por especialistas mediante modelos. La intencionalidad de estos ataques es el último punto diferencial. Mientras que las crisis financieras surgen de fallos del mercado, los ciberataques son intencionados y con fines maliciosos que suelen derivar en inestabilidad financiera[9].

Es por ello, que, la regulación penal, va adecuando la tipificación del fraude cibernético como delito, fijando lineamientos de un Derecho Penal Económico, conforme a normas jurídico-penales que protegen todo el orden económico, y ante los nuevos paradigmas de la actual sociedad que responde al fenómeno ilícito de la "cibercriminalidad". Hemos de precisar que, estos nuevos fenómenos delictivos (Scam), implican nuevas modalidades en la comisión de aquellos delitos tradicionales de engaño,

[9] Montoya Moreno, G., Rincón Arteaga, J., Quijano Díaz, A., & Tocaría Díaz, D. (2019, 26 de marzo). Riesgo cibernético y el futuro de la estabilidad financiera. [Edición 1178]. [Figura 3]. https://www.asobancaria.com/wp-content/uploads/semana-economica-edicion-1178.pdf

pero, bajo la utilización desmedida de sistemas o redes informáticas de transmisión e intercambio de datos, cuya complejidad se encuentra enlazada al apoderamiento de la información personal (datos concretos), a modo de administrar las identidades financieras que implican una dimensión de gran interés dogmático bajo el reconocimiento de las estafas informáticas.

Conclusión

Ante un esbozo conclusivo, debemos reconocer que el nivel típico de la delincuencia informática se encuentra conectando con aquellas conductas que buscan desvirtuar el orden económico legal, bajo parámetros de fraude, engaños o inducciones a la comisión de sabotajes contra empresas, corrupción de altos funcionarios, entre otras.

Esto, evidencia la importancia respecto a una ineludible inversión en seguridad económica desde factores de sistemas y/o programas de prevención contra la ciberdelincuencia. En tanto, estos fácticos conducen a niveles probatorios e investigativos de alta complejidad, pues bien, los ciber-ataques pueden crear un gran perjuicio económico a las corporaciones, y con ello, desvirtuar todo un régimen financiero - económico.

Ante ello, el margen del perjuicio a las corporaciones y/o sociedades no se limita a la interrupción de negocios comerciales nacionales e internacionales, sino, también afecta al margen de la seguridad jurídica, en virtud a la pérdida de confianza con razón a potenciales inversores.

Es, por tanto, que el sistema penal nuclear se encuentra invirtiendo en una adecuación normativa/dogmática, ante las diversas acciones que presentan los agentes infractores con respecto al injusto económico con alcance específico en el empleo de nuevas tecnologías, atendiendo a que la globalización económica ha obligado a la política criminal a asumir nuevos retos.

Así, los lineamientos dogmáticos deducen márgenes delincuenciales como el *Phishing* (medio ilícito por el cual se envían correos electrónicos engañosos con apariencia de un mensaje proveniente de un banco u otro organismo, buscando obtener datos comerciales); el *Vishing* (que resulta útil a los estafadores cibernéticos, para solicitar a las potenciales víctimas mediante argumentos engañosos, la revelación de datos personales); el *Smiching* (que es ejecutado a través de mensajes de textos o whatsapps, informándole a la víctima que se hizo acreedor de un (supuesto) premio y un número de teléfono para

comunicarse, y con ello, lograr la ejecución de operaciones fraudulentas); el *Pharming* (consistente en una estafa mediante el ataque a la red y equipos modificando el tráfico a sitios fraudulentos); o todas aquellas que puedan llegar a analizarse en el sentido de la seguridad de los datos, que se encuentran dentro de los parámetros a ser repelidos, atendiendo a las actuales ciber-amenazas.

También, se puede inferir en que dentro de los ciberdelitos podemos encontrar en mayor medida a la estafa. En tal sentido, atinamos a lo que se reconoce como *skimming/clonning* (clonación de tarjetas), método ilícito por medio del cual se utiliza un dispositivo de carácter *skimmer* que sirve para capturar los datos de las tarjetas (crédito y/o débito) desde los cajeros automáticos para la lectura posterior de la banda magnética, y luego, la acción propia de transferencias de datos a una tarjeta en blanco.

