THOMSON REUTERS
CHECKPOINT

Primer caso argentino sobre "apropiación" de criptomonedas

Chomczyk, Andrés
Palazzi, Pablo A.

I. Introducción.— II. Delitos informáticos y criptomonedas.— III. Primera decisión judicial argentina sobre apropiación de criptomonedas.— IV. Conclusiones.

Abstract: El alto valor económico de estos activos los hace atractivos para todo tipo de delitos patrimoniales. Dada su naturaleza digital, las "apropiaciones" de criptomonedas revisten la forma de ataques a los sistemas informáticos de sus tenedores, ya sean empresas o individuos, para lograr tomar el control del sistema y transferir estos bienes digitales a cuentas propias. En esta nota se busca dar un marco teórico a los delitos relacionados con criptomonedas y para ello se analizan los casos más difundidos a nivel internacional, así como un caso argentino reciente.

(*)
(**)

I. Introducción

El surgimiento y difusión de las criptomonedas ha generado nuevas situaciones relacionadas con delitos informáticos. El alto valor económico de estos activos los hace atractivos para todo tipo de delitos patrimoniales. Dada su naturaleza digital, las "apropiaciones" de criptomonedas revisten la forma de ataques a los sistemas informáticos de sus tenedores, ya sean empresas o individuos, para lograr tomar el control del sistema y transferir estos bienes digitales a cuentas propias.

En esta nota buscamos dar un marco teórico a los delitos relacionados con criptomonedas y para ello analizamos los casos más difundidos a nivel internacional, así como un caso argentino reciente.

II. Delitos informáticos y criptomonedas

II.1. Nociones básicas de las criptomonedas

A modo de introducción creemos conveniente analizar brevemente qué son las criptomonedas desde el punto de vista conceptual y legal. En este sentido, y como hemos señalado en otras oportunidades, las criptomonedas son monedas virtuales de emisión descentralizada sin respaldo de ningún gobierno o entidad en particular, basada en la tecnología blockchain (1). La determinación de la naturaleza jurídica de las criptomonedas es de crucial importancia, puesto que ello permite identificar qué figuras penales podrían involucrar criptomonedas y cuáles no.

Las criptomonedas pueden ser consideradas como un subtipo de token, unidad asociada a una blockchain y que es generada conforme las reglas de funcionamiento que están programadas en el software de aquella blockchain. De modo simplificado, podemos definir a una blockchain como una base de datos mantenida a través de una red pública de servidores distribuidos a lo largo del mundo que no confían entre sí para mantener un registro ordenado de movimientos de unidades pero que sí confían en las reglas fijadas por el software que usan para mantener funcionando esta red. Estas unidades que son registradas por una blockchain se conocen con el nombre de token. Para motivar que las personas participen en el mantenimiento de la red pública, el mismo software tiene previsto la asignación de "recompensas" a esas entidades mediante la entrega de nuevas unidades, conforme las reglas de emisión fijadas en el software, así como mediante la entrega de las comisiones que los usuarios de la red pagan para que los movimientos de esas unidades sean registrados en la red.

Si bien no existe una clasificación única sobre qué tipos de token existen, se suele clasificar a estos en tres grandes categorías: (i) tokens de pago, o criptomonedas, que se comportan como medios de pago e intentan imitar el funcionamiento del dinero, como puede ser el bitcoin ; (ii) tokens de utilidad, que son empleados para los servicios asociados a las funcionalidades de una determinada blockchain, como puede ser ether; y (iii) los tokens de valores negociables, los cuales buscan replicar el funcionamiento de los valores negociables en el mundo de las blockchains, como pueden ser las unidades que se reparten en una Initial Coin Offering (ICO) para recolectar fondos y representan una participación en determinado proyecto.

II.2. Naturaleza jurídica de las criptomonedas

Dentro del análisis que estamos realizando, vamos a centrarnos exclusivamente en las criptomonedas o tokens de pago. Sin perjuicio de que se comportan, o lo intentan al menos, como monedas. Ahora bien, estas tienen la particularidad de no ser consideradas como monedas en el sentido jurídico, puesto que no son subsumibles dentro del concepto de moneda nacional previsto en el art. 30 de la Carta Orgánica del Banco Central de la República Argentina (2) (el "BCRA"); así, como tampoco, a la fecha de este artículo, han sido clasificadas como moneda nacional de ningún otro país soberano. La consecuencia directa de ello hace que estas monedas escapen a las normativas del BCRA relacionadas con el mercado único y libre de cambios; y la necesidad de cursar las operaciones de compraventa derivadas.

En consecuencia, debemos encontrar otra categoría jurídica que sea coherente con las características de las criptomonedas. Los tokens en las blockchains son creados y repartidos según los lineamientos fijados en el software que gobierna y hace funcionar tecnológicamente a estas criptomonedas. En este sentido, todos aquellos que quieren ser titulares de criptomonedas deben aceptar estos términos de gobernanza y unirse a la blockchain que se rige por esos términos o bien crear su propia blockchain con sus propias reglas. En cualquiera de los dos casos, las personas que forman parte de la red aceptan que todo lo que suceda en esa blockchain se rija por el código informático, actuando como una suerte de "contrato" que vincula a quienes participan en la red. Por lo tanto, ser titular de criptomonedas implica ser titular de los derechos que la red reconoce a cada persona que posee tokens y que le permiten interactuar en aquella.

