LA LEY

Acceda **sin cargo** al portal de noticias jurídicas **TRLaLey,** escaneando el siguiente **código QR.**

AÑO LXXXIII Nº 68

TOMO LA LEY 2019-B

**BUENOS AIRES, ARGENTINA -** MIÉRCOLES 10 DE ABRIL DE 2019

**ISSN 0024-1636**

**EDICIÓN ESPECIAL: COMENTARIOS A LA PRIMERA CONDENA POR APROPIACIÓN DE CRIPTOMONEDAS EN ARGENTINA**

# Defraudación informática

**Transferencia de criptomonedas mediante técnicas de manipulación informática. Mala fe y conciencia de ilicitud. Inclusión del inc. 16 al art. 173 del Cód. Penal por la ley 26.388. Violación de secretos y de la privacidad. Derecho a la intimidad informática. Sentencia condenatoria. Prisión efectiva. Ludopatía. Incorporación del imputado a un Programa de Juego Responsable**

**Hechos:** *Se condenó a la pena de dos años de prisión efectiva a una persona que ingresó indebidamente a la cuenta de distintos usuarios de una empresa de criptomonedas y logró transferir a su cuenta más de quinientos activos mediante técnicas de manipulación informática. Asimismo, se ordenó su incorporación a un Programa de Juego Responsable en la provincia del Chaco.*

**1.-** El imputado debe ser condenado a la pena de dos años de prisión efectiva por los delitos de defraudación informática en concurso real con violación de secretos y de la privacidad —acceso ilegítimo a un sistema informático—, en tanto se acreditó que, tras advertir la posibilidad de evadir la seguridad de un sitio *web* de criptomonedas en el procedimiento de transferencias, logró transferir diversos montos de bienes ajenos para su beneficio personal, mediante un proceso no autorizado por la empresa ni por sus legítimos usuarios, obrando de mala fe y con conciencia de ilicitud.

**2.-** El condenado por el delito de defraudación informática debe ser incorporado a un Programa de Juego Responsable —en el caso, en la provincia del Chaco— atento a lo manifestado respecto a su padecimiento de ludopatía y a su consentimiento para realizar el tratamiento; teniendo en cuenta la expectativa de que su aplicación resultará beneficiosa para la vida del imputado y su reinserción familiar y social, tendiente a provocar una reflexión sobre su conducta y respeto de los derechos de terceras personas.

**3.-** La inclusión del inc. 16 al art. 173 del Cód. Penal por la ley 26.388 puso fin a la dificultad para encuadrar como fraude a la acción ilegítima de obtener un crédito o la supresión de un débito, por ejemplo, de un sistema informático al que se accediera mediante una computadora, en el entendimiento de que no había un sujeto engañado, pues el ardid o engaño debían tener como víctima a una persona y su inteligencia.

**4.-** La manipulación informática en sí misma no es típica, pero sí lo será aquella que, además, provoca una alteración en el sistema informático o transmisor de datos de la víctima o de un tercero —art. 173, inc. 16, del Cód. Penal—.

**5.-** La violación de la dignidad de la persona a través de medios informáticos crea un nuevo derecho fundamental denominado indistintamente "libertad informática", "derecho de autodeterminación informativa" o "derecho a la intimidad informática".

**121.816 —** CCrim. Nº 3 Resistencia, 21/11/2018. - P., H. M. s/ defraudación informática en concurso real con violación de secretos y de la privacidad.

**[Cita on line:** AR/JUR/89902/2018]

**2ª Instancia**.- Resistencia, noviembre 21 de 2018.

Antecedentes y consideraciones generales:

Arribó a esta instancia H. M. P., mayor de edad, de profesión comerciante, hoy bajo prisión preventiva, alojado en la Comisaría Segunda Capital. Fue requerido a juicio en la presente causa, en virtud de la pieza acusatoria formulada por el Sr. fiscal de investigación Nº 13, Dr. Lucio Gonzalo Otero —OS Nº 124— acusado penalmente por el delito de "defraudación informática en concurso real con violación de secretos y de la privacidad (acceso ilegítimo a un sistema informático)" (art. 173, inc. 16, art. 153 bis, 2º supuesto, en función del art. 55 del CP).

La convocatoria a resolver estas actuaciones por este procedimiento tuvo su inicio con el acta de acuerdo de juicio abreviado realizada ante el Equipo Fiscal Nº 13 en fecha 13/08/2018, por el imputado en autos H. M. P., habiéndose formalizado mediante el acuerdo entre el Ministerio Público, el imputado y sus defensores, a OS Nº 122.

En la referida acta de acuerdo, consta también que se informó detalladamente al imputado sobre el contenido y los alcances de la normativa, y se lo puso nuevamente en conocimiento del hecho generador de la presente causa, en el modo descripto en la requisitoria de elevación a juicio, acusado H. M. P. de ser el autor de delitos ya mencionados.

He admitido la procedencia de la vía de juicio abreviado respecto del imputado, por decreto de fecha 25/10/2018 —Nº de OS 155—.

Realizada la audiencia *de visu*, conforme se refleja del acta referida, atento a las previsiones del art. 414 del Código, habiéndose cumplido con todas las formalidades exigidas por el rito, el imputado H. M. P., asistido por sus abogados defensores, ratificó la existencia del hecho puesto a su conocimiento en sus circunstancias de tiempo, lugar y modo, admitiendo asimismo su respectiva participación como autor en él, en la forma en que fue redactado en la pieza acusatoria, constando la aceptación del encuadramiento penal, propiciado por el Ministerio Público Fiscal como adecuado a su conducta y su conformidad con la calificación impetrada en la acusación. Asimismo respecto del monto de la pena acordada para H. M. P. —dos (2) años de prisión de cumplimiento efectivo—; de conformidad con lo prescripto en el art. 173, inc. 16, art. 153 bis, 2º su-

# Primer caso argentino sobre "apropiación" de criptomonedas

*Andrés Chomczyk* (*) *y Pablo A. Palazzi* (**)

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

## 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



**NOTA A FALLO**

Primer caso argentino sobre "apropiación" de criptomonedas
*Andrés Chomczyk y Pablo A. Palazzi*..... 1

**JURISPRUDENCIA**

DEFRAUDACIÓN INFORMÁTICA. Transferencia de criptomonedas mediante técnicas de manipulación informática. Mala fe y conciencia de ilicitud. Inclusión del inc. 16 al art. 173 del Código Penal por la Ley 26.388. Violación de secretos y de la privacidad. Derecho a la Intimidad Informática. Sentencia condenatoria. Prisión efectiva. Ludopatía. Incorporación del imputado a un Programa de Juego Responsable (CCrim. Nro. 3, Resistencia)..... 1

puesto, en función del art. 55 del CP, en la forma en que le fue debidamente informado en el acuerdo celebrado y por composición con la pena de la sentencia condenatoria Nº 41, dictada por el Juzgado Correccional Nº 1 de esta ciudad, en fecha 19/05/2017, que le impuso una pena de seis meses de prisión en suspenso.

Seguidamente la sala unipersonal Nº 3 se plantea la siguiente cuestión:

1ª ¿Es cierto el hecho y el acusado su autor en el proceso, hoy en instancia de juicio abreviado? 2ª ¿Qué calificación legal le corresponde por la responsabilidad asumida y la sanción punitiva convenida? 3ª ¿Le cabe la imposición de costas?

Materialidad y autoría: He reseñado el trámite procesal previo que impone la norma adjetiva vigente, basándome en el contexto al cual nos circunscribe esta normativa —específica para esta modalidad de juicio—, por los fundamentos que expondré, coincido con el cuadro fáctico descripto en el requerimiento de elevación a juicio y admitido en el convenio, el que encuentra su aval en los elementos probatorios reunidos en el proceso que dieron base a la requisitoria fiscal de elevación a juicio —conforme OS Nº 124—, y que actualmente constituyen la plataforma que me permite corroborar la congruencia del acuerdo celebrado entre las partes, como asimismo apreciar que se hallan incorporadas válidamente al proceso aquí analizado, y a las que *brevitatis causae* me remito y doy por reproducidos totalmente, todo lo cual valoraré conforme la sana crítica racional. En este sentido, aludo en primer término a las pruebas producidas en esta causa, instrumentales: En expediente policial digitalizado en orden 9 de SIGI: denuncia de M. E. H. de fecha 26/12/2017 (fs. 03/vta.), copia del DNI del denunciante (fs. 04), copia del poder que lo inviste como representante legal (fs. 05/08), informe de Mercury Cash (fs. 09/15), formulario de referencia de queja de Mercury Cash ante el Internet Crime Complaint Center —IC3— del FBI (fs. 16/25); informe de Cablevisión de fs. 27/30, informe de Comisión de fs. 26/12/2017 (fs. 31 y 32 vta.), acta de allanamiento de fs. 38/39, informe del oficial principal de Policía C. E. E. (fs. 41), planilla de antecedentes de H. M. P. (fs. 43), informe de resultado de allanamiento (fs. 47), informe del subcomisario de Policía C. A. R. (fs. 50), informe de Comisión de fecha 28/12/2017 (vuelta de fs. 51); en SIGI: declaración testimonial de M. E. H. de orden 27; acta de allanamiento de fs. 04/05 y vta. de orden 34; informe del cabo de Policía M. J. F.; informe del agte. de Policía R. D. P. de fs. 12/13, orden 34, informe del cabo de Policía C. F. A. de fs. 14, orden 34, (1) soporte DVD-R conteniendo imágenes y videos del allanamiento realizado en Av. Rivadavia Nº ..., fs. 15, orden 34; acta de secuestro y volcado de imágenes y videos de fs. 15, orden 34; informe del cabo de Policía C. F. A. de fs. 20 y 21 orden 34; informe de Cablevisión Fibertel de fs. 27/28, orden 34; acta de secuestro impostergable de fs. 02/03, orden 34; informe de Mercury Cash de orden 47; declaración testimonial y ampliación de M. A. P. B. de orden 64 y 66 respectivamente; acta de Gabinete Científico del Poder Judicial de orden 76; informe pericial Nº 17/2018 del Gabinete Científico del Poder Judicial del orden 115 junto a su respectivo DVD; actas del Gabinete Científico del Poder Judicial; un DVD aportado por el denunciante M. H., con filmación de Lucky Orange.

La materialidad del hecho descripto como la participación punible del imputado en el mismo, ha sido acreditada con: la denuncia de M. E. H. de fecha 26/12/2017 (fs. 03/vta., orden 9 SIGI), quien con copia de DNI (fs. 04) y copia de poder (fs. 05/08), acreditó ser representante de Aventurous Entertainment LLC DBA: Mercury Cash por medio de V. R. (representado). Manifestó M. H. desempeñarse laboralmente como accionista en la empresa Mercury Cash con sede en el Estado de Florida, Estados Unidos, con oficinas en calle ..., 6º piso C, provincia de Buenos Aires. Hace saber que la empresa funciona como un sistema de cartera multi-divisas para criptomonedas, la cual ha sido creada desde cero con la idea principal de convertirla en un lugar de negocios para usuarios que desean comprar, vender o tan sólo enviar o recibir criptomonedas. Dentro de las mismas, una de las criptomonedas con la cual trabajan es la del Ethereum, donde la misma es una plataforma *open source* descentralizada que permite la creación de acuerdos de contratos inteligentes entre pares, basada en el modelo *blockchain*. Tal es así que el motivo de su presentación es en calidad de representante con su respectivo poder, para dar a conocer el delito que sufrió la empresa por parte de un delincuente informático, cuyo accionar ya fue denunciada por el Sr. V. R. (CEO) en las empresas del FBI en Estados Unidos. Por ello hace saber que luego de un arduo trabajo, realizado por la empresa para mejorar la seguridad a nivel de servidor, página *web* y API, notaron un ataque que se generó utilizando tecnología avanzada, la cual traspasaba las capacidades y conocimientos tecnológicos en el funcionamiento actual de la empresa. El resultado al momento del ataque fue el robo de 636,61 Ethereum de su "Cartera Maestra" los cuales al momento del delito tendrían un valor de cuatrocientos treinta y cuatro mil trescientos cincuenta y dos con sesenta y tres dólares (U$D 434.352,63). Por ello hace saber que la empresa cuenta con el uso de programas (Lucky Orange) que permiten llevar el registro en video de todos los movimientos que realiza el usuario desde su computadora al momento en el que manipula la cuenta. Tal es así que poseen registros de imágenes fílmicas que muestran cómo el delincuente informático o el grupo de delincuentes informáticos, primero intentó robar los Ethereum usando viejos métodos de *hacking*, activando las nuevas funciones de seguridad y bloqueando la cuenta en su primer intento. El registro también muestra al delincuente informático tratando de comunicarse con sus equipos y enviando una imagen falsa para la validación de un pasaporte. A causa de esto especulan que esta persona utilizó algún tipo de tecnología de *software* externo para evadir el nivel de seguridad e ingresar de forma "limpia" a sus sistemas, sin dejar rastros de registros y brindando al mismo capacidades avanzadas de programación. Se cree que el *software* externo fue ejecutado durante el ataque, porque durante su último intento, la actividad de clics no era normal y le permitió alterar el código sin bloquear su cuenta. Aclara que esta persona no violó la integridad de los servidores ni modificó archivo alguno, siendo que los mismos están utilizando Centos 7, semanalmente actualizado y CPanel con actualizaciones automáticas, como así también hace saber que usan protección de *software* como Inmunify 360 con escaneo automático de archivos que permite detectar cualquier *malware* para aplicar un cambio de permiso inmediato de 0644 a 0000. Cualquier intento de fuerza bruta a cualquier puerto SQL e inyección *web* desencadena un bloqueo del *firewall* de *software*. El denunciante además hace mención a que en la actualidad el delincuente sigue ingresando a su plataforma, pero con el desconocimiento de que sus acciones están siendo grabadas continuamente. En virtud al modelo que posee el Ethereum (*blockchain*) permite al personal idóneo de la empresa, rastrear casi a donde sea que hayan sido transferidos los mismos. El día 14 de diciembre la empresa Mercury Cash fue pirateada por un usuario bajo el *e-mail* ... usando como dirección IP ... En algunos de los videos se puede observar cómo el usuario ha usado varias direcciones IP de Suiza y Reino Unido para enmascarar su verdadera ubicación. Posterior a este evento, el usuario creó una cuenta con el mismo dominio, esta vez como ... usando la dirección IP ... Durante su sesión el usuario hizo un *request* (el *request* permite el acceso a toda la información que pasa desde el navegador del cliente al servidor) de Ethereum al usuario H. P. (sospechoso) (...com) por un monto de 500 Ethereum, siendo ésta una suma altamente sospechosa y siendo similar el monto a los del ataque, lo que llevó a personal apto de la empresa a revisar los *logs* (registro de actividad de un sistema) de sesión para ese usuario. En esa misma sesión el usuario hizo *logout* (cierre de sesión) y se conectó a la cuenta del sospechoso (...com) para intentar completar su ataque. Al hacer un chequeo en la base de datos, notaron que la cuenta del sospechoso es una cuenta legítima y completamente verificada por la plataforma de la empresa teniendo la documentación física, dirección y número de teléfono real de esta persona. Aclara que se comunicaron al número telefónico que poseen en la base de datos para corroborar así que se trataba de una cuenta legítima, donde en esa

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.