En tanto, la seguridad económica precisa congeniar sus programas de cumplimiento al reconocimiento internacional del Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia (Convenio de Budapest). Dicha disposición normativa internacional resultó en un acuerdo para combatir el crimen organizado transnacional, específicamente los delitos informáticos, en el sentido de fortalecer el Estado de Derecho en el ciberespacio.

Así también, debemos recordar que durante la Sesión N°109 del Comité de Ministros del Consejo de Europa, celebrada el 8 de noviembre de 2001, se adoptó el Convenio sobre Ciberdelincuencia, el que fue presentado para su firma en la ciudad de Budapest, con fecha 23 de noviembre de 2001, entrando en vigencia el 1 de julio de 2004. No obstante, el 20 de diciembre de 2017, a través de la Ley 5.994/17, el Paraguay se adhirió oficialmente a la dicha disposición internacional.

Por consiguiente, el sistema normativo empieza a reconocer la necesaria (adecuación) tipificación de conductas delictivas dentro del derecho (positivo) interno, de los siguientes actos: -El acceso deliberado e ilegítimo a la totalidad o una parte de un sistema informático; - La intercepción deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas en un sistema informático; - La comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos; - La obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático; - El abuso de los dispositivos, a través de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: un dispositivo incluido en un programa informático y una

contraseña, con el fin de que sean utilizados para cometer cualquiera de los delitos indicados con anterioridad; y la falsificación informática, el fraude informático, entre otros.

En tal sentido, la amplitud de la seguridad económica y las actividades afectadas dentro del relacionamiento financiero deducen un aumento de los delitos informáticos; es decir, de la ejecución de actos "a distancia" a través del ciberespacio. Pues, es sabido que los delitos económicos tradicionales precisaban de la concurrencia física (en espacio – tiempo) entre la víctima y el sujeto infractor. Sin embargo, con los avances tecnológicos van apareciendo nuevas configuraciones de modelos de conductas que transcienden por otros parámetros del *iter criminis*.

Por ello, en correspondencia a todo lo analizado, debemos dar la razón al sentido de sociedad de riesgo, ante las amenazas del ciberdelito, que son tan complejas e importantes como la globalización económica, pues bien, las filtraciones de datos corporativos e informaciones sobre cuentas bancarias pueden llegar a desestabilizar todo el orden económico y geopolítico mundial.

Referencias bibliográficas

BBC Mundo. Los secretos del cibercrimen organizado para robar tarjetas de crédito. http://www.bbc.com/mundo/noticias/2014/11/141110_tecnologia_crimen_organizado_cibercrimen_tarjetas_credito_ ig

Consejo de Europa. Decisión Marco 2005/222/AI de 24 de febrero de 2005. http://goo.gl/3QNdd

Deloitte Advisory, S. L. (2013). Ciberseguridad es su negocio. https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk compliance/Deloitte_ES_GRC_Ciberseguridad.pdf

Montoya Moreno, G., Rincón Arteaga, J., Quijano Díaz, A., & Tocaría Díaz, D. (2019, 26 de marzo). *Riesgo cibernético y el futuro de la estabilidad financiera*. [Edición 1178]. [Figura 3]. https://www.asobancaria.com/wp-content/uploads/semana-economica-edicion-1178.pdf

Pardo Albiach, J. (2010). *Ciberacoso: "cyberbullying", "grooming", redes sociales y otros peligros*, En González, Javier (coordinador), en Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet (Valencia, Tirant lo Blanch).

Roubini, N. (2018). *Las promesas rotas de blockchain*. https://es.weforum.org/agenda/2018/01/las-promesas-rotas-deblockchain/

Urueña Centeno, F. J. (2015, 16 de enero). *Ciberataques, la mayor amenaza actual*. Instituto Español de Estudios Estratégicos (IEEE) http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

Vásquez Ruano, T. (2002). Aproximación jurídica al spam desde la protección de datos de carácter personal. *Revista de Contratación Electrónica*, 33.