El art. 15 del Cód. Civ. y Com. dispone que "las personas son titulares de los derechos individuales sobre los bienes que integran su patrimonio conforme con lo que se establece en este Código". Resulta imposible negar que las criptomonedas tienen un valor patrimonial para aquellos que las poseen y, por lo tanto, forman parte del patrimonio de una persona. Ahora bien, al tener que darles una categoría dentro de ese patrimonio, y teniendo en cuenta el art. 16 del Cód. Civ. y Com., que dispone que "los derechos referidos en el primer párrafo del art. 15 pueden recaer sobre bienes susceptibles de valor económico. Los bienes materiales se llaman cosas", podemos concluir que las criptomonedas pueden ser clasificadas como bienes inmateriales. En concreto, las criptomonedas califican también como una suerte de derechos crediticios que tiene el titular de los tokens y que pueden ser ejercidos contra toda la red que opera la blockchain, para que se permita el ejercicio de los derechos asociados al token en cuestión, los cuales, en líneas generales, suelen conceder la posibilidad de ceder o transferir esa cantidad de tokens a un tercero diferente.

Esta concepción de las criptomonedas es aplicable únicamente cuando es el usuario quien posee las llaves privadas para disponer su disposición. En el caso que el usuario haya asignado los tokens al control de otras llaves privadas, como podría ser el caso en el que el usuario haya entregado sus criptomonedas a una plataforma que haga custodia de estas (una bóveda de criptomonedas, un exchange o un proveedor de soluciones de billetera digital, entre otros), allí el usuario deja de tener una relación directa con la red y pasa a tener dicha conexión con la blockchain por intermedio de un tercero que hace actos en su nombre. En este caso, el usuario únicamente tiene un derecho crediticio frente a la plataforma y, tal como ha sucedido en los casos comentados previamente, puede ocurrir que la plataforma pierda el control de las criptomonedas y sea imposible que esta cumpla con su obligación de entregar las criptomonedas al usuario cuando las demande, incurriendo así en un incumplimiento contractual con el usuario, pasible de ser reclamado judicialmente e indemnizado de forma integral.

Ahora bien, esta visión general desde el Derecho privado puede verse afectada por interpretaciones especiales factibles desde otras ramas del Derecho para determinadas finalidades que pueden ser perseguidas; por ejemplo, en materia de prevención de lavado de activos y financiamiento del terrorismo, podría interpretarse que las criptomonedas son un circulante como cualquier otra moneda nacional y, por ello, sometidas al régimen general previsto para el análisis y revisión de los clientes y operaciones que las involucre. Es decir, cada sector del Derecho podrá tener una diferente visión de lo que es una criptomoneda, como podría ser el bitcoin , en función de los intereses que se pretenden regular.

Para concluir, una criptomoneda es un bien (arts. 15 y 16 del Cód. Civ. y Com.), de carácter patrimonial con soporte inmaterial, creado mediante un sistema informático, de emisión privada y que suele utilizarse como medio de pago o de intercambio.

II.3. Delitos y criptomonedas

Ya vimos que las criptomonedas, desde el punto de vista del Derecho privado, pueden ser calificadas

como bienes y forman parte del patrimonio de una persona. Por lo tanto, dada su naturaleza, son factibles de estar involucradas en los delitos clásicos contra la propiedad previstos en el Código Penal.

Sin embargo, la primera clasificación que debemos estudiar requiere diferenciar a las criptomonedas como objeto del delito o como medio comisivo de otro delito. Una segunda clasificación que debemos tener en cuenta también es quién es la víctima del delito: en este sentido, podemos identificar a las posibles víctimas desde los tenedores individuales de criptomonedas, los intermediarios que ofrecen algún tipo de servicio relacionado a las criptomonedas que implique su custodia e, incluso, al mismo sistema blockchain conformado como los diferentes participantes que ponen su poder computacional al servicio de la red.

Cuando hacemos referencia a las criptomonedas como objeto de delito, nos referimos básicamente a los delitos contra la propiedad.

Así una persona podría acceder en forma no autorizada a la billetera virtual de la víctima e incurrir en el delito de acceso no autorizado (art. 153 bis Cód. Penal), que es un delito contra la propiedad o contra el espacio virtual titularidad de esa persona (3). También podría intentar apoderarse de todo o parte de las criptomonedas allí guardadas mediante su transferencia a una dirección bajo control propio o de un tercero. También podría ingresar a la billetera y cambiar su clave, si es que el acceso estuviera protegido con contraseña, a los fines de excluir al verdadero titular, lo cual sería otra forma de apropiación ilícita de esos bienes. En cambio, si son apropiados, transferidos o retenidos legalmente pero no devueltos a su titular en tiempo y forma legal, se deberá aplicar la norma del Código Penal correspondiente (ej. arts. 162, 172 o 173, Cód. Penal) y podrán ser considerados como cosas a los fines de hurto, o derechos, por estafa y otras defraudaciones.

Cuando hacemos referencia a las criptomonedas como instrumento o medio comisivo de un delito, aparecen infinidad de variantes.

Dado que las criptomonedas funcionan como medio de pago, pueden aparecer implicadas en diferentes delitos en los cuales se involucren valores más clásicos, como las monedas fiduciarias. Existe una idea en el "imaginario popular" que por ser seudónimas, resulta imposible determinar el origen de las criptomonedas o rastrear el camino que hicieron para llegar hasta la persona que las posee en un momento determinado; bueno, la realidad nos demuestra todo lo contrario. Las criptomonedas de blockchains públicas son perfectamente trazables al estar expuestas o ser visibles para el público en general todas las transacciones realizadas (4). Si bien es cierto que la red opera de forma seudónima, puesto que no hay registro en la blockchain sobre la identidad presente detrás de cada dirección pública, es posible combinar esa información con otros datos para asociar direcciones a personas y así reconstruir una cadena de tenencias de criptomonedas. A modo de ejemplo, en el caso de la estafa a Mt. Gox, el cual reseñaremos más adelante, una investigación privada logró encontrar, después de años, dónde fueron las criptomonedas robadas en aquel ataque al exchange japonés (5). Es decir, es viable la realización de una investigación de informática forense para identificar el origen o destino de una criptomoneda.