**{ NOTAS }**



**(*)** 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

llamada fueron atendidos por la contestadora y la misma hizo mención del nombre del sospechoso. Luego de esto, verificaron que el sospechoso se conectó a la plataforma desde la IP del atacante siendo la siguiente: ... para lo cual utilizó una plataforma VPN (red privada virtual), la misma que usó el delincuente informático, lo cual permitió hacer un examen cruzado y verificar que en efecto el sospechoso es quien está detrás de este ataque a la plataforma de la empresa. Posteriormente, en fecha 16 de diciembre del corriente año se conectó en su cuenta legítima desde donde trató de hacer una compra por tarjeta de crédito por pesos diez ($ 10) en Ethereum. Por ello se comunicaron con el comerciante que maneja las transacciones de tarjetas de crédito (https://www...com/) y el mismo informó que la tarjeta de la cual hizo la compra es robada. El dicente aclara que las únicas conexiones de la IP ... son las del atacante y del sospechoso, como así también hace saber que el sospechoso se ha conectado desde donde creen sería su lugar de residencia con las siguientes direcciones IP ... y ... Se adjunta a la presente los datos reales correspondientes al delincuente informático, copia del DNI del denunciante, como así también copia del poder que lo inviste como representante legal. Se glosa los datos técnicos de las direcciones IP mencionadas más arriba como así también hace entrega de las imágenes fílmicas donde se observa las acciones llevadas a cabo por el delincuente informático. Funda sospechas en H. M. P., masculino, nacido el 12 de febrero de 1982, 35 años de edad, residente en Argentina, domiciliado en Av. ..., Resistencia, Chaco, DNI Nº ... Agrega que al momento de la denuncia los seiscientos treinta y seis con sesenta y uno Ethereum (ETH 636,61) tendrían un valor aproximado de cuatrocientos noventa mil doscientos treinta y cuatro con veintiséis dólares (U$D 490.234,26).

El informe de Mercury Cash (fs. 09/15, orden 9 SIGI), firmado por V. R. M., CEO de Mercury Cash con sede en ..., Florida da cuenta que se han levantado preocupaciones acerca de un ataque digital (*hackeo*) contra la compañía el pasado 14 de diciembre de 2017. Continúa diciendo: "...Luego de un arduo trabajo mejorando la seguridad a nivel de servidor, página *web* y API, fuimos víctimas de un feroz ataque, usando tecnología avanzada, el cual desafortunadamente traspasaba nuestras capacidades y conocimientos tecnológicos. El resultado fue el robo de 636,61 Ethereum (ETH) de nuestra 'Cartera Maestra' (U$D 434.452,63 al momento del robo). Tenemos registros en video que muestran como 'el *Hacker* o el grupo de *hackers'* (el '*Hacker'*) primero intentó robar los ETH usando viejos métodos de *hackeo*, activando nuestras nuevas funciones de seguridad y bloqueando la cuenta en su primer intento. El registro también muestra a el *Hacker* tratando de comunicarse con nuestro equipo y enviando una imagen falsa para la validación de un pasaporte. Creemos que el *Hacker* utilizó algún tipo de tecnología de *software* externo para *hackear* de forma 'limpia' nuestros sistemas. Sin dejar rastros de registros, evitando todos nuestros sistemas de seguridad y brindando a el *Hacker* capacidades avanzadas de programación. Creemos que el *software* externo fue ejecutado durante el ataque porque, durante su último intento, la actividad de clics no era normal y le permitió alterar el código sin bloquear su cuenta. El *hacker* no violó la integridad de nuestro servidor ni modificó ningún archivo, nuestros servidores están usando Centos 7, semanalmente actualizado y CPanel con actualizaciones automáticas. Ninguno de nuestros operadores, desarrolladores o personal de directores se vio comprometido antes y después de este evento. Usamos protección de *software* como Inmunify 360 con escaneo automático de archivos que permite detectar cualquier *malware* para aplicar un cambio de permito inmediato de 9644 a 0000. Cualquier intento de fuerza bruta a cualquier puerto SQL e inyección *web* desencadena un bloqueo de nuestro *firewall* de *software* que se actualiza con las mejores prácticas sugeridas. El *Hacker* ha continuado ingresando continuamente a nuestra plataforma, pero aparentemente desconoce que usamos programas (Lucky Orange) que nos permite llevar registro en video de todos los movimientos que realiza desde su computadora, lo que nos ha brindado evidencias *de facto* y claves, en el que hemos podido obtener los datos reales y documentos del *Hacker*. Afortunadamente el *blockchain* nos permite rastrear los ETH casi a donde quiere que vayan pero se debe hacer una intervención rápida para bloquear los fondos en todas las plataformas y permitir a los organismos de seguridad identificar al *Hacker* y recuperar el dinero robado a nuestros clientes. Plataformas y billeteras usadas para extraer las criptomonedas. El *Hacker* usó diferentes billeteras externas para extraer los ETH, aparentemente de las siguientes plataformas: Billeteras de Kraken: ...; Billetera de Bitfinex: ... (billetera ya confirmada por oficiales de Bitfinex: ...com). ... Billeteras no identificadas ...

Nota: los nombres de las plataformas son mera suposición y no debe ser tomadas con afirmaciones. Detalle de las acciones del *hacker* durante y luego del ataque. El día 14 de diciembre Mercury Cash fue *hackeado* por un usuario bajo el *e-mail* ... usando ... como dirección IP. En los videos almacenados en la plataforma Lucky Orange podemos ver cómo el usuario ha usado varias direcciones IP de Suiza y Reino Unido para enmascarar su verdadera ubicación. Y en estos mismos videos se puede observar el comportamiento particular de navegación y clics que realiza en nuestra plataforma. Posterior a este evento, el usuario se creó una cuenta con el mismo dominio, esta vez con ... usando la dirección IP ... En el video almacenado en Lucky Orange podemos observar cómo el usuario tiene el mismo comportamiento que el atacante con los clics. Durante su sesión, el usuario hizo un *request* de ETH al usuario H. P. (el sospechoso) (...com) por un monto de '500 ETH' siendo éste un monto altamente sospechoso y siendo similar el monto a los del ataque, los que nos llevó a revisar nuestros *logs* de sesión para ese *user*. En esa misma sesión el usuario hizo *logout* y se conectó a la cuenta de el sospechoso (...com) para intentar completar su ataque. Al hacer chequeo en nuestra base de datos notamos que la cuenta de el sospechoso es una cuenta legítima y completamente verificada por nuestra plataforma, teniendo nosotros en nuestro poder su documentación física, dirección y número de teléfono. Cabe destacar que nosotros tratamos de comunicarnos al número de teléfono que tenemos en nuestra base de datos y pudimos verificar que en efecto es una cuenta legítima. Luego de esto, verificamos que el sospechoso se conectó a nuestra plataforma desde la IP del atacante ... usando una plataforma VPN, la misma que usó el *hacker*, lo cual nos permitió hacer un chequeo cruzado y verificar que en efecto el sospechoso es quien está detrás de este ataque a nuestra plataforma. El sospechoso envió a nuestra base de datos su pasaporte, dirección y número de teléfono, por lo cual pudimos verificar que su identidad y documentación es real (la verificación de teléfono se hizo pero atendió la contestadora en el que menciona su nombre). El 16 de diciembre se conectó en su cuenta legítima desde donde trató de hacer una compra por tarjeta de crédito por $ 10 en ETH. Nos comunicamos con el *merchant* que maneja nuestras transacciones de tarjetas de crédito (https://www...com/) y se nos informó que la tarjeta de la cual hizo la compra es robada. Las únicas conexiones de la IP ... son las del atacante y del sospechoso. El sospechoso se ha conectado desde la que creemos es su lugar de residencia con las siguientes direcciones IP: ... y ...

Datos del *hacker*:

Nombres: H. M. Apellido: P. Sexo: masculino. Fecha de nacimiento: 12 de febrero de 1982. Edad: 35 años. País de residencia: Argentina. Dirección: Av. ... Localidad: Resistencia. Provincia: Chaco. Código Postal: ... Número de teléfono: ... Pasaporte: ...". Consta en el informe una fotografía de la página del pasaporte de H. M. P. en la cual se pueden leer sus datos filiatorios. "...Hemos realizado un chequeo del pasaporte en la agencia de información Thomson Reuters y nuestra investigación determinó que el pasaporte es real. Ponemos a disposición de los organismos de seguridad

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 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.

**{ NOTAS }**

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-goa-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, R. - OERLEMANS, J-J. - VAN DEVENTER, O., "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*.

toda la evidencia que hemos recolectado durante las últimas 72 horas, compuestas por: Videos de las acciones del sospechoso. Intento de pagos con tarjetas de crédito por parte del sospechoso. Evidencia que demuestra que la dirección IP del hogar del sospechoso fue efectivamente utilizada por el *Hacker*. Relaciones e interacciones entre el sospechoso y el *Hacker*. El sospechoso además ha sido acusado en diversas páginas *web* domo un *hacker* que ha robado a muchas personas: https://... Esperamos que esta información sea suficiente para que puedan ubicar al sujeto y tomar acciones judiciales de inmediato, para recuperar los ETH que fueron robados a nuestros clientes...".

Formulario de referencia de queja de Mercury Cash ante el Internet Crime Complaint Center —IC3— del FBI (fs. 16/25) donde V. R., CEO de la firma Mercury Cash consigna los datos de la empresa damnificada, la transacción financiera realizada y realiza la descripción del incidente, la cual sería la misma que la obrante en el informe anteriormente descripto, sólo que en idioma inglés. También aporta datos sobre el sospechoso identificándolo como H. M. P., número de teléfono y dirección IP.

Informe de fs. 27/30, respecto de la dirección IP ... y la dirección IP ... donde se establece que ambas están ubicadas en Resistencia, Chaco y corresponden al proveedor Cablevisión SA.

Informe de comisión del agte. de Policía R. D. P. (fs. 31 y 32/vta.) donde consigna que en base al hecho investigado se dirigió a ..., Resistencia, Chaco y estableció que efectivamente allí vive H. M. P., brindando la descripción de la vivienda situada en la dirección consignada.

Acta de allanamiento de fs. 38/39 ordenado por dec. 6215/2017 del Juzgado de Garantías Nº 4, realizado el 28 de diciembre de 2017 en ..., Resistencia, donde reside H. M. P., quien presente en el lugar hace entrega voluntaria de un teléfono celular marca Samsung Galaxy A7 año 2017, color dorado, pantalla táctil, IMEI Nº ..., Serie Nº ... que se encontraba en uso de M., el cual se coloca en modo avión y se procede al secuestro, siendo colocado en el sobre identificado como Nº 1. Asimismo, el ciudadano S. P. presente en el acto, hace entrega de un teléfono celular marca Samsung, modelo GT-I8190L, color blanco, pantalla táctil, IMEI Nº ..., con funda de silicona de color negro, abonado Nº ... el cual es puesto en modo de avión, secuestrado y colocado en sobre identificado como Nº 3. Se constata que la vivienda posee varios ambientes y uno de ellos es utilizado como sala donde se procede al secuestro de una computadora portátil, color negro, marca Compac Presario CQ, serie Nº ..., la cual se encontraba apagada y se coloca en sobre identificado con el Nº 2. Al consultar a H. M. P. cuál es lugar de residencia, el mismo manifiesta que primeramente hablará con su abogado. Posteriormente se secuestra un *router* color negro, marca Hitro, modelo CGNV2; CM MAC: ..., MTA MAC: ... con su respectivo cargador el cual es colocado en un sobre identificado con el Nº 4. Seguidamente, la principal moradora R. P. de P. exhibe una factura tipo "B" de la empresa Gigared a nombre de S. P., número de cliente ... Se notificó la detención a H. M. P. Se hizo constar que todos los ambientes de la casa se encuentran pintados blanco y las ventanas poseen cortinas color blanco. Una síntesis de los elementos secuestrados se consigna en el informe de resultado de allanamiento (fs. 47).