Los casos más frecuentes de comisión de delitos que involucran a las criptomonedas son los de ransomware. Estas son situaciones de ataques informáticos donde se encriptan todos o parte de los archivos de un ordenador o sistema informático de la entidad atacada, ya sea una persona física o una empresa, y donde el atacante solo desencriptará los archivos a cambio de un pago, generalmente en criptomonedas. Estas situaciones pueden encuadrarse en la figura de daño informático definida por el art. 183, segundo párrafo del Cód. Penal, que dispone: "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños". También resulta aplicable el delito de extorsión previsto en el art. 168 del Cód. Penal, donde se establece que: "Será reprimido con reclusión o prisión de cinco a diez años, el que con intimidación o simulando autoridad pública o falsa orden de la misma, obligue a otro a entregar, enviar, depositar o poner a su disposición o a la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos".

Cabe señalar que existen ciertas modalidades de ransomware donde los archivos no son encriptados, sino simplemente cambiados los permisos de acceso y vista a los archivos; o donde es configurado el software para retransmitir la información del sistema informático a menos que un pago tenga lugar. Algunos ejemplos de estos ataques fueron el WannaCry o el CryptoLocker, los cuales llegaron a causar

estragos en compañías como Telefónica (6). Estos casos son bastantes sencillos de resolver, puesto que la única dificultad radica en, tal como señalamos anteriormente, el seguimiento informático-forense de las criptomonedas involucradas: y desde aquí, particularmente, mediante el rastreo de los fondos entregados por la víctima al victimario a fin de lograr dar con este (7).

En línea con este tipo de ataques informáticos, otra posibilidad que cabe, y sobre la cual ha habido numerosos casos —incluso en Argentina (8)—, es la introducción de malware en otros dispositivos, ya sean ordenadores, tabletas, teléfonos, para hacer que ese dispositivo participe en un esquema de minería sin saberlo: las criptomonedas generadas a partir de la introducción de ese malware van al hacker que infectó el dispositivo, incurriendo en una suerte de "hurto de uso" del tiempo de procesamiento de los sistemas infectados.

Finalmente, y no por ello menos importante, las criptomonedas también han sido empleadas como medio para la comisión de delitos en materia de prevención de lavado de activos y financiamiento del terrorismo (9). Ahora bien, en modo alguno aquí se generan nuevos delitos ni resulta necesario legislar específicamente sobre la materia. Esta cuestión, junto con la determinación de reglas tributarias "claras", ha sido uno de los focos principales de los reguladores en la breve vida de las criptomonedas, principalmente alimentado por ese mito de la anonimidad de las transacciones, lo cual, como mencionamos antes, es solo eso, un mito ya que la realidad nos demuestra la perfecta trazabilidad de las operaciones. Tan así es que una de las primeras regulaciones a nivel internacional fue dictada por la Financial Crimes Enforcement Network, el organismo estadounidense a cargo de dictar y hacer cumplir la normativa a nivel federal en materia de prevención del lavado de activos y financiamiento del terrorismo; dicha normativa era una guía interpretativa (FIN-2013-G001) para identificar qué entidades debían cumplir con las reglas dictadas por ese organismo.

Al día de la fecha, muchos países han avanzado con normas o guías similares a la dictada en el año 2013 por el gobierno estadounidense. Es de destacar que la comprehensión de la tecnología subyacente por el regulador, ya que la Oficina de Control de Activos Extranjeros del Departamento del Tesoro estadounidense ha llegado a poner en una lista negra a direcciones de criptomonedas asociadas con ataques de ransomware (10). Ese no es un detalle menor, puesto que todos aquellos obligados a cumplir con esa orden deberían realizar un due diligence informático para verificar que las criptomonedas que están manipulando no hayan estado involucradas con esas direcciones en cuestión.

En esta línea, las autoridades nacionales de Argentina también han seguido un camino similar, ya que la primera norma que hace referencia, aunque sea de forma indirecta, a las criptomonedas está relacionada a la prevención de lavado de activos y financiamiento del terrorismo. Se trata de la res. 300/2014 de la Unidad de Información Financiera ("UIF"). Esta norma, su art. 2º, define a las "monedas virtuales" como "la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción" (11). El citado artículo agrega que "En este sentido las monedas virtuales se diferencian del dinero electrónico, que es un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción".

La norma citada de la Unidad de Información Financiera impone a ciertos sujetos obligados (12) la adopción de medidas reforzadas de seguimiento de las operaciones realizadas con criptomonedas, así como también el reporte de todas las operaciones en las que aquellas intervengan y se involucren. Este seguimiento reforzado implica una presunción por parte del regulador de que las criptomonedas son elementos que facilitan la comisión de los delitos que se busca prevenir; por ejemplo, podría incluir la revisión de listas internacionales de direcciones de criptomonedas asociadas con células terroristas.

Sin perjuicio de ello, es importante remarcar que estas obligaciones solo son exigibles a quienes están incluidos como sujetos obligados y no son extensibles a quienes no están expresamente señalados como destinatarios de la regulación. En tal sentido, resulta criticable que por medio de una decisión judicial se haga una interpretación analógica y se extienda estas obligaciones a una persona física que no actúe como sujeto obligado para imputar a una persona por lavado de dinero (13).

Finalmente, respecto a los sujetos atacados o afectados se puede diferenciar a los tenedores individuales de criptomonedas, los intermediarios que ofrecen algún tipo de servicio relacionado con las

criptomonedas que implique su custodia, incluso, al mismo sistema blockchain conformado como los diferentes participantes que ponen su poder computacional al servicio de la red.

Los tenedores individuales suelen ser víctimas frecuentes de accesos no autorizados o estafas informáticas. Desde un phishing que le permite al atacante obtener la clave y cuenta de la billetera electrónica donde están almacenadas las criptomonedas, hasta un ataque como el que comentamos en el próximo punto, que permite al atacante tomar el control virtual de un intermediario y transferirse criptomonedas a otra billetera virtual a su nombre.

Los intermediarios que ofrecen servicios suelen ser las víctimas más directas de ataques informáticos. Esto es así por una sencilla razón: son quienes almacenan la información para acceder a posibles transferencias de criptomonedas. Esto fue lo que ocurrió en el caso argentino que comentamos en el punto siguiente: el atacante accedió en forma no autorizada a un exchange y una vez allí logró acceder a los sistemas informáticos de la compañía y cursar transferencias de ether , el token asociado a la blockchain de Ethereum, a cuentas que tenía en otras plataformas.

Por último están los ataques directos a la red blockchain. Cabe aquí hacer una aclaración: dado que las criptomonedas funcionan como sistemas descentralizados, no hay un punto común de control único, sino que el blockchain está distribuido en todos los usuarios de la red. Por lo tanto un ataque al sistema de blockchain implica, al menos, un ataque a un 51% de los usuarios de toda la red: es casi imposible que esto ocurra, dado que es imposible reemplazar o impersonar todos los ordenadores en cuestión localizados en diferentes partes del mundo y conectados a la red. La potencia de cálculo que se requiere es tan alta que ni un gobierno o una empresa podría lograrlo. Asimismo, y en particular con las criptomonedas más tradicionales como el bitcoin, la misma red está en constante estado de alerta y detectando posibles situaciones que puedan sentar las bases para que una entidad controle el "famoso" 51% de esta. A modo de ejemplo, hubo varias situaciones donde pools de minería llegaron a obtener poder considerable de cómputo de la red. Pero en esos casos, los mismos usuarios han tomado cartas en el asunto y transfieren poder de cómputo de ese pool hacia otros o inclusivo a la creación de nuevos grupos de mineros (14).

Si bien esto es poco probable, dada la arquitectura del sistema, un ataque a todo el sistema sólo sería posible si el atacante domina una mayoría de nodos de la red encargados de verificar las transacciones. Ahora bien, supongamos que este "supervillano" existe, y desea atacar exitosamente el sistema de blockchain de bitcoin para alterar alguna transacción. En este supuesto, que es totalmente hipotético, cabe preguntarse: ¿quiénes son las víctimas del delito? Aquí entendemos que podrían darse dos líneas argumentales: (i) por un lado, las afectaciones que sufran aquellas personas que intentaron realizar transacciones y quedaron en una cadena menor; y (ii) por otro lado, las afectaciones que podrían sufrir todos los tenedores de tokens como consecuencia de una bajada de precio motivada por el ataque y la pérdida de confianza en la blockchain en cuestión.

II.4. Primeros casos de robos de criptomonedas

El primer caso conocido de apropiación de criptomonedas que tomó relevancia internacional fue el ataque al exchange japonés denominado "Mt. Gox", el cual involucró una cantidad superior al medio millón de bitcoins equivalente a 368 millones de dólares estadounidenses según la cotización de aquel momento (15). Además de ser el primer caso importante de robo de criptomonedas, la caída de Mt. Gox resultó ser un disparador de reflexiones para toda la industria, ya que mostró la importancia que reviste la ciberseguridad en materia de custodia de criptoactivos, dando lugar a la oferta de soluciones de almacenaje de criptomonedas más robustas, así como también a admitir la necesidad de controles por terceros independientes como firmas de auditoría.

Asimismo, la caída de Mt. Gox mostró al mundo jurídico que las criptomonedas se integran sin problema alguno con el resto del ordenamiento jurídico y el resto de la normativa general es de aplicación. A modo de ejemplo, la quiebra de Mt. Gox fue llevada a cabo siguiendo las normas generales del procedimiento concursal de Japón; en todo caso, este incidente lo único que hizo fue poner de relieve la necesidad de facilitar el acceso a la justicia por parte de los damnificados, ya que Mt. Gox tenía clientes en todas partes del mundo y muchos de estos no pudieron presentar su crédito en sede concursal por no contar con los recursos para acceder a la justicia nipona. Sin embargo esta cuestión excede el presente artículo y corresponde ser analizada desde otras aristas.

Este solo fue uno de los principales hurtos de criptomonedas dentro de una lista mucho más grande y

que sigue creciendo día a día, siguiendo la tendencia general de los ataques informáticos a compañías tecnológicas (16), como puede apreciarse en publicaciones especializadas en la materia (17). Simplemente para poner cifras sobre estos fenómenos, luego del incidente de Mt. Gox, tuvieron lugar los ataques a Coincheck y a Bitfinex, por montos de 534 millones de dólares estadounidenses y 65 millones de dólares estadounidenses, respectivamente. Estos ataques pudieron prosperar por las ineficientes medidas técnicas desplegadas por esas compañías para salvaguardar los fondos de los usuarios y no por la inseguridad de la tecnología subyacente. Es decir, se trata de actividades que podrían haber tenido lugar en otras industrias con efectos equivalentes, si no se adoptaban medidas de seguridad informática como sucedió en estos casos.

III. Primera decisión judicial argentina sobre apropiación de criptomonedas

III.1. Los hechos del caso

El 21 de noviembre de 2018 la sala III de la Cámara Tercera en lo Criminal de la Provincia de Chaco dictó sentencia en el marco de la causa "P., H. M. s/ defraudación informática en concurso real con violación de secretos y de la privacidad", en la cual se dispuso la primera condena por la "apropiación" de criptomonedas en la República Argentina.