Informe del oficial principal de Policía C. E. E. (fs. 41) donde el 27 de diciembre de 2017 pone en conocimiento que en la fecha en horas el mediodía al momento de estar llevando allanamiento conforme dec. 6215/2017 extendido por el Juzgado de Garantías Nº 4 a cargo del Dr. Carlos Codina, en el domicilio ..., el ciudadano H. M. P. a viva voz y delante de los presentes comenta que sabía el porqué de la presencia policial en el lugar, manifestando textualmente: "Sí ya sé por qué están acá...". "Los Ethereum los tengo en la billetera que está en mi celular, ahí van a encontrar lo que buscan...". "Hay un tipo que encontró un agujero en la página de Mercury Cash y me paso los datos...". "Yo tengo las cosas con el tema de Ethereum, yo no hice nada un contacto que tengo, que no me acuerdo ahora, pero tengo en el Telegram después se los paso si quieren".

Informe del subcomisario de Policía C. A. R. (fs. 50) donde se consignan los elementos secuestrados y que los mismos fueron remitidos al Gabinete Científico del Poder Judicial por nota Nº 2617-J/17.

Informe de Comisión de fecha 28/12/2017 (vuelta de fs. 51) donde se consigna que la prevención policial realizó un trabajo de campo para determinar el domicilio real de H. M. P., constituyéndose en ..., siendo informados que desde hace dos años a la fecha no reside allí. También se determinó que el mismo residiría en ...

Declaración testimonial de M. E. H. del orden 27 del SIGI quien en sede del Equipo Fiscal manifestó: "...la empresa Mercury Cash con sede en Orlando y Buenos Aires es una minera, lo cual significa que posee un sistema de 200 computadoras que produce Ethereum. Mi hija A. H. es responsable de la empresa en Orlando, a cargo de la administración y la parte comercial; el marido de ella que se llama V. R. es el CEO. Mi función en Buenos Aires y Latinoamérica es conseguirle clientes que compren la criptodivisa. El día 21 de diciembre me llama mi hija por teléfono y me dice que le *hackearon* la cuenta de Argentina y le quitaron 534 Ethereum. Yo quedé sorprendido porque me dijo que era concretamente del Chaco. Llamé a mi cuñado J. L., un contacto que tengo comisario general en la provincia de Buenos Aires y le pregunto si conoce a alguna persona que me pueda guiar en esto. Me dice que me contacte con delitos informáticos de la Policía del Chaco. Yo estaba recién operado y pongo en contacto a la gente de Delitos Informáticos y a mi hija en conferencia. Luego de navidad viajé a Chaco y formulo la denuncia en calle Santiago del Estero, Resistencia, con el poder correspondiente. Comienzan las investigaciones y logran rastrear la IP de esta persona y lo detienen. Esperé el mes de enero y vine sobre fin de mes para contratar un abogado y seguir con las acciones penales correspondientes. De todas maneras se hizo la denuncia en el FBI de Orlando e Interpol está trabajando con el tema, es decir hay varias instituciones que están trabajando. Yo poseo conocimientos medios en informática, y lo que pude conocer es que el que hizo esto realizó una inyección de SQL que permitió modificar la base de datos de la plataforma, permitiendo hacer cualquier operación que él quiera. Se sospecha que haya realizado un *Javascript injection* la cual todos los navegadores permiten visualizar el código fuente y modificar los archivos de manera local —como si hubiera estado en la empresa— en la sesión que está abierta en ese momento y ejecutar las transacciones, es decir que pudo adicionalmente al SQL *injection*, cargar la información dentro de su perfil y realizar las transferencias; se transfirió los Ethereum para él. La criptomoneda está actualmente en poder del autor, probablemente en distintas billeteras. Preguntado si la empresa tiene posibilidad de rastrear los Ethereum. Contesta: sí, está en las billeteras que figuran en el informe que aporté al momento de la denuncia. La empresa sabe que los Ethereum salieron a una billetera virtual, pero luego no se puede saber qué hizo el autor con la moneda, si la cambió, si estaba en un *pendrive* y lo descartó, si compró lo que sea, o si cambió por otra criptomoneda. La criptomoneda tiene un número pero una vez que el autor se apoderó, ya no se puede rastrear lo que hizo con ella. Aclaro que las billeteras pueden estar en un *pendrive*, en un celular, en un disco duro. Estimo que no pudo haber gastado toda esa cantidad de Ethereums porque desde que se detectó hasta que lo detuvieron al autor pasó poco tiempo. Agrego que cuando el autor pretendió seguir estafando a la empresa mediante el uso de tarjeta de crédito robada, en un momento dado, porque ya se sabía que era él, se le pidió una validación para que la empresa le entregue los Ethereum que había ad-

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 e, 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 la misma. 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 incluso a la creación de nuevos grupos mineros **(14)**.

**{ NOTAS }**

**(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", *Ars-Technica*, 16/07/2014, disponible en *https://arstechnica.com/information-technology/2014/07/bitcoin-pool-ghash-*

quirido por ese medio, y él envía una fotografía de él, validándose y pone '*Only for use in Mercury Cash*'. Mi hija personalmente estaba manteniendo comunicación por *mail* o *chat* porque ya estaba alertado Delitos Informáticos del Chaco y lo estaban rastreando y estábamos demorando sus intentos de compra por tratarse de tarjetas robadas. Mi hija le solicitó una validación al sujeto requiriéndole la fotografía que menciono y el mismo día que el sujeto envió esa foto, la gente de Delitos Informáticos del Chaco lo detiene y lo sabemos por la camisa de color verde que tenía en la foto que según la policía, estaba usando al momento de la detención y era la misma. Mi hija le mandó la foto a los de delitos informáticos y denunció todo al FBI y se armó una causa allá. Los abogados de la empresa con sede en Orlando están trabajando para su extradición. Acto seguido se hace lectura en alta voz de la denuncia realizada por el compareciente el 26 de diciembre de 2017 a 09.00 horas en el Departamento de Investigaciones Complejas, ratificando íntegramente su contenido y reconociendo la firma inserta al pie por haber sido puesta de su puño y letra...".

Acta de allanamiento del fs. 04/05 y vta. del orden 34 del SIGI, realizado el día 29 de diciembre de 2017 en ..., donde se secuestró un disco rígido de 1 TB marca Seagate sin: ..., y un *router* marca Cisco con su cargador, oportunidad en la cual el imputado manifestó que no se encontraba la computadora personal de su propiedad que había dejado en su habitación. Consta en el acta que se realizaron tomas fotográficas y videos del lugar. El ingreso se realizó mediante llaves del lugar aportadas por la madre del imputado, R. P., constatándose que las aberturas del inmueble no presentaban signos de violencia y que en el interior había un desorden total.

Informe del cabo de Policía M. J. F. de fs. 10 bis, orden 34 del SIGI, donde hace constar que en oportunidad de realizar allanamiento en ..., en un momento determinado el imputado H. M. P. consultó si el motivo de la presencia policial en el lugar se debía sólo al tema de las criptomonedas, manifestando además que si era por otros motivos de tiempos atrás, él no se dedicaba a esas cosas. Al consultarle a qué hacía referencia aclaró que se refería al tema de las compras con tarjetas robadas, estafas a través de la red internet y temas similares. Hizo saber también que una vez manifestó de manera pública a través de un comentario en un *blog* que "él llevaba a cabo esas acciones delictivas ya que la policía no tenía conocimiento sobre el tema y no hacía nada al respecto", pero que ese comentario no hacía referencia al personal que se encontraba presente en ese momento. Hace constar el cabo de Policía que tiempo atrás en diferentes grupos, *blogs* y demás páginas de internet similares, se generaban múltiples comentarios en contra de H. M. P., donde manifestaban diferentes maneras en las cuales habían sido estafados por el mismo.

Informe del agte. de Policía R. D. P. de fs. 12/13, orden 34 del SIGI, quien hace saber que al realizarse el allanamiento de la morada de P. en ..., Resistencia, al momento de la requisa se pudo constatar que en el dormitorio no se encontraba su computadora de uso personal, la cual según dichos de P., el día anterior estaba situada sobre el escritorio de su dormitorio; también se pudo observar un gran desorden dentro del departamento y se constató que la puerta de acceso no se encontraba forzada en su cerradura ni la ventana, las cuales poseen rejas. A causa de lo manifestado por el morador se consultó a los vecinos del edificio si habían notado movimientos extraños en el departamento de P., donde el vecino que reside en el departamento lindante al del mismo, el cual no quiso brindar sus datos por temor a futuros problemas, manifestó que el día 28/12/2017 observó en horarios entre 21.00 y 23.00 horas, no recordando el horario preciso, a una persona mayor de edad, de unos 75 años aproximadamente, estatura 1,71 metros de alto aproximadamente, de contextura delgada, el mismo traía puesto anteojos de receta, cabello corto, no recordando la vestimenta que poseía en ese momento. Ante estas circunstancias, teniendo en cuenta las características descriptas correspondientes a esa persona, se le exhibió una fotografía extraída del usuario de Facebook M. P., la cual está adjunta al informe y retrata al imputado junto a su madre, padre, hermano e hijos, manifestando el vecino que la persona que observó en el departamento de P. tendría la misma característica que su padre.

Informe del cabo de Policía C. F. A. de fs. 14, orden 34 del SIGI, donde hace constar que el 29 de diciembre de 2017 a 12.20 horas se realizó allanamiento en ..., —ciudad— en compañía del ayudante fiscal Javier García, donde se encontraba presente su principal morador, siendo H. M. P., siendo designado el informante para realizar tomas fotográficas y grabación de video correspondiente al lugar y momento del allanamiento. Posteriormente en el asiento de la División Delitos Tecnológicos A. realizó el volcado de las imágenes y videos digitales en un (1) soporte DVD-R y su correspondiente *hackeo* a fin de incorporarlos a la presente causa, labrando acta de secuestro y volcado de imágenes y videos de fs. 15, orden 34 del SIGI.

Informe del cabo de Policía C. F. A. de fs. 20 y 21 orden 34 del SIGI quien hace constar que habiendo tomado conocimiento de que P. suministró el 29 de diciembre de 2017 una *selfie* —autorretrato o autofotografía— a la empresa Mercury Cash donde se visualiza el rostro y una inscripción en inglés sobre un papel donde versa la leyenda "*Only for use by Mercury Cash december 28th 2017*" incautado como impostergable en el expediente, también hace saber que en dicha fotografía se observa en el fondo una cortina de color azul y que P. vestía en el momento de dicha *selfie* una chomba de color verde y rayas blancas. Conforme lo informado vía electrónica por la empresa Mercury Cash, se informa que H. M. P. al momento de ser allanado el mismo día 28 de diciembre de 2017 en ..., domicilio de sus padres, vestía con la misma chomba anteriormente mencionada, mismo día en horas de la mañana, adjuntándose la fotografía. También se deja constancia que mediante tomas fotográficas realizadas al momento del allanamiento realizado el 29/12/2017 en ..., al requisarse la habitación de H. M. P., aparece la cortina descripta en la fotografía aportada por Mercury Cash vía mensaje a la División Delitos Tecnológicos, como también se observó un desorden en todos los habitáculos del lugar allanado.

Informe de Cablevisión Fibertel de fs. 27/28, orden 34 del SIGI, donde consta que la titularidad del servicio que utilizó las IPs ... y ... en las fechas requeridas, corresponde a H. M. P., servicio instalado en ..., Resistencia, Chaco, teléfono móvil ..., correo electrónico ..., habiéndose utilizado la conexión instalada en dicho domicilio desde la IP ... los días 24 y 25 de agosto de 2017, 04, 05 y 06 de septiembre de 2017 y desde la IP ... los días 12, 13, 14, 15, 16, 17 y 18 de diciembre de 2017.

Acta de secuestro de fs. 02/03, orden 34 del SIGI, donde consta el secuestro impostergable de un trozo de papel escrito con tinta azul, el cual versa "*Only for use by Mercury Cash december 28th 2017*", (1) una libreta tipo cuero, color marrón, con anotaciones varias, (1) un pasaporte color azul oscuro del Mercosur República Argentina, a nombre de H. M. P.; (2) dos tarjetas de la firma OSDE a nombre de P. S. A. y P. L. M.; (1) un documento nacional de identidad a nombre de H. M. P.; (1) una tarjeta de débito Visa BBVA Francés; (1) una tarjeta de crédito Payments Association MasterCard; (1) una tarjeta Visa del Nuevo Banco del Chaco; (1) una tarjeta MasterCard del Nuevo Banco del Chaco; (1) una tarjeta MasterCard del Nuevo Banco del Chaco; (1) una tarjeta Tuya del Nuevo Banco del Chaco; (1) una tarjeta Visa del Nuevo Banco del Chaco; (1) una tarjeta de débito Maestro del Nuevo Banco del Chaco; (1) una tarjeta de débito Debit Card Visa todos a nombre de H. M. P.

Informe de Mercury Cash del orden 47 del SIGI, en el cual M. P. CTO, por sus siglas en

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.

*d. 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

**{ NOTAS }**

*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

inglés "*chief technical officer*", cuyo significado en castellano se traduce como director de tecnología. Un CTO es responsable de gestionar las cuestiones técnicas que una empresa se enfrenta, incluyendo la investigación y desarrollo. Es así que P. realiza un informe técnico del ataque consignando: "...Luego de un arduo trabajo mejorando la seguridad a nivel de servidor, página *web* y API, fuimos víctimas de un feroz ataque, usando tecnología avanzada, el cual desafortunadamente traspasaba nuestras capacidades y conocimientos tecnológicos. El resultado fue el robo de 619,31 Ethereum (ETH) de nuestra 'Cartera Maestra' (USD 434.352,63, al momento del robo). Tenemos registros en video, que muestran cómo el *Hacker* primero intentó robar los ETH usando viejos métodos de *hackeo*, activando nuestras nuevas funciones de seguridad y bloqueando la cuenta en su primer intento. El registro también muestra a el *Hacker* tratando de comunicarse con nuestro equipo y enviando una imagen falsa para la validación de un pasaporte. Creemos que el *Hacker* utilizó algún tipo de tecnología de *software* externo para *hackear* de forma 'limpia' nuestros sistemas, sin dejar rastros de registros, evitando todos nuestros sistemas de seguridad y brindando a el *Hacker* capacidades avanzadas de programación. Creemos que el *software* externo fue ejecutado durante el ataque porque, durante su último intento, la actividad de clics no era normal y le permitió alterar el código sin bloquear su cuenta. El *hacker* no violó la integridad de nuestro servidor ni modificó ningún archivo, nuestros servidores están usando Centos 7, semanalmente actualizados y CPanel con actualizaciones automáticas. Ninguno de nuestros operadores, desarrolladores o personal de directores se vio comprometido antes y después de este evento. Usamos protección de *software* como Inmunify 360 con escaneo automático de archivos que permite detectar cualquier *malware* para aplicar un cambio de permiso inmediato de 0644 a 0000. Cualquier intento de fuerza bruta a cualquier puerto, SQL e inyección *web* desencadena un bloqueo de nuestro *firewall* de *software* que se actualiza con las mejores prácticas sugeridas. El *Hacker* ha continuado ingresando continuamente a nuestra plataforma, pero aparentemente desconoce que usamos un programa (Lucky Orange) que nos permite llevar registro en video de todos los movimientos que realiza desde su computador, lo que nos ha brindado evidencias *de facto* y claves, en el que hemos podido obtenerlos los datos y documentos del *Hacker*. Afortunadamente, el *blockchain* nos permite rastrear los ETH casi a donde quiera que vayan, pero se debe hacer una intervención rápida para bloquear los fondos en todas las plataformas, y permitir a los organismos de seguridad identificar al *Hacker* y recuperar el dinero robado a nuestros clientes. Plataformas y billeteras usadas para extraer las criptomonedas. El *Hacker* usó diferentes billeteras externas para extraer los ETH, aparentemente de las siguientes plataformas: Billeteras de Kraken: ... Billetera de Bitfinex: ... (billetera ya confirmada por oficiales de Bitfinex: ...) Shapeshift: ... Freewailet: ... Billeteras no identificadas: ...1Ca; * Nota: los nombres de las plataformas son mera suposición y no deben ser tomadas como afirmaciones.

Detalle de las acciones del *Hacker* durante y luego del ataque. El día 14 de diciembre Mercury Cash fue *hackeado* por un usuario bajo el *e-mail* ... usando ... como dirección IP. En los videos almacenados en la plataforma Lucky Orange (una plataforma utilizada para monitorear usuarios en tiempo real, es decir podemos ver dónde hacen clic y en qué sección de la página están) podemos ver cómo el usuario ha usado varias direcciones IP de Suiza y Reino Unido para enmascarar su verdadera ubicación. Y en estos mismos videos se puede observar el comportamiento particular de navegación y clics que realiza en nuestra plataforma. Los *wallets* (carteras digitales) externos a Mercury Cash utilizados para transferir los fondos son: ... en el cual fueron transferidos 469,49 ETH; ... en el cual fueron transferidos 33,50 ETH; ... en el cual fueron transferidos 26,00 ETH; ... en el cual fueron transferidos 90,00 ETH. Esto nos da un total de 619,31 ETH. Dentro de estos *wallets* se realizaron múltiples transferencias las cuales podremos definir como un intento de intercambiar los Ether por otras monedas para así ir perdiendo el rastro. Dentro de la investigación logramos contactar con una persona en Rusia que tiene un *website* donde se intercambian monedas digitales, donde él explica que un usuario con *e-mail* ... realizó una solicitud de cambio de ETH (Ethereum) a BTC (Bitcoin) el cual fue procesada el mismo día del ataque informático y se puede consultar en el siguiente enlace ... (Etherscan es donde consultamos las transacciones realizadas en el *blockchain* de Ethereum y es donde logramos realizar la trazabilidad de las transacciones). Una persona administradora de Buy-Bitcoins.pro nos brindó los detalles en un correo electrónico donde nos informa cuándo realizó la transacción y cómo el usuario identificado con el *e-mail* ... consiguió su *website* mediante publicidad en internet. A continuación el correo: ... Este acto fue realizado con la misma dirección IP ... con la cual sospechamos que el mismo usuario H. P. (el sospechoso) a través de una VPN (red privada virtual, la cual se utiliza para hacer que tu conexión de internet tenga otra dirección IP en otro país, ocultando así la real ubicación de tu ordenador) utilizando el *software* navegador TOR (navegador que cuenta con una tecnología la cual permite conectarse a través de 4 o 6 VPNs al mismo tiempo para evitar ser detectado), la conclusión de que H. (el sospechoso) realizó este intercambio es porque en registros posteriores vemos cómo él inicia sesión utilizando la VPN en la cuenta legítima de H. P. (el sospechoso) bajo el correo ... que mencionamos a continuación. Posterior a este evento, el usuario se creó una cuenta ... usando la dirección IP ...

En el video almacenado en Lucy Orange podemos observar cómo el usuario tiene el mismo comportamiento que el atacante con los clics. Durante su sesión, el usuario hizo un *request* (solicitud de monedas que un usuario puede realizar a otro con sólo utilizar el correo electrónico registrado en Mercury Cash) de ETH al usuario H. P. (el sospechoso) (...) por el monto de 500 ETH, siendo éste un monto altamente sospechoso y siendo similar el monto a los del ataque, lo que nos llevó a revisar nuestros *logs* (registros almacenados por cada usuario de cada acción realizada en nuestro *website* con dirección IP) de sesión para ese usuario. En esa misma sesión el usuario hizo *logout* y se conectó a la cuenta del sospe-

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 cri-

**{ NOTAS }**

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", 3ª ed., p. 169.

**(21)** Cfr. PALAZZI, Pablo, "Delitos informáticos", ob.

choso (...) para intentar completar su ataque. Al hacer revisión en nuestra base de datos, notamos que la cuenta del sospechoso es una cuenta legítima y completamente verificada por nuestra plataforma, teniendo nosotros en nuestro poder su documentación física, dirección y número de teléfono. Cabe destacar que nosotros tratamos de comunicarnos al número de teléfono que tenemos en nuestra base de datos y pudimos verificar que en efecto es una cuenta legítima. Luego de esto, verificamos que el sospechoso se conectó a nuestra plataforma desde la IP del atacante ..., usando una plataforma VPN, la misma que uso el *hacker*, lo cual nos permitió hacer un chequeo cruzado y verificar que en efecto, el sospechoso es quien está detrás de este ataque a nuestra plataforma. El sospechoso envió a nuestra base de datos su pasaporte, dirección y número de teléfono por lo cual pudimos verificar que su identidad y documentación es real (la verificación de teléfono se hizo pero atendió la contestadora en el que menciona su nombre). El 16 de diciembre se conectó en su cuenta legítima, desde donde trató de hacer una compra por tarjeta de crédito por $ 10 en ETH. Nos comunicamos con el *merchant* que maneja nuestras transacciones de tarjetas de crédito (...) y se nos informó que la tarjeta de la cual hizo la compra es robada...". Se detallan múltiples transacciones: una realizada sin éxito por H. con una tarjeta MasterCard que termina en ... del Banco Fidelity Information Services Inc., tipo débito MasterCard de negocios en Estados Unidos; una transacción realizada con éxito con H. con una tarjeta MasterCard que termina en ... del Banco Fidelity Information Services Inc. tipo débito MasterCard de negocios en Estados Unidos. El 23 de diciembre realizó otras transacciones por tarjeta de crédito: transacción realizada sin éxito por un monto de $ 53 USD con una tarjeta MasterCard que termina en ... de Banco Santander Río SA MasterCard, Card Level Personal, de Argentina; transacción realizada sin éxito por 53 USD con una tarjeta Visa que termina en ... de Bahamas que según código BIN pertenece al banco First Caribbean International Bank Bahamas LTD Visa Debit Card Level: Classic; transacción realizada con éxito por un monto de 53 USD con tarjeta MasterCard terminada en ... de First Data Cono Sur SRL MasterCard, Crédito Corporativa; otra transacción realizada con éxito por 26,5 USD y otra más realizada con éxito por un monto de 264,98 USD con la última tarjeta terminada en ... Esto levantó una gran cantidad de alertas en nuestro equipo de *compliance* ya que un usuario normalmente no realiza compras seguidas utilizando tarjetas de diferentes países y menos por montos tan variados. Otra alerta que levantó el sistema es que las transacciones fueron realizadas una vez por minuto; esto nos lleva a la sospecha de que el usuario H. P. estaba tanteando los montos que podía procesar con dichas tarjetas. Otra prueba incriminatoria es que H. P. tiene registrada como favorito una cartera digital con el número ... en la cual recibe la cantidad de 25 ETH desde el *wallet* utilizado para recibir la mayoría de los fondos robados durante el ataque informático identificado ... Las únicas conexiones de la IP ... son las del atacante y del sospechoso. El sospechoso se ha conectado desde la que creemos es su lugar de residencia con las siguientes direcciones IP: ... y ... Una investigación fue hecha donde podemos observar, que la dirección IP ... encaja con la dirección IP de la dirección de su hogar...". El informe adjunta datos de P., pasaporte ... Se consigna que el sospechoso además ha sido acusado en diversas páginas *web* como un *hacker* que ha robado a muchas personas: https://... Incluso el mismo da respuestas burlándose de los usuarios que intentan incriminarlo en el robo de criptomonedas...".