Los hechos que motivaron el caso fueron los siguientes. Entre los días 14 de diciembre y 16 de diciembre del 2017, el Sr. H. M. P. realizó un ataque informático al exchange "Mercury Cash", mediante el cual logró acceder a los sistemas de la empresa afectada, mediante una técnica de ataque muy común (18), y tomar su control. Ello le permitió cursar transferencias de ether , la criptomoneda asociada a la blockchain de Ethereum, a cuentas que el condenado mantenía en otras plataformas, para luego descargarlas en una billetera de su titularidad y dominio almacenada en un teléfono celular.

En total el atacante logró transferir fuera del exchange "Mercury Cash" un total de 500 ethers, que a la fecha del hecho delictivo equivalían a la suma de 434.352 dólares.

El atacante fue identificado gracias a las medidas de seguridad informática que mantenía el exchange, que permitió identificar las direcciones IP desde las cuales el atacante ingresó al sistema, así como también gracias a la colaboración entre los exchanges, ya que parte de las primeras direcciones a las cuales se enviaron ethers eran de billeteras de otros exchanges.

III.2. Decisión judicial

En atención a estos hechos, el imputado fue condenado por el delito de defraudación informática en concurso real con violación de secretos y de la privacidad —acceso ilegítimo a sistemas informáticos (art. 173 inc. 16, art. 153 bis 2do supuesto en función del art. 55 del Cód. Penal)—, tras la solicitud de juicio abreviado en la cual admitió su culpabilidad sobre los hechos imputados.

A criterio del tribunal interviniente, el imputado defraudó a los dueños del portal "Mercury Cash" mediante el ataque informático ocasionándoles el perjuicio de perder una suma considerable de ethers.

A su vez, el tribunal consideró que correspondía agravar la pena, puesto que la estafa ha recaído sobre un proveedor de servicios financieros. En atención a todo, el tribunal interviniente dispone la aplicación de una pena de 2 años de prisión de efectivo cumplimiento.

III.3. Nuestro comentario

Estamos de acuerdo con las conclusiones del fallo en cuanto a que condena al imputado por una estafa informática. Las manipulaciones realizadas en el presente caso son las habituales en este tipo penal. En tal sentido, realizó manipulaciones en el sistema del exchange, precisamente una inyección de SQL en la plataforma atacada, lo que le permitió obtener acceso como administrador de sistema al back office del exchange y disponer de la transferencia de una determinada cantidad de ethers de la billetera del exchange (19).

En cuanto a la calificación del delito cometido, creemos que el tribunal adoptó la figura de estafa informática por la amplitud que tiene ese tipo penal para su comisión. En tal sentido, entendemos que el tribunal ha considerado que en este caso se ha configurado una alteración de registros informáticos (20), supuesto que habilita a la aplicación del tipo penal previsto en el art. 173 inc. 16 del Cód. Penal. En concreto, el condenado había ingresado en los sistemas del exchange haciéndose pasar como administrador y disponiendo la transferencia de fondos a los cuales no tenía derecho alguno.

Pasando al análisis de los elementos del delito de estafa, es posible concluir que, efectivamente, la

conducta del atacante ha configurado todos los elementos del tipo penal, a saber: (i) la defraudación; (ii) el ardid informático; (iii) la afectación al normal funcionamiento del sistema informático; y (iv) la disposición o afectación patrimonial. A todo ello debe agregarse que las acciones con ánimo de defraudar deben ser realizadas de forma dolosa.

En primer lugar, el atacante elaboró un ardid para engañar al sistema de back office del exchange para hacerle creer que estaba operando un usuario con privilegios suficientes (una suerte de súper usuario) para disponer transferencias sobre los fondos en la billetera de la compañía mediante el ataque informático acreditado en autos. Con lo cual, además de configurar el segundo elemento del tipo penal, también podemos dar por satisfecho el requisito de una conducta que califique de "defraudar" y se cumpla con el verbo típico necesario. Claramente esto da lugar a que se haya visto afectado el normal funcionamiento de la plataforma, ya que el atacante no era parte del personal de la empresa ni contaba con ningún tipo de autorización que le permitiese realizar la operación que realizó, así como también es probable que durante cierto período la operatoria para el resto de los usuarios se haya visto afectada. Finalmente, con las transferencias a las billeteras del condenado, quedó perfeccionada la disposición patrimonial al salir de la esfera de control del exchange los criptoactivos "robados", ahora bajo el dominio del atacante; tal como mencionamos al principio, estos criptoactivos tienen valor pecuniario y medible en términos dinerarios, permitiendo así la configuración del último elemento.

Un tema que no nos parece menor es la condena del delito de acceso ilegítimo a sistemas informáticos en concurso real con el delito de estafa informática. Dicha figura, prevista en el art. 153 bis del Cód. Penal, presenta el carácter de un tipo penal subsidiario o residual. En este sentido, la doctrina (21) señala que este delito es, en muchos casos, la antesala a otros tipos penales; claramente, para configurar la estafa informática aquí reseñada, el atacante tuvo que obtener un acceso ilegítimo a los sistemas del exchange, con lo cual, una vez que el delito de estafa queda configurado —lo cual tuvo lugar en este caso, ya que el atacante pudo hacerse con casi medio millón de dólares en criptoactivos—, el delito de acceso ilegítimo queda subsumido en la estafa.

Respecto a la prueba informática, nos interesa resaltar la importancia de su valoración en forma adecuada por los tribunales de justicia. En este caso, las pruebas eran varias, pero todas parecen indicar la autoría del condenado. Sin perjuicio de ello, consideramos que los órganos intervinientes durante la etapa de instrucción deberían haber ensayado medidas probatorias propias en lugar de apoyarse exclusivamente sobre las pericias privadas realizadas por el personal del exchange; aquí no está en juicio la seriedad de la evidencia presentada por la víctima, la cual parecería ser coherente y realizada conforme el estado de la técnica, pero la realidad es que se trata de evidencia proporcionada por el querellante sin ningún tipo de control judicial, donde sus resultados podrían haber estado alterados para mostrar una realidad que no era. De la lectura del fallo, parecería que a partir de esta prueba se dispuso el allanamiento y detención del condenado, actividad que dio lugar a su confesión. En razón de ello es importante dejar en claro que, al tratarse de un fallo de primera instancia, cabía la posibilidad de apelarlo por estos motivos. La única pericia judicial practicada en autos fue aquella sobre los elementos secuestrados al condenado con motivo del procedimiento antes indicado. Lo correcto, a nuestro entender, hubiera sido que el contenido de la pericia informática privada hubiera sido reproducido en sede judicial para dotar de validez a los procedimientos practicados. La complejidad técnica de la materia subyacente no puede ser un obstáculo para nuestra infraestructura judicial a la hora de atender las nuevas realidades con las cuales trabaja el cibercrimen.

Otra cuestión también merecedora de ser remarcada es la aparente colaboración entre el exchange afectado y otras plataformas donde el atacante habría movido los ethers en un primer momento. A nuestro criterio, esto responde principalmente a la falta de entendimiento por parte de las autoridades judiciales y de las fuerzas de seguridad de la tecnología subyacente. Los propietarios del exchange Mercury Cash consideraron más oportuno poner en conocimiento del resto de la industria la situación para colaborar en la identificación de las billeteras de destino de los fondos sustraídos indebidamente, que en informar primero a las autoridades gubernamentales para que estas coordinaran las tareas de investigación con el resto del ecosistema. Esto es consecuencia de la tendencia del ecosistema cripto de tender hacia la autorregulación.

Finalmente, el último punto que merece un comentario es la calificación que hace el tribunal de los

sistemas del querellante como servicios financieros para disponer la aplicación del delito agravado previsto en el art. 153 bis del Cód. Penal. En este sentido, parte de la doctrina señala que este concepto de servicios financieros va más allá de las instituciones sometidas a las regulaciones del BCRA y que podrían contemplar a compañías fintech; la razón de ello, a criterio de tal doctrina, radica en que el objeto de tutela penal de la modalidad agravada del delito es la protección de los servicios que están involucrados en la gestión de fondos de terceros, sean parte del sistema financiero tradicional o no. A efectos de interpretar el tipo de servicios comprendidos, consideramos que resulta apropiado seguir el criterio fijado por el BCRA en diversas oportunidades, por el cual se incluye a los actores de la industria fintech dentro del ámbito de control de aquella entidad, aun cuando el BCRA a la fecha ha decidido no aplicarles una normativa específica y simplemente realiza un monitoreo o seguimiento de sus actividades. Entendemos que esta cuestión, por lo tanto, deberá ser resulta caso por caso.

Ahora bien, dado que la empresa atacada era una proveedora de soluciones de custodia y negociación de criptoactivos, debemos analizar si este tipo de actividades está incluido dentro de aquellas que hacen al sistema financiero. Siguiendo el criterio sentado por el BCRA en su comunicado de prensa de 2014 (22), los criptoactivos se encuentran fuera de ámbito de su competencia y, a la fecha, no ha habido ningún tipo de comunicación formal que exprese lo contrario. Con lo cual, creemos que la calificación de "servicio financiero" por parte del tribunal no ha sido acertada y no procedía la aplicación del delito en su modalidad agravada. Si el tribunal pretendía hacer esto, era necesario, como condición previa, que el BCRA cambie su postura al respecto y admita que las criptomonedas forman parte del sistema financiero.

IV. Conclusiones

Las criptomonedas están teniendo impacto en todo tipo de relaciones humanas; los delitos no son la excepción a ello. Si algo tiene valor para una persona, existirá otro individuo que estará interesado en hacerse de ello contra la voluntad del legítimo titular. Asimismo, las criptomonedas, como el efectivo de Internet, también serán usadas de la misma forma en que es usado el dinero fiduciario emitido por los Estados y podría estar involucrado como instrumento en un delito. En cualquier caso, como juristas, debemos estar en condiciones de dar respuestas a estas situaciones preparándonos para ello mediante una acabada comprensión de la tecnología subyacente.

Este caso nos demuestra que es posible lograr recuperar una suma de criptomonedas en el caso de un ataque informático así como también es posible recuperar el dinero físico que es robado de un banco. Claramente por las características técnicas de las redes basadas en tecnología blockchain, el análisis forense para dar con los criminales será diferente, pero ello no es un obstáculo para recuperar los fondos y condenar a los responsables del hecho ilícito. Por lo tanto, tampoco debería ser, como bien ha resuelto el tribunal, un obstáculo el uso de esta tecnología para la resolución jurídica del caso y la condena de los delincuentes. Es por ello que consideramos positivo que la justicia argentina esté en condiciones de hacer frente a estos nuevos desafíos jurisprudenciales al lograr un entendimiento acabado de la realidad tecnológica para resolver este caso y dar una solución a los nuevos hechos jurídicos.

(*) Consultor legal de la Alianza Blockchain Iberoamérica y de Signatura. Es egresado de la Universidad Austral y actualmente esta realizando una maestría en protección de datos en la Universidad de Santiago de Compostela. Es profesor e investigador del CETyS de UdeSA.