Declaración testimonial de M. A. P. B. del orden 64 del SIGI, donde manifestó: "...Soy ingeniero en informática graduado en la Universidad Católica Andrés Bello, de Venezuela, Caracas. Actualmente me desempeño como CTO de Mercury Cash y Mercury Cash es una empresa constituida en Orlando, Florida, los Estados Unidos de América la cual tiene una plataforma de *trading* o de intercambio entre monedas convencionales como el dólar y las criptomonedas, en este caso el Ethereum —ETH—. Significa que somos lo que llamamos actualmente una casa de cambio la cual le permite a personas naturales registrarse para adquirir estos cripto-activos, como se les llama actualmente. Las personas pueden recibir transferencias de otros usuarios u otras compañías que se desempeñan de la misma manera que nosotros, enviar transferencias de la misma manera y a su vez comprar con métodos como una transferencia bancaria o utilizando una tarjeta de crédito. El Ethereum es una moneda virtual que funciona tal cual como funciona el peso argentino o el dólar americano. Tiene un valor en el mercado y este valor varía igual como varía el euro y el dólar gracias a la oferta y la demanda que existe al intercambiarse entre varias monedas y criptomonedas. El Ethereum trabaja en algo llamado *blockchain* que en español sería la 'cadena de bloques' y ésta funciona como un libro contable. Este libro contable que además es público, es decir que cualquier persona que tenga acceso a internet lo puede consultar, nos permite auditar las billeteras virtuales, nos permite saber cuándo una persona que tiene una billetera, envía las monedas a otra persona y después si esta persona que la recibe la envía a otra persona, también podemos ver hacia qué dirección o número de cuenta es enviada. Muchas billeteras están identificadas gracias a un procedimiento que las regulaciones de muchos países como Estados Unidos le exigen a empresas como a nosotros. Esta práctica se llama KYC o '*know your customer*', o 'conoce a tu cliente'. Es una práctica que incluso los bancos que actualmente funcionan en todos los países con monedas físicas como el peso o el dólar utilizan. Esta práctica permite que las instituciones financieras tengan un control de sus usuarios para así auditarlos cada cierto tiempo y poder detectar potenciales anomalías como lo es el lavado de activos, financiación al terrorismo y cualquier cosa que atente contra la seguridad nacional de un país. Seguidamente es preguntado: ¿Cómo se registra un usuario en Mercury Cash? Contesta: una persona natural —persona física— se puede registrar en Mercury Cash utilizando su nombre, correo electrónico y una contraseña de su preferencia. Una vez iniciado el proceso, el usuario recibe un correo electrónico el cual le pide que valide su cuenta de *e-mail* o correo electrónico. Una vez completado ese paso, el usuario puede iniciar sesión y luego de iniciada la sesión, el sistema le obliga a completar un procedimiento llamado TIER 1 o en español, nivel 1 que forma parte del KYC (conoce a tu cliente). El usuario no podrá comprar, vender ni transferir monedas o criptomonedas sin completar ese paso. Me gustaría aclarar que el 14 de diciembre, el día que sucedió el ataque informático, los usuarios podían hacer transferencias —no comprar ni vender— sin completar el proceso de conoce a tu cliente, lo cual más adelante explicaré qué sucedió ese día. Preguntado ¿de qué manera se valida y aprueba un usuario para transferir, comprar y vender criptomonedas en Mercury Cash? Contesta: cuando los usuarios terminan el proceso de registro, hablaba del nivel 1. Este nivel 1 se les solicita en una sección de nuestro sistema llamada Mi Perfil o Configuración, se les solicita completar los datos siguientes: apellido, número de pasaporte en caso de ser extranjero; si es americano se le solicita la licencia de conducir ya que en USA se puede validar una persona con la licencia; se le solicita la dirección de su domicilio, un número de teléfono, ocupación y profesión. También se le solicita el Código Postal en caso de que exista en el país del usuario. Adicionalmente para validar físicamente que esta persona está diciendo la verdad, se le solicitan escaneados su pasaporte o cualquier documento de identificación emitido por un gobierno, extractos bancarios en caso de ser necesario para verificar la dirección de su hogar o cualquier factura de servicio público. Adicionalmente se le solicita una *selfie*, que es una foto que se debe tomar el usuario a sí mismo sosteniendo su pasaporte en una mano y en la otra mano un papel donde el usuario debe escribir con su propia letra 'Para el uso exclusivo de Mercury Cash' en inglés: '*Only for trading in Mercury Cash*' u '*Only for use by Mercury Cash*'. Una vez que recibimos los documentos, la foto y toda la información, un oficial de cumplimiento que es designado por la empresa, se encarga de validar cada uno de estos documentos: los verifica con lo que llamamos la lista OFAC 'Office of Foreign Assets Control' lo que en castellano sería la Oficina de Control de Activos Extranjeros. Esta lista nos permite verificar si el usuario ha actuado ilícitamente haciendo lavado de activos o financiando terrorismo. Esto quiere decir que la OFAC aplica sanciones y estas mismas están basadas en la política exterior y los objetivos para resguardar la seguridad nacional de los Estados Unidos previniendo el uso del sistema financiero para propósitos que van en contra de las buenas políticas o de las buenas costumbres. Adicionalmente utilizamos otro sistema llamado World Check. Este sistema permite junto con el documento de identidad, en este caso el pasaporte es el que más solicitamos, nos permite verificar si esta persona está vinculada con algún grupo terrorista, nos ayuda a identificar si la persona es políticamente expuesta o tiene algún cargo gubernamental, lo cual ayuda al oficial de cumplimiento a tomar una decisión de si debe aprobar dichos documentos o los debe negar. Funciona tal cual como cuando una persona va a abrir una cuenta bancaria: El banco analiza los documentos y al finalizar el estudio decide si abre la cuenta o no. Preguntado cómo realizar una compra, una venta o una transferencia en Mercury Cash, contesta: Una vez que el usuario está validado por el oficial de cumplimiento, el mismo tiene tres métodos para obtener criptomonedas. El primero de ellos que es el más sencillo, es recibir una transferencia ya sea desde un tercero, es decir desde otra plataforma u otro banco de criptomonedas hacia su cuenta en Mercury Cash y podemos comparar este ejemplo con un depósito en efectivo o transferencia que una persona pueda realizar en el primer instante en que abre una cuenta bancaria en cualquier banco del país. Es una recepción de dinero sólo que este dinero se recibe en criptomoneda llamada Ethereum. El segundo método es cuando el usuario que se registra en Mercury Cash realiza una transferencia bancaria desde su banco, ya sea en Argentina o en cualquier lugar del mundo que le permita realizar una 'transferencia por cable' (de internet o de datos) —*wire transfer*— a la cuenta de Mercury Cash en Estados Unidos. Es importante destacar que estas transferencias no tienen nada de especiales, funcionan tal cual como las transferencias locales de un banco a otro en Argentina, solamente que se cambian los pesos argentinos a dólares y el dinero sería recibido en dólares. En muchas ocasiones los usuarios tienen cuentas en Estados Unidos y muchos de ellos prefieren realizar una transferencia doméstica ya que sale mucho más económico que una internacional. Al realizar la notificación de transferencia, Mercury Cash genera un código especial para esa transferencia y el usuario debe utilizar ese código a la hora de realizar el movimiento bancario. De esta manera Mercury Cash reconoce de manera rápida y eficaz que la transferencia le pertenece a dicho usuario. Una vez la transferencia es realizada por el usuario, el oficial de cumplimiento se encarga de validar que los fondos llegaron y fueron depositados en la cuenta de Mercury Cash y al verificar esta información procede a aprobar la liberación de los fondos en dólares americanos dentro de Mercury Cash en algo que nosotros llamamos como la moneda de Estados Unidos: *USD wallet* que comúnmente se puede denominar como una billetera virtual de dólares y funciona de la misma manera que una cuenta bancaria en dólares en Estados Unidos. La única limitante es que solamente se puede utilizar para comprar la criptomoneda dentro de Mercury Cash. Una vez que el usuario tiene sus fondos habilitados, puede tomar la decisión de comprar ya sea un porcentaje del monto o si desea, el monto completo que no puede sobrepasar los quince mil dólares semanales. El tercer método es con una tarjeta de crédito. Una vez la persona realiza la compra con su tarjeta de crédito y nuestro procesador de pago verifica que las tarjetas son válidas y no están en alguna lista negra, autoriza la transacción y el usuario recibe inmediatamente las criptomonedas. Una vez que el usuario tiene sus criptomonedas en su billetera digital, puede hacer tres cosas: la primera es, de manera externa, conversar con algún comercio que le acepte la moneda para adquirir un bien, un activo o un producto o un servicio y el comercio le dirá cuántas monedas tiene que transferirle para recibir el usuario dicho producto o servicio. El usuario debe inscribir como favorito dentro del sistema de Mercury Cash, la dirección o número de cuenta de esta persona o comercio que le esté vendiendo el producto o servicio; es lo mismo que agregar un beneficiario. Una vez registrado va a llegarle un correo al usuario donde manualmente el usuario debe validar o aprobar la aceptación de agregar esa dirección como beneficiario o como favorito dentro de su cuenta de Mercury Cash y una vez validado esa persona o usuario de Mercury Cash puede enviar las criptomonedas al comercio o al usuario que se las acepte. Cabe destacar que en el mundo se han transaccionado de esta manera, compra y venta de todo tipo de productos y servicios dentro del marco legal, ya que después de venderlas, se debe proceder al registro o a la facturación de los mismos en moneda local, según las regulaciones de cada país. El segundo método de venta es que las personas pueden dentro de Mercury Cash, vender sus criptomonedas a nosotros —Mercury Cash—. Simplemente se revierte el proceso de compra: recibimos las criptomonedas y colocamos el balance en dólares en su cuenta de Mer-

terio 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.

**Cita on line:** AR/DOC/833/2019

**{ NOTAS }**

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*.

cury Cash y el usuario puede decidir si dejarlos en dólares en Mercury Cash o solicitar una transferencia de salida de esos dólares en su cuenta bancaria, ya sea en Estados Unidos o en el extranjero. Preguntado: cómo un usuario puede transferir criptomonedas. Contesta: antes del ataque informático como mencioné anteriormente, los usuarios podían transferir criptomonedas de manera inmediata, sin pasar por el proceso de conoce a tu cliente. Sin embargo, a raíz de los eventos sucedidos el 14 de diciembre y otras anomalías detectadas, decidimos cambiar la regla y solicitamos ahora a todos los usuarios realizar la validación de su cuenta. Esto incluye agregar beneficiarios y transferir criptomonedas. Preguntado cómo funciona el monitoreo de Mercury Cash, contesta: La empresa tiene dos niveles de monitoreo, de los cuales uno de ellos funciona de manera automática por un proveedor externo al cual le pagamos, llamado Lucky Orange, el cual es un proveedor completamente externo o un tercero, al cual le pagamos por sus servicios. Este proveedor nos ayuda a conocer las reacciones de nuestro cliente dentro de nuestra plataforma, permitiéndonos ver grabaciones de hasta un año de antigüedad y sesiones en vivo, es decir, si el usuario está en estos momentos a Mercury Cash, yo puedo ver en vivo y en directo qué está haciendo el usuario, sin ver su información confidencial, solamente veo su comportamiento. Obviamente esta herramienta nos sirve para estudiar anomalías o usuarios que realizan comportamientos inadecuados o sospechosos dentro de nuestra plataforma. Cabe destacar que esta plataforma debe ser manejada por una persona, en este caso un oficial de cumplimiento que conoce o tiene los conocimientos necesarios dentro de las regulaciones legales, parte del conocimiento técnico y la capacidad para estudiar a los usuarios. Nos permite ver cuál es el dispositivo o el tipo de dispositivo desde el cual se está conectando, ya sea un computador, ya sea un celular o un teléfono móvil o una tableta. Adicionalmente a este sistema, el propio sistema de Mercury Cash tiene una plataforma o metodología para registrar tanto los movimientos de los clientes, es decir cuándo inicia sesión, desde qué dirección IP inicia sesión, desde qué dispositivo móvil o dispositivo físico inicia sesión, cuántas veces al día con hora y fecha. Adicionalmente si se descarga la *app* —aplicación— de Mercury Cash ya sea para Android o IPhone, nos permite identificar la versión de la aplicación que está utilizando. Cada día vamos mejorando nuestra aplicación y cada día sacamos una versión nueva. Hoy puede ser la versión 1.0, mañana la 1.2 y pasado la versión 1.3. Es importante explicar qué es una dirección IP. Todas las computadoras o todos los dispositivos móviles tienen lo que llamamos hoy en día un adaptador de red, ya sea inalámbrico o por cable. El concepto de IP que inglés significa *internet protocol* —protocolo de internet— se compone de cuatro combinaciones de números. Por ejemplo ... Este número es un identificador único en el mundo, en conjunto con la hora y con la fecha puede ser utilizado por las autoridades para saber el lugar de origen de una conexión o una aproximación. Nuestro sistema guarda estos registros de direcciones IP de cada dispositivo que un usuario utiliza para conectarse a su cuenta de Mercury Cash. Preguntado cómo se vinculó a H. M. P. con el delito informático contesta: Voy a definir una serie de ítems que vamos a utilizar. El primero de ellos es el nombre D. A éste le vamos a llamar *hacker*/cuenta principal que extrajo de manera satisfactoria el Ethereum de los clientes existentes con balances reales de Mercury Cash a billeteras externas a nuestra plataforma. Esta cuenta —D.— se conectó el 14 de diciembre a Mercury Cash desde lo que sospechamos que fue un acceso VPN con la dirección IP ... la cual es proveniente del Reino Unido. La persona que nosotros entendemos es H. realiza una inyección SQL. Ello significa que el usuario consigue una vulnerabilidad en nuestra base de datos logrando cargar de manera exitosa en el perfil de D. cada una de las cuentas de los usuarios registrados en Mercury Cash y comenzando a hacer las transferencias a tres direcciones externas. Entonces voy a nombrar la billetera 1 que termina en '...' donde hace múltiples transferencias hasta completar un monto de 469,49 monedas. Posteriormente se transfieren 26 monedas a la billetera número 5 que termina en '...'. Esta billetera, después de una investigación y de un reporte técnico enviado a la Fiscalía, se encuentra registrada dentro de los favoritos de la cuenta de Mercury Cash de H. M. P. y por esto es que consideramos una vinculación con los balances transferidos, ya que nuestra incógnita es la siguiente: por qué H. tiene una billetera digital en sus favoritos que recibe Ethereum de lo que llamamos la billetera número 1, la cual recibió 469,49 monedas el día del ataque (14 de diciembre) y estos 26 Ethereum fueron recibidos en esta billetera número 5, el día 15 de diciembre, es decir un día después del ataque. Procedemos a lo que llamamos una vinculación por múltiples inicios de sesión con la misma IP que la cuenta que utilizó el atacante. El día 14 de diciembre, luego de la extracción de todas las criptomonedas de la plataforma de Mercury Cash, un usuario con nombre A. se registra en la plataforma utilizando la misma dirección IP del Reino Unido la cual identificamos con la numeración ... Ese usuario A. únicamente inició sesión el día 14 de diciembre desde la misma dirección IP del usuario D. El 15 de diciembre la cuenta A. inicia sesión con la IP de Suiza identificada como ... El usuario que manipulaba la cuenta A. intenta replicar el ataque realizado el día anterior utilizando los mismos mecanismos. Al no poder realizarlo satisfactoriamente, intenta utilizar una funcionalidad dentro de Mercury Cash que se llama solicitud o *request* a la cuenta de H. M. P. por 500 Ethereum. Al finalizar el *request* el usuario cierra sesión de la cuenta de A. y luego inicia sesión en la cuenta de H. con la dirección IP de Suiza que describí y es aquí donde finalmente logramos vincular a H. con las cuentas que nos atacaron y comenzamos nuestra investigación técnica y los oficiales de cumplimiento su investigación de ingeniería social respecto del usuario. De esta manera hacemos la conexión entre H. y las cuentas D. y A. donde nosotros sospechamos que existe un grado de culpabilidad y es por ello que acudimos a las autoridades para que se proceda a la investigación. En conclusión, podemos afirmar que la cuenta D. y el usuario detrás de ella nos atacó desde la IP de Reino Unido y sólo nombrando el caso más grande, transfirió 469,49 ETH a la billetera terminada en '...'. Luego esa misma billetera envía 25 ETH a la billetera o cartera digital '...' que fue validada por H. vía *e-mail* el 15 de diciembre. La cuenta de A. inició sesión el 14 de diciembre con la IP de Reino Unido que es la misma que usó D. y al día siguiente A. y H. inician sesión con la IP de Suiza, vinculándose así las tres cuentas, ya que físicamente es imposible que una persona esté en tres lugares distintos en tan corto tiempo y es por eso que sospechamos que utilizó una VPN para así engañar la ubicación real donde se encontraba conectado. Las cuentas de A. y D. no pasaron por el proceso de conoce tu cliente a raíz de que antes de la fecha del ataque, sólo se solicitaba la validación para la compra y la venta de ETH, mas no para la transferencia, por lo tanto no tenemos cómo verificar la propiedad de estas cuentas. Sin embargo, existe vinculación directa entre estas cuentas y H., por lo ya explicado. Preguntado para que explique qué es una VPN, contesta: Una VPN es una *virtual private network* o red privada virtual nos permite generar un túnel entre nuestra conexión de internet y un servidor que está conectado físicamente en otro país o ubicación geográfica a una conexión de internet, permitiéndonos así utilizar la dirección IP de ese país y de ese país y de ese servidor para enmascarar la nuestra. Para poner un ejemplo, es como ir a una fiesta de disfraces ocultando la verdadera identidad. Las personas que lo conozcan tendrán dificultades para saber que es usted. Preguntado en qué consiste la inyección SQL que menciona utilizó el imputado, contesta: Ello es algo ilegal porque se trata de vulnerar un acceso a un servidor para leer una información confidencial o modificar datos dentro de la base de datos, sin autorización del administrador del sistema. SQL es un lenguaje que se utiliza para crear bases de datos en sistemas informáticos. Las bases de datos almacenan información. Es lo mismo que cuando dentro de una oficina administrativa existe una caja fuerte que tiene información confidencial que solamente puede ser vista por las personas autorizadas que poseen la combinación para abrir la caja. Si alguien descubre esa combinación y lee, modifica, hurta o incluso destruye es considerada una violación a la seguridad de dicha información. En la informática, este tipo de ataques son utilizados para modificar datos de nuestros servidores y es particularmente notorio porque no forma parte de la sintaxis normal. Un ejemplo utilizando el español como lenguaje, es que imaginemos que una persona lee un discurso en este lenguaje y de repente en la mitad del mismo aparecen letras en otro idioma. Es allí donde nos damos cuenta que algo sucede con nuestro discurso y nos percatamos de un comportamiento inadecuado. Esto mismo sucedió con nuestra base de datos y por ende descubrimos que estas tres cuentas estuvieron involucradas en el ataque informático del 14 de diciembre. El atacante insertó variables utilizando una herramienta que los navegadores *web* traen llamada inspector de elementos. Este inspector le permite modificar ciertos parámetros del sitio *web* y al haber una vulnerabilidad que el atacante detectó, logra insertar una codificación que le permite accionar dentro de nuestra base de datos, dándole la posibilidad de transferir de manera rápida y sencilla los fondos de nuestros usuarios. Esta funcionalidad no está permitida dentro de nuestra plataforma y es considerada un *hackeo*. Preguntado para que diga qué dominios *web* utilizó H. M. P., contesta: ... El utilizó esos dominios para registrar las cuentas de D., A. y H. El correo ... fue utilizado para intercambiar ETH por Bitcoins a un *exchange*, una empresa similar a Mercury Cash de origen ruso que nos envió el correo electrónico con toda la información de la transacción. Hago constar que el monto exacto de lo sustraído a las cuentas de clientes de Mercury Cash es de 619,31 Ethereum —ETH—...".