(**) Master en Derecho de Fordham University. Es Profesor de Derecho en la Univ. de San Andrés y Director del Programa de Derecho de Interent de la misma Universidad, y codirector del CETYS de UDESA.

(1) Para mayor detalle sobre la naturaleza jurídica de las criptomonedas, recomendamos la lectura de los siguientes artículos: (i) CHOMCZYK, Andrés, "Reflexiones sobre el incipiente marco legal de la industria fintech en Argentina", RDYNT - Revista Derechos y Nuevas Tecnologías, 1, Ed. CDYT, 2017, ps. 51 a 76; y (ii) MORA, Santiago J., "Monedas virtuales. Una primera aproximación al bitcoin", LL 2016-A, 717.

(2) "Art. 30: El Banco es el encargado exclusivo de la emisión de billetes y monedas de la Nación Argentina y ningún otro órgano del gobierno nacional, ni los gobiernos provinciales, ni las municipalidades, bancos u otras autoridades cualesquiera, podrán emitir billetes ni monedas metálicas ni otros instrumentos que fuesen susceptibles de circular como moneda. Se entenderá que son susceptibles de circular como moneda, cualesquiera fueran las condiciones y características de los instrumentos,

cuando: i) El emisor imponga o induzca en forma directa o indirecta su aceptación forzosa para la cancelación de cualquier tipo de obligación; o ii) Se emitan por valores nominales inferiores o iguales a 10 veces el valor del billete de moneda nacional de máxima nominación que se encuentre en circulación".

(3) Sobre la privacidad como un espacio virtual o digital ver PALAZZI, Pablo, "Delitos contra la intimidad informática", Ed. CDYT, 2019, ps. 67 y ss.

(4) Sobre el tema ver FURNEAUX, Nick, "Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence", Wiley, 2018.

(5) WIZSEC, "Breaking open the Mt. Gox case, part 1", 27/07/2017, disponible en https:// blog.wizsec.jp/2017/07/breaking-open-mtgox-1.html.

(6) NATOUR, Lydia, "WannaCry: el ransomware que tiene 'secuestrados' los sistemas de Telefónica y de otras empresas", Diario ABC, 25/09/2017, disponible en https://www.abc.es/ tecnologia/redes/ abci-wannacry-ransomware-tiene-secuestrados-sistemas-telefonica-y-otras-empresas-201705121910_noticia.html.

(7) En tal sentido, recomendamos la lectura de los siguientes artículos sobre la cuestión: (i) HEAVEN, Douglas, "Sitting with the cyber-sleuths who track cryptocurrency criminals", MIT Technology Review, 19/04/2018, disponible en https://www.technologyreview.com/s/ 610807/sitting-with-the-cyber-sleuths-who-track-cryptocurrency-criminals/; y (ii) KIRK, Jeremy, "Ransomware Payments: Where Have All the Bitcoins Gone?", BankInfo Security, 28/03/2018, disponible en https://www.bankinfosecurity.com/ ransomware-where-does-bitcoin-money-go-a-10747.

(8) Cfr. JAIMOVICH, Desireé, "Así se usaron las redes wi-fi de tres locales de Starbucks para generar criptomonedas", Infobae, 16/12/2017, disponible en https://www.infobae.com/tecno/2017/12/16/asi-se-usaron-las-redes-wi-fi-de-tres-locales-de-starbucks-para-generar-criptomonedas/.

(9) VAN WEGBERG, Rolf - OERLEMANS, Jan Jaap - VAN DEVENTER, Oskar, "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin", Journal of Financial Crime, 25(2), 419-435, (2018), disponible en https://doi.org/10.1108/ JFC-11-2016-0067.

(10) Comunicado de prensa de la Oficina de Control de Activos Extranjeros del Departamento del Tesoro de los Estados Unidos de Norteamérica disponible en https://home.treasury.gov/news/ press-releases/ sm556.

(11) Esta definición proviene del informe sobre monedas virtuales —Virtual Currencies Key Definitions and Potential AML/CFT Risks— confeccionado por el Grupo de Acción Financiera Internacional de junio de 2014, el cual se encuentra disponible para su consulta en http://www.fatf-gafi.org/media/fatf/documents/ reports/ Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, consultado el 16 de marzo de 2019.

(12) Los sujetos obligados indicados por la res. 300/2014 de la UIF son los siguientes: (i) las entidades financieras sujetas al régimen de la ley 21.526 y modificatorias; (ii) las entidades sujetas al régimen de la ley 18.924 y modificatorias y las personas físicas o jurídicas autorizadas por el Banco Central de la República Argentina para operar en la compraventa de divisas bajo forma de dinero o de cheques extendidos en divisas o mediante el uso de tarjetas de crédito o pago, o en la transmisión de fondos dentro y fuera del territorio nacional; (iii) las personas físicas o jurídicas que como actividad habitual exploten juegos de azar; (iv) los agentes y sociedades de bolsa, sociedades gerente de fondos comunes de inversión, agentes de mercado abierto electrónico, y todos aquellos intermediarios en la compra, alquiler o préstamo de títulos valores que operen bajo la órbita de bolsas de comercio con o sin mercados adheridos; (v) los agentes intermediarios inscriptos en los mercados de futuros y opciones cualquiera sea su objeto; (vi) las personas físicas o jurídicas dedicadas a la compraventa de obras de arte, antigüedades u otros bienes suntuarios, inversión filatélica o numismática, o a la exportación, importación, elaboración o industrialización de joyas o bienes con metales o piedras preciosas; (vii) las empresas aseguradoras; (viii) las empresas emisoras de cheques de viajero u operadoras de tarjetas de crédito o de compra; (ix) las empresas prestatarias o concesionarias de servicios postales que realicen operaciones de giros de divisas o de traslado de distintos tipos de moneda o billete; (x) los escribanos públicos; (xi) las entidades comprendidas en el art. 9º de la ley 22.315; (xii) todas las personas jurídicas que reciben donaciones o aportes de terceros; (xiii) los agentes o corredores inmobiliarios matriculados y