Ampliación de declaración testimonial de M. A. P. B. del orden 66 del SIGI, donde fue preguntado qué operatorias realizó H. M. P. con tarjetas de crédito con la empresa Mercury Cash, contesta: "...el día 16 de diciembre de 2017 H. intentó realizar desde su cuenta verificada y legítima, una compra con tarjeta de crédito por el monto de diez dólares equivalentes en Ethereum —ETH—. Esta transacción fue aprobada y la misma es una MasterCard de Estados Unidos que termina en ... del Banco Fidelity Information Services, la cual es una tarjeta de negocios, es decir de una empresa, de Estados Unidos. En todos los bancos hay un BIN —*bank identification number*— o número de identificación bancaria que tiene cada banco a nivel mundial y al consultar ese número dentro de las plataformas que el sistema financiero nos permite, logramos identificar la información allí mencionada. La tarjeta estaba reportada como robada, sin embargo la misma pudo realizar una transacción de diez dólares exitosamente. Nuestro procesador de pago que lleva como nombre Paydo nos reportó vía telefónica que la tarjeta se encontraba en una lista negra. Luego de eso se intentó procesar con la misma tarjeta, una transacción por U$S 986,45 la cual fue declinada con el error transacción no permitida. Luego H. intenta hacer el 23 de diciembre otras transacciones comenzando por una tarjeta de Argentina que termina en ... del Banco Santander Río SA, tipo MasterCard, una tarjeta personal; no contamos con la información del titular, ello por el monto de U$D la cual fue rechazada con el mismo error de transacción no permitida. Ese mismo día, H. intenta realizar dos transacciones con una tarjeta Visa que termina en ... de las Bahamas del Banco First Caribbean International Bank por los montos de 53 y 37,09 dólares, ambas fueron rechazadas. Este error fue diferente, porque el error que nos indicaba era que el monto excedía el crédito permitido en la tarjeta, lo cual nos lleva a creer firmemente que H. estaba utilizando tarjetas robadas ya que cualquier persona que tenga una tarjeta de crédito sabe cuál es su límite de crédito y cómo maneja los montos en la misma y que también se nos hace imposible por el tipo perfil que analizó nuestro oficial de cumplimiento que H. pueda tener tarjetas en Estados Unidos y Bahamas. En la banca existen muchas vulnerabilidades dentro de cada institución. En muchas ocasiones las bases de datos de los bancos son vulneradas y por ello reportan que se les darán tarjetas nuevas a los tarjeta-habientes. Muchas veces esos datos correspondientes a las tarjetas se venden en lo que se llama *dark web*, la *web* oscura, que para poder entrar a ella debes utilizar el navegador Tor, ya que es el único navegador que permite entrar de manera anónima a los dominios *.onion* —punto onion—, es así como una persona puede obtener datos de una tarjeta de crédito que no es suya, no siendo necesario poseer el plástico de la tarjeta. También dentro de la *dark web* hay personas que roban o clonan los plásticos y los envían a cualquier parte del mundo. También en fecha 23 de diciembre de 2017 H. hizo dos transacciones con una tarjeta MasterCard Crédito Corporativa que pertenece al First Data Conosur SRL por 53 y 158,99 dólares con la terminación 6188 tipo MasterCard. Es importante destacar que cuando un usuario está realizando compras por tarjeta de crédito conoce el monto exacto que va a comprar, no comienza a probar de a diez, 50, 30 o montos diferentes, lo cual nos indica que el usuario está utilizando tarjetas que no son de su propiedad y por ende nos llevó a realizar el bloqueo preventivo de estos fondos. Fuimos comunicándonos con el señor H. vía *chat* donde se le solicitaron los plásticos, fotos de todas las tarjetas que nombré por delante, por detrás de cada uno junto a su identificación, lo cual sólo recibimos la identificación y la fotografía que está adjunta en el expediente donde él sostiene su identificación y el papel donde escribió *Only for use by Mercury Cash*. Respecto de las demás tarjetas nunca hizo comentarios a pesar de que fuimos insistentes. El sólo nos amenazaba con hacer público este hecho para desprestigiar nuestra empresa, comentando que éramos fraudulentos y que nos estábamos robando su dinero. Me gustaría destacar que la empresa que nos suministra el servicio de *chat* es un tercero 'Kayaco' a quien le pagamos, pudiendo corroborarse con ellos cualquier información necesaria. Todos los registros del *chat* están guardados en los servidores de Kayaco, lo que nos impide modificarlos y solamente el administrador de sistema puede borrarlos, es decir el Sr. V. R., el presidente de la compañía. Cabe resaltar que resulta sumamente necesario que se arbitren los medios a fin de que se consiga la manera de accesar a cada uno de los dominios la cual controla la creación de cada uno de estos correos y en el caso de *hush.com*, contactar a esta empresa para solicitar la información o el acceso a la cuenta vía judicial ya que pasadas tres semanas la cuenta es suspendida y no es posible accesar a menos que se realice un pago en dólares por el mantenimiento de la cuenta. Los dominios, como recalcamos anteriormente son ... y ...; las cuentas de correo son ... Para el caso de ... necesitamos autorización de la Fiscalía para realizar el pago de mantenimiento de la cuenta y evitar que la empresa borre dicha cuenta. En el caso de las demás, solicitamos a la Fiscalía contactar al proveedor registrante de dominios Namecheap Inc. la cual trabaja en conjunto con la organización Whoisguard Inc. La primera registró el dominio y tiene los datos de pago, dirección y nombres de la persona que lo registró y la segunda es la que se encarga de proteger estos datos para que no sean públicos, por ende la comunicación o solicitud debe hacerse a ambas. Recalcamos que la empresa de Hush tiene protocolos de encriptación para proteger la información utilizando protocolos como *openpgp*; todos los *e-mails* se envían cifrados para que nadie los pueda leer o interceptar y puede utilizar alias ilimitados con la misma cuenta de correo. Los servidores están alojados en Canadá lo cual gozan con una protección de datos especial ya que la ley canadiense en virtud del secreto fiscal. Preguntado respecto de su anterior declaración, para que describa o aclare a través de qué se realiza la inyección SQL y la transferencia de los fondos de los clientes de Mercury Cash, contesta: H. manipula la cuenta D., la cuenta de A. y su cuenta personal validada. Primeramente se conecta a través de la cuenta de usuario D. y realiza varias transferencias por un total de 619,31 ETH distribuidas en tres billeteras: la terminada en '...' (billetera 1) por ETH 469,49, la terminada en '...' (billetera 2) por ETH 33,5, a la terminada en '3952' (billetera 3) por ETH 26 y a la terminada en '...' (billetera 4) por ETH 90. La suma de los montos no da el total, puede haber alguna diferencia en los montos porque las transferencias tienen un costo. Posteriormente desde la billetera 1 se transfieren 26 monedas a la billetera número 5 terminada en '...' que se encuentra entre los favoritos de la cuenta validada de H. El usuario A., registrado el 14 de diciembre, justo después que D. terminara de extraer las monedas para realizar acciones similares, iniciando sesión desde la misma IP que D.,

registrada en Reino Unido. El día 15 de diciembre de 2017 A. intenta replicar el ataque desde la dirección IP de Suiza y como no pudo realizar su cometido, realiza un *request* a la cuenta de H., cierra sesión y luego en forma inmediata inicia sesión H. con su cuenta validada desde la misma IP de Suiza y el mismo equipo. Debo resaltar que para todas las operatorias, tanto de la cuenta usuario D., A. y H. se utilizó el mismo equipo, consistente en un PC que utilizaba navegador Firefox y sabemos que es el mismo equipo porque de haberlo cambiado esta grabación se hubiese interrumpido. El hecho de que un equipo tenga diferentes direcciones IP no significa que sea otro computador diferente ya que el computador puede estar conectado a una o varias VPN. Ello se podría determinar a través del análisis que se realice al computador, al *router* y al módem que conmutaban con el proveedor de internet. El imputado decidió utilizar una VPN que le permitiera cambiar su IP tantas veces como quisiera para evitar ser ubicado, no obstante, cometió el error de no conectarse a la VPN en varias ocasiones y de iniciar sesión con su cuenta validada utilizando la IP que utilizó A. y a su vez A. es la cuenta que conecta con D. Acto seguido se procede a la exhibición de los secuestros detallados en acta de secuestro impostergable del 29 de de diciembre de 2017 en ..., primer piso, ciudad, consistentes en: (1) una libreta tipo cuero, color marrón, con anotaciones varias, (1) un trozo de papel color blanco escrito con tinta color azul con las siguientes palabras textuales: '*Only use by Mercury Cash december 28th 2017*', (1) un pasaporte color azul oscuro del Mercosur República Argentina, a nombre de H. M. P.; (2) dos tarjetas de la firma OSDE a nombre de P. S. A. y P. L. M.; (1) un documento nacional de identidad a nombre de H. M. P.; (1) una tarjeta de débito Visa BBVA Francés; (1) una tarjeta de crédito Payments Association MasterCard; (1) una tarjeta Visa del Nuevo Banco del Chaco; (1) una tarjeta MasterCard del Nuevo Banco del Chaco; (1) una tarjeta MasterCard del Nuevo Banco del Chaco; (1) una tarjeta Tuya del Nuevo Banco del Chaco; (1) una tarjeta Visa del Nuevo Banco del Chaco; (1) una tarjeta de débito Maestro del Nuevo Banco del Chaco; (1) una tarjeta de débito Debit Card Visa todos a nombre de H. M. P., a lo que manifiesta: respecto del trozo de papel color blanco escrito con tinta color azul con las siguientes palabras textuales: '*Only use by Mercury Cash december 28th 2017*' y el pasaporte color azul oscuro del Mercosur República Argentina, a nombre de H. M. P., son los mismos que figuran en la fotografía —*selfie*— que envió H. a Mercury Cash. Respecto de la tarjeta de débito Debit Card Visa, número ... - My Choice Corporate, corresponde al WaveCrest Holdings Ltd. y es de España y sería útil solicitar informe si en esa cuenta hay movimientos de compra y venta de criptomonedas a cualquier proveedor o persona. Asimismo se exhibe y reproduce un DVD aportado por el denunciante M. H., a lo que manifiesta: Se corresponde con la filmación que nos da Lucky Orange y allí se puede determinar los clics que hace la persona imputada y corresponden a una persona que posee una práctica y conocimientos amplios para realizar esta actividad. En las filmaciones se observa también cómo carga la información de transacciones de diferentes usuarios utilizando una sola cuenta, es decir ha ingresado a la base de datos y ha cargado la información de otros usuarios en esta cuenta. Adicionalmente se expone cómo intenta realizar cambios con etiquetas de código en los alias de las billeteras e incluso en el nombre del perfil de su usuario con la finalidad de adquirir acceso a la base de datos a través de inyección SQL. Si no arroja resultado, lo vuelve a intentar hasta que lo logra. Es así que utilizando el inspector de elementos del navegador y cualquier otro *software* que le ayude, logra cargar en el campo *from* (desde) las billeteras de cada uno de los clientes de Mercury Cash, cuando el sistema sólo le permitiría en condiciones normales, cargar la suya propia. Es así que pudo ver los balances de cada billetera y transferir los montos completos a las billeteras 1, 2 y 3...".