las sociedades de cualquier tipo que tengan por objeto el corretaje inmobiliario, integradas y/o administradas exclusivamente por agentes o corredores inmobiliarios matriculados; (xiv) las asociaciones mutuales y cooperativas reguladas por las leyes 20.321 y 20.337 respectivamente; (xv) las personas físicas o jurídicas cuya actividad habitual sea la compraventa de automóviles, camiones, motos, ómnibus y micrómnibus, tractores, maquinaria agrícola y vial, naves, yates y similares, aeronaves y aerodinos; (xvi) las personas físicas o jurídicas que actúen como fiduciarios, en cualquier tipo de fideicomiso y las personas físicas o jurídicas titulares de o vinculadas, directa o indirectamente, con cuentas de fideicomisos, fiduciantes y fiduciarios en virtud de contratos de fideicomiso; y (xvii) las personas jurídicas que cumplen funciones de organización y regulación de los deportes profesionales. (ley 26.683, art. 15)

(13) Cfr. https://www.cij.gov.ar/nota-26599-Procesaron-a-diez-imputados-en-el-marco-de-la-causa--Bobinas-Blancas--.html, consultado el 16 de marzo de 2019.

(14) Cfr. FAVIVAR, Cyrus, "Bitcoin pool GHash.io commits to 40% hashrate limit after its 51% breach", ArsTechnica, 16/07/2014, disponible en https://arstechnica.com/information-technology/2014/07/bitcoin-pool-ghash-io-commits-to-40-hashrate-limit-after-its-51-breach/, consultado el 16 de marzo de 2019.

(15) Para mayor detalle sobre el incidente de seguridad sufrido por el exchange Mt. Gox recomendamos consultar los siguientes enlaces: (i) https://medium.com/@jimmysong/mt-gox-hack-technical-explanation-37ea5549f715; y (ii) https://www.wired.com/2014/03/bitcoin-exchange/, ambos consultados el 16 de marzo de 2019.

(16) Para mayor detalle sobre el fenómeno de los incidentes de seguridad recomendamos la lectura de: CHOMCZYK, Andrés - PALAZZI, Pablo A., "La notificación de incidentes de seguridad en el anteproyecto de Ley de Protección de Datos Personales", RLPDP - Revista Latinoamericana de Protección de Datos Personales, 4, Ed. CDYT, Buenos Aires, 2017, ps. 191-210.

(17) Para mayor detalle sobre los principales "robos" de criptomonedas recomendamos consultar los siguientes enlaces: (i) https://www.statista.com/chart/12707/largest-known-crypto-currency-thefts/; y (ii) https://bitcoinexchangeguide.com/top-cryptocurrency-theft-hacks/, ambos consultados el 16 de marzo de 2019.

(18) Se trató de una inyección de SQL en el código de la base de datos del exchange. Esta forma de ataque a sitios web que generalmente usan Java, SQL o PHP consiste en aprovechar fallas en las rutinas de validación de acceso para lograr el acceso a la base de datos de SQL del sitio, y de esa forma acceder a las contraseñas del administrador del sistema. Cabe aclarar que todo acceso no autorizado surge de una falla en el desarrollo de la aplicación o de un error humano. En el primer caso, las vulnerabilidades que permiten una inyección de SQL se originan generalmente en un error en el desarrollo. Por eso muchas empresas que desarrollan software de seguridad implementan un "ciclo de vida" seguro en el desarrollo. Pero es casi imposible llegar a testear todas las opciones posibles antes de lanzar un producto un producto de software. En la práctica la seguridad nunca está 100% garantizada.

(19) En líneas generales, suele hablarse de que los exchanges manejan billeteras "calientes" y "frías", las cuales pueden distinguirse en función de la rapidez con la cual pueden disponerse de los fondos que están asociados a cada una de ellas. Las billeteras "frías" implican la interposición de medidas de seguridad informática que demoran la disposición de los tokens, como podría ser la necesidad de contar con la firma de dos o más personas, esperar cierto tiempo desde que se pretende hacer la transacción, etc. Por otro lado, las billeteras "calientes" implican la inmediata disposición de los fondos que tienen asociados sin la necesidad de superar medidas de seguridad estándar para el tipo de billetera que se trate. Hasta el momento no existen normas definidas sobre los requisitos para la custodia de criptoactivos, incluyendo criptomonedas. Sin perjuicio de ello, quienes ofrecen ese servicio suelen emplear únicamente billeteras "calientes" para almacenar una porción ínfima de todos los fondos custodiados y exclusivamente para atender las necesidades del giro comercial ordinario de la compañía; el resto de los fondos y aquellos que han sido entregados para ser custodiados. En el caso que nos ocupa, parecería que el exchange manejaba todo desde una única billetera, situación propia de un exchange con malas prácticas de seguridad informática o con escaso volumen de transacciones, ambas características de exchanges "jóvenes".

(20) Cfr. PALAZZI, Pablo, "Delitos informáticos", Abeledo-Perrot, Buenos Aires, 2016, 3ª ed., p. 169.

(21) Cfr. PALAZZI, Pablo, "Delitos informáticos", ob. cit., p. 191.

(22) El comunicado original podía ser encontrado en el siguiente enlace: www.bcra.gov.ar/bilmon/bm023000.asp. Actualmente solo es accesible mediante The Wayback Machine.