Acta de Gabinete Científico del Poder Judicial del orden 76 donde se hace constar que en fecha 14 de marzo de 2018 se hacen presentes en el Gabinete Científico del Poder Judicial sito en Ruta 11, Km 1008, de Resistencia, Chaco, el ciudadano argentino P. M. C. DNI: ..., el ciudadano venezolano ... Pasaporte Nº ..., y el ciudadano venezolano M. P. Pasaporte Nº ... quienes presenciaron la apertura de los seis (6) elementos remitidos a esta instancia por el Departamento de Investigaciones Complejas - División Delitos Tecnológicos de la Policía del Chaco, cada uno de ellos con sus respectivas planillas de cadena de custodia. En este mismo acto se realizaron las copias forenses de los elementos a detallar: a) un (1) teléfono celular Samsung SM-A720F Galaxy A7 2017 y una tarjeta SIM que se encontraba insertada en su correspondiente ranura, sin tarjeta de memoria expansible; b) un (1) teléfono celular Samsung GT-I8190L Galaxy S III Mini y una tarjeta SIM que se encontraba insertada en su correspondiente ranura, sin tarjeta de memoria expansible; c) una (1) computadora tipo *notebook* color negra, marca Compaq Presario CQ, serie Nº ... que posee un disco rígido marca Toshiba s/ Nº ... EU9 EC.B, del que queda pendiente de realizar la copia forense debido a fallas en la verificación de la copia; d) un (1) disco rígido marca Seagate s/ Nº: ..., siendo que de este último elemento no fue posible realizar una copia forense debido a que se encuentra dañado y no es posible acceder al contenido con los medios que ese laboratorio posee. En este mismo acto se realizó el embalaje de los elementos para su debido resguardo, como así también el embalaje del disco con número de inventario ... s/ Nº: ... donde se realizaron las copias forenses. Actas del Gabinete Científico del Poder Judicial del orden 106 del SIGI que dieron cuenta de las operaciones realizadas por los peritos oficiales y de parte para la pericial informática ordenada en autos.

Informe pericial Nº 17/2018 del Gabinete Científico del Poder Judicial. El mismo versaba inicialmente sobre seis elementos: Elemento 1 —celular en poder del imputado H. M. P. al momento de efectuar allanamiento en la casa de sus padres, Av. Rivadavia ..., Resistencia—. Un (1) teléfono celular marca Samsung, modelo Galaxy A7 año 2017, color dorado, pantalla táctil, IMEI Nº ..., Serie Nº ... Elemento 2 —computadora secuestrada en uno de los ambientes del domicilio de Av. ..., Resistencia—. Una (1) computadora portátil, color negra, marca Compac Presario CQ, serie Nº ..., la cual se encontraba apagada. Elemento 3 —celular hallado en poder de S. P., padre del imputado en el mismo allanamiento citado—: un (1) teléfono celular marca Samsung, modelo GT-I890L, color blanco, pantalla táctil, IMEI Nº..., con funda de silicona de color negro, abonado Nº ... Elemento 4: un (1) *router*, color negro, marca Hitron, modelo CGNV2; Cm Mac: ...; Mta Mac: ..., con su respectivo cargador. Elemento 5: un (1) disco rígido interno, con la capacidad de 1 TB, marca Seagate, s/ Nº: ..., ST: ... Elemento 6: un (1) *router*, marca Cisco, color negro, modelo ..., Wan Mac ..., con su respectivo cargador. En primer lugar se hace constar que no se pudo peritar los elementos número 5 (disco rígido que se encontraba dañado internamente), ni los elementos número 4 ni 6 (*routers*, por no contar con datos de su configuración por defecto), por lo cual el informe se circunscribe a los elementos 1, 2 y 3, siendo el elemento 1 —teléfono de M. P.— el único con registros de interés.

Es así que en el elemento 1 se halló que el mismo posee el *browser* Chrome instalado, que posee el sistema operativo Android 6.0.1 ID Android: ..., lo cual coincide con lo solicitado por la querella en sus puntos periciales en cuanto a que solicita realizar una búsqueda del historial del teléfono confiscado Samsung, Galaxy A7 ya que en la base de datos de Mercury Cash coincide un dispositivo con las mismas características, la información es la siguiente: Mozila/5.0 (Linux; Android 6.0.1; SM-A720F Build/MMB29K). En las conversaciones extraídas del elemento 1 —celular secuestrado en poder del imputado M. P.— realizadas a través de Telegram entre el usuario ... y el usuario M. P. ..., se puede apreciar que se comunica la realización de una operación de transferencia de moneda virtual. En ella el usuario "M. P." el día 17/12/2017 a 16:36:16 (UTC-3) expresa: "...tio, aparece. Cuanto sacaste de Mercury Cash? Han sido mas que 200 eth, no? Envía algo mas, comparte. Además que solo he recibido 25, ya que estos hijos de puta de ccex.com no me han solucionado el tema. Otra cosa, ayer apareció un deposito en usd en mi cuenta mercury de 10 usd. Has sido tu supongo? Vale, pero porfa envia algunos eth mas. Tu quedate con la mayoría, pero comparteme algo mas que necesito, mas con esos 25 que no me han acreditado en ccex.com...". El 18/12/2017 a 08:02:15 (UTC-3) M. P. manifestó: "...tio aparece por dios. Hace cuanto trabajamos juntos? Puedes enviar algo más de eth. Has hecho mas de 400 eth, podrías haber enviado al menos el 25%, no? Yo te dije que envíes 50 porque pensé que habías hecho 200 solamente. Y encima he perdido 25 eth a manos de los ladrones de ccex.com, no es culpa tuya ni mía, pero bueno, ya está, lo he perdido. Por eso te pido que al menos envíes el resto, seria justo y seria compartir. Tú hiciste el trabajo pero yo he encontrado el *bussiness*, como tantas otras veces. Espero aparezcas y puedas enviar el resto o algo mas, ya que me he quedado solo con 25 eth y quisiera usar el resto para ir de vacaciones y pagar algunas deudas. Te lo agradeceré tio. Envía aquí: ...". Se encontraron doscientos veinte (220) registros en el elemento 1 que coinciden con la siguiente palabra clave ..., éstos se grabaron en el DVD adjunto, haciéndose constar que el correo electrónico ... es el mismo con el cual M. P. registró su cuenta validada ante Mercury Cash, sumado a lo cual en la pericial se encontraron registros del uso de una cuenta con dominio *hush.com*. Los registros obtenidos se grabaron en el DVD adjunto. Se encontraron en el elemento 1, coincidencias en las *cookies* e historial de internet con la dirección IP ..., la cual se corresponde al servicio de internet instalado en el domicilio de P. sito en ..., registrado mediante el correo electrónico ..., los días 12, 13, 14, 15, 16, 17 y 18 de diciembre de 2017. En la búsqueda de la billetera virtual ... se produjo una coincidencia en el elemento 1, en el cuerpo de un correo electrónico, el cual fue enviado y recibido por la cuenta ..., donde no se pide ningún tipo de autorización.

Concluido el respectivo análisis de las probanzas, el suceso histórico reconstruido materialmente en el hecho descripto en su plataforma fáctica que sustentara la elevación a juicio del proceso, según el principio de verdad-correspondencia en su valoración, se encuentra ciertamente avalado por la conjunción de las pruebas enunciadas y analizadas. Caudal que también sostiene mi absoluto convencimiento de que respecto de la modalidad implementada, se puede concluir que el procedimiento implementado por el imputado consistió en que tras advertir la posibilidad de evadir la seguridad del sitio —Mercury Cash— en el procedimiento de transferencias, previo enmascarar su IP, mediante el uso de una VPN y al solo efecto de no ser correctamente detectado, decidió y logró —posiblemente a través de un navegador *web*— introducir un código que le permitió obtener conocimiento del estado de cuentas de los usuarios de dicho sitio para posteriormente transferir diversos montos de bienes ajenos para su beneficio personal. Proceso desconocido y por lo tanto no autorizado por la empresa ni por sus legítimos usuarios/propietarios de los bienes transferidos; obrando de mala fe y con conciencia de ilicitud y utilizando diversas direcciones de IP ubicadas geográficamente en otros países, tal como surge de la declaración testimonial del Sr. P. B. (RI 64 y ampliación de RI 66).

En dicho sentido la Cámara Federal de Casación Penal, sala III, "Castelo, Pablo Alejandro", causa Nº 51772/2011, 16/06/2015 —defraudación por medios informáticos— destacó que "de acuerdo a la nueva tecnología de que dispone cualquier persona con conocimientos de informática puede operar un 'IP' situado en otro país desde la República Argentina, tal como se explica, incluso, mediante tutoriales en internet [...] que brindan instrucciones no sólo para navegar con un IP de otro país sino también para hacerlo en forma anónima, esto es, sin poder ser identificado".

Aquí a través de una manipulación informática —posible acceso por medio de un navegador *web* al código de la página en cuestión —Mercury Cash— y sin la debida autorización— provocó la transferencia de un activo con contenido apreciable económicamente (moneda virtual) en

perjuicio del patrimonio de las víctimas y en beneficio del imputado.

De todo lo descripto y detallado, surge con certeza la autoría indubitada de H. M. P., respecto del hecho acreditado en autos, cuya materialidad le fuera atribuida oportunamente, al momento de ejercer su defensa material en fecha 02/01/2018 —OS Nº 14— y su ampliación de fecha 01/08/2018, oportunidades en las que el imputado se abstuvo de prestar declaración. Sin perjuicio de ello, el reconocimiento expreso del hecho y su respectiva participación en él neutralizaron tales estrategias defensivas, dado que a esta altura del procedimiento el contexto procesal ha variado en función de su adhesión expresa ya referida. Lo expuesto al analizar el contexto de este proceso, hoy en instancia de juicio abreviado, constituye el plexo probatorio a cuya valoración me constriñe la normativa vigente para este tipo de juicio (art. 429 del CPP). He evaluado concienzudamente las pruebas reunidas, siguiendo las reglas de la sana crítica racional. Así, he puntualizado el hecho que considero se ha materializado en el proceso elevado a juicio. Conclusiones que con certeza, me autorizan a afirmar que en el mismo, ha tenido participación activa el enjuiciado.

En consecuencia, concluyo afirmando que en el camino convictivo abordado, en función de las pruebas analizadas, doy por cierto en esta causa, el siguiente hecho: Que entre los días 14 de diciembre y 16 de diciembre del 2017, H. M. P., a través del ingreso indebido a las cuentas de distintos usuarios o clientes de la empresa "Mercury Cash", mediante técnicas de manipulación informática de forma ilegal logró transmitir a su cuenta/usuario la cantidad de 500 Ethereum —criptomoneda— "datos" perjudicando a la empresa y sus clientes en el monto de USD 434.352,63 (valor de Ethereum al momento del hecho). Hecho cuyo autor es el acusado H. M. P. interviniendo como autor material del acontecimiento narrado, en sus circunstancias de tiempo, modo, lugar y modo por lo que merece reproche penal a título de autor material. Así me expreso.

Calificación legal: en autos el imputado, H. M. P., fue requerido a juicio por la comisión del delito de defraudación informática en concurso real con violación de secretos y de la privacidad (art. 173, inc. 16, art. 153 bis, 2º supuesto, en función del art. 55 del CP), al formalizar el acuerdo entre el fiscal de investigación, el imputado y la defensa han consensuado la misma calificación legal.

El derecho penal ha sufrido en la historia, determinados cambios tecnológicos (energía eléctrica, aparición del automóvil, maquinaria industrial, etc.), y ha logrado resolver dichos inconvenientes normativos con la aplicación de tipos preexistentes a dichos fenómenos tecnológicos innovadores y revolucionarios. Pero, en la actualidad y a raíz de esta "nueva revolución" que muchos llaman "la era digital" o "revolución informática" —entre varias denominaciones que se le ha dado a la revolución de la tecnología del siglo XX— la violación de la dignidad de la persona a través de medios informáticos, crea un nuevo derecho fundamental denominado indistintamente "libertad informática", "derecho de autodeterminación informativa" o "derecho a la intimidad informática".

Para ello, fue necesario la creación de nuevos tipos para cubrir ese vacío legal generado por nuevas situaciones de peligrosidad. Sabido es que la informática interactúa con la sociedad a velocidades exponenciales, en lugar de las lineales correspondientes a las ciencias jurídicas.

Así la doctrina especializada y la legislación especial —junto con la adaptación de tipos preexistentes— ha debido abocarse a la creación de nuevos tipos que puedan otorgar protección jurídico-penal a nuevos bienes jurídicos o intereses, que en la actualidad se ven vulnerados mediante la evolución de las tecnologías y las nuevas modalidades de cometer delitos a través de ellas.

El delito informático implica actividades criminales que muchas veces encuadran en las figuras tradicionales como robos, hurtos, falsificaciones, estafa, sabotaje, daños —entre otros—. Sin embargo, debe destacarse que el uso de las técnicas informáticas, ha creado nuevas posibilidades del uso indebido de computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del derecho penal.

La ley 26.388 (04/06/2008, BO: 25/06/2008) por el art. 9º incorpora art. 173 en los "Delitos contra la propiedad", al Código Penal el inc. 16 que establece: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos", configurándose el delito de defraudación informática.

La inclusión del inc. 16 por la ley 26.388 puso fin a la dificultad que algunos hallaban para encuadrar como fraude a la acción ilegítima de obtener un crédito o la supresión de un débito, por ejemplo, de un sistema informático al que se accediera mediante una computadora, en el entendimiento de que no había un sujeto engañado, pues el ardid o engaño debían tener como víctima a una persona y su inteligencia. En líneas generales consisten en acceder a un sistema o dato informático restringido, sin que medie consentimiento del sujeto pasivo. Por "acceso" se entiende todo ingreso no consentido.

La tipificación se configura teniendo como bien jurídico, objeto protegido, la propiedad o el patrimonio, considerándose que en ciertos casos resultaría más apropiado consignar el bien jurídico del "patrimonio" como el verdaderamente afectado, ya que especialmente en este caso, no es la propiedad ni un elemento de propiedad del sujeto pasivo el que será objeto de la conducta típica, sino el patrimonio mismo de la víctima.

En cuanto al verbo típico "defraudar", según la ubicación sistemática del nuevo tipo penal lleva a afirmar que deben requerirse todas las exigencias propias de cualquier defraudación patrimonial, se ha resuelto, que la utilización de un mecanismo de manipulación informática es constitutivo del ardid y del consecuente error característicos de esta clase de delitos.

Actualmente el abanico de posibilidades de la manipulación informática va al compás de la imaginación del agente y de las posibilidades superadoras de la técnica y no sólo se reduce a la utilización del ordenador sino que abarca otros aparatos o sistemas —por ejemplo, cajeros automáticos—, por ello, se adopta la frase "mediante cualquier técnica de manipulación informática".

En lo concerniente al concepto de "manipulación informática" el mismo se corresponde con la conducta de alterar, modificar u ocultar datos informáticos de manera que, se realicen operaciones de forma incorrecta o que no se lleven a cabo, y también con la conducta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener. De esta forma un sujeto puede enclavar instrucciones incorrectas.

La manipulación en el ingreso de los datos a la computadora que se basa en una información que será luego ingresada a la misma por medio de un programa adecuado el cual procederá a ordenarla, archivarla, clasificarla y/o realizar operaciones. En el caso se trata de la manipulación de datos ingresados a la computadora, en este supuesto, el autor manipula los datos lo que se puede hacer al menos de dos formas (1), introduciendo información falsa al ordenador —como en el caso anterior— (2) o alterando los datos una vez que éstos han sido correctamente introducidos al sistema (3) o bien eliminando información. En estos supuestos se puede hablar de estafa.

Ejemplo de manipulación es el de los datos que se obtienen de la computadora objetivo (a través del acceso solapado que habilita un "caballo de Troya" previamente ingresado y ejecutado en el sistema de la víctima). Es posible manipular la información que se ejecuta y almacena de manera tal que la alteración no pueda detectarse, durante el procesamiento de los datos y el uso cotidiano del sistema.

Si bien la norma elabora como verbo típico el acto de manipular lo que de por sí nada explica puesto que tiene sabor a actividad prolongada sobre un objeto para la obtención de algún provecho y dado que el concepto de perjuicio patrimonial no se aprecia ni siquiera en la norma, ello debe derivarse de su calidad de defraudación especial y su ubicación sistemática en el Código sustantivo en el capítulo de los delitos contra la propiedad.

Apunta Palazzi —en "Los delitos informáticos en el Código Penal. Análisis de la ley 26.388", Ed. Perrot, Buenos Aires, 2009, p. 181— que la norma al indicar "mediante cualquier técnica de manipulación informática" se está haciendo alusión en forma abierta al accionar central de la estafa informática, al que no se lo precisa, como hacen otras legislaciones, porque se trata de un elenco muy abierto de posibilidades, aunque no debe ser cualquier técnica sino aquella que altere el funcionamiento de un sistema informático o la transmisión de datos. Este último es el supuesto donde no se altera el sistema informático, aunque se lo engaña en la recepción de información, por ejemplo, impidiendo el funcionamiento de rutinas de chequeo o validación de datos.

Es preciso aclarar, con respecto a la manipulación informática, que la misma en sí no es típica, sino que lo es, sólo aquella que además ha provocado una alteración en el sistema informático o transmisor de datos de la víctima o de un tercero.

La expresión "que altere" el funcionamiento del sistema informático o de transmisión de datos, se vincula necesariamente con la misma manipulación y sólo excluye el manejo o la operación que se sirve del medio tecnológico para obtener una ventaja patrimonial indebida, que no modifica su normal programación o funcionamiento.

La nueva ley ha extendido ahora la inclusión en la categoría de estafas o defraudaciones, a todo otro perjuicio patrimonial ocasionado por manipulación de sistemas informáticos o de transmisión de datos cuando se altera su sistema operativo... Es una figura residual de la tipificada en el inciso anterior ya que todos los casos que no se puedan comprender dentro del anterior inciso —el 15— son atrapados por el presente —inc. 16—. La manipulación de sistemas informáticos o transmisión de datos que se vincula con tarjetas de crédito, débito o de compras, será una modalidad defraudatoria propia del inc. 15, mientras que toda otra operación no vinculada con tales instrumentos encontrará su adecuación típica en el inc. 16 —ambos del art. 173 del CP—, cuando se altere el normal funcionamiento del sistema o de la transmisión de sus datos".

El fraude a que alude el tipo es consecuencia de la manipulación informática, por medio de la cual se altera el normal funcionamiento del sistema o la transmisión de datos, siendo este último supuesto lo que ocurrió en autos. La manipulación consiste en cualquier modificación del resultado de un proceso automatizado de datos, sea introduciendo nuevos datos o alterando los ya existentes, en cualquiera de las fases de su procesamiento o tratamiento.

La acción típica: la manipulación informática para que se concrete debe "alterar" el normal funcionamiento de un sistema informático o la transmisión de datos. No es cualquier manipulación informática, sino sólo la que es apta para producir dicho efecto.

Etimológicamente "alterar", del latín *alterare*, significa modificar, cambiar la esencia o forma de algo, trastornar, perturbar. Estos conceptos se adaptan perfectamente al término referido a la manipulación alterativa, pues aquélla consiste en justamente modificar o cambiar el funcionamiento normal de un sistema o la transmisión de datos, y el agente incurre en el tipo al llevar a cabo esa actividad. Si por un error en la programación ello no sucede, estaremos ante un delito tentado o uno imposible (si por la programación del sistema nunca hubiera sido posible realizar la alteración de la forma en que se lo intentaba).

Desde el punto de vista legal sistema informático es todo dispositivo separado, o que forma parte de dispositivos interconectados o emparentados, que asegure mediante la ejecución de un programa, un tratamiento automatizado de datos; el dato es la información que debe suministrarse a un ordenador, preparada en forma adecuada, para ser usada en sistemas de computación. A su vez por "sistema informático" la definición que se daba en la res. 476/2001 de la Secretaria de Comunicación de la Nación, la conceptualiza como: "Todo dispositivo o grupo de elemento relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio". Y por "trasmisión de datos" —se entiende de dato informático— "toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático" a lo que agrego que además puede ser transmitido por medios físicos de un sistema informático a otro.

Los sujetos activos de estos delitos tienen la particularidad de poder llevar a cabo varias conductas que tienen múltiples connotaciones y alcances.

Sujeto activo puede ser cualquier persona, el dato lo da el comienzo de la redacción de la norma "el que", es decir que no se requiere una calidad especial. Si bien estos casos en términos latos, se podría decir que normalmente intervienen sujetos "especializados" en estos menesteres.

Usualmente se menciona al *hacker* como aquel que capta o interfiere información sensible y puede utilizarla en perjuicio del poseedor de la misma, en principio puede ser una mera intromisión en la intimidad de la persona —intruso—, pero si se sirve de dicha información para defraudar, es obvio que se produce una situación progresiva —por ejemplo ingresar en las cuentas corrientes, en operaciones bancarias, o base de datos de un banco y de esta manera establecer la frecuencia de los depósitos en cuenta corriente de una empresa; qué porcentaje es en efectivo y qué porcentaje es en otros valores; a qué hora realiza los depósitos y en qué agencia bancaria— pues de mero intruso pasa a ser ejecutor de un delito contra la propiedad.

Lo real y concreto, es que tanto los *hackers* en la medida en que manipulen fraudulentamente alterando el normal funcionamiento de un sistema informático o la transmisión de datos, incurren en el tipo en análisis.

Entre las víctimas o sujetos pasivos del delito informático encontramos a individuos, empresas, instituciones, gobiernos, etc., que utilizan sistemas automatizados de información, los cuales, por lo general se encuentran conectados a otros, también puede ser cualquiera, quien, en definitiva, resultó engañado y dispuso perjudicialmente del patrimonio. También como en el caso del inc. 15 se puede dar la estafa en triángulo.

La figura penal en trato, al igual que en todas las formas de estafa, requiere para su configuración el causar un perjuicio de contenido patrimonial a otra persona. En el caso, la disposición patrimonial debe ser consecuencia de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos que produce el hecho lesivo. En esta dirección, se entiende como manipulación a cualquier modificación del resultado de un proceso automatizado de datos, a través de la alteración de los existentes o la introducción de nuevos, en cualquiera de las fases del proceso [...].

Las maniobras ejecutadas permiten inferir un alto grado de conocimientos informáticos con entidad para violar los sistemas de seguridad que la firma damnificada, al tiempo de los hechos instrumentaba, acreditándose de este modo, el elemento subjetivo del tipo penal en juego.

A su vez, el perjuicio económico, ha tenido lugar puesto que los sujetos pasivos, se han visto privados de un elemento integrante de su patrimonio por obra de la acción delictiva, cuya disminución resulta evaluable económicamente, lo que se verifica en el expediente, y en los registros de la firma Mercury Cash, en un monto aproximado de USD 434.352,63 (valor de Ethereum al momento del hecho)". En este caso, el acceso se produjo mediante técnicas de manipulación informática de forma ilegal, logrando de esta manera ingresar a las cuentas de distintos usuarios y transmitir a su cuenta perjudicando a la empresa y sus clientes.

Por lo que la conducta desplegada por P. encuadra en la figura penal de defraudación informática (art. 173, inc. 16, del CP).

Además de ello, el imputado ha sido asimismo reprochado en tanto con la misma maniobra, el imputado logra acceder al sistema y a datos restringidos. En este caso, la norma penaliza el mero intrusismo informático, lo que opera como conducta de antesala de otras más graves, las que se quiere evitar aun penalizando etapas tempranas del *iter criminis*. La escala penal se eleva cuando el sujeto pasivo —titular del sistema o *dateo*— es un organismo público estatal o un proveedor de servicios públicos o financieros, lo que ocurre en este caso particular al tratarse de la empresa Mercury Cash, destinada a servir a la población.

Este tipo penal se ocupa del intrusismo propiamente dicho, despojado de cualquier otra intención distinta del acceso mismo y de los diversos protagonistas del llamado mundo subterráneo de la computación.

El resultado requerido es, como en las demás defraudaciones, el perjuicio patrimonial para el sujeto pasivo. Aquí se manifiesta en una transferencia electrónica no consentida de un activo patrimonial en beneficio propio o de un tercero; el acto dispositivo se traduce en un traspaso de dinero contable, de un asiento a otro. Acción que despliega P. al transmitir a su cuenta la cantidad de 500 Ethereum —criptomoneda— "datos restringidos" perjudicando a la empresa, su credibilidad y sus clientes en el monto de USD 434.352,63 (valor de Ethereum al momento del hecho)"; obligando a esta empresa a reforzar sus procesos de seguridad en la acreditación de cada transacción.

Por lo que la conducta que desplegó H. M. P. encuadra en la figura penal de violación de secretos y de la privacidad (art. 153 bis, 2º supuesto, en función del art. 55 del CP).

Éste es el contexto legal general dentro del cual he examinado la conducta del encartado puesto que así me lo impone la legislación procesal aplicable para el proceso tratado.

Así, coincido con la calificación legal definitivamente consensuada por las partes, Fiscalía, defensa e imputado en el acta de acuerdo —Nº de OS 122—, especificándose que la calificación legal correspondiente al accionar de H. M. P. es la de: defraudación informática en concurso real con violación de secretos y de la privacidad (acceso ilegítimo a un sistema informático) arts. 173, inc. 16, 55, art. 153 bis, 2º supuesto, en función del art. 45 del CP. Presupuestos necesarios con los que ha quedado acreditada la vulneración del bien jurídico protegido por la norma. Así me expreso.

Responsabilidad asumida: determinado el hecho y definida la autoría del imputado en el mismo, sostengo la existencia en el caso, de comportamientos que contradicen la norma penal. Que se adecuaron a conductas perfectamente típicas en la que se demostró la ausencia de intereses prevalentes que lo determinen. Habida cuenta que ha obrado sin causas de justificación alguna, siendo culpable de dichas acciones típicas y antijurídicas.

Habiéndose demostrado que se trata de una persona sana física y mentalmente a tenor de la impresión personal que me dio en la audiencia *de visu*, oportunidad en la que ha demostrado comprender su situación, ha podido mantener una conversación con sentido lógico y ha manifestado su adicción a la ludopatía reclamando la implementación de un tratamiento adecuado a su circunstancia personal.

En el ámbito de la culpabilidad, tampoco hay mucho para agregar en relación a estas nuevas modalidades de comisión de delitos. El derecho tiene dos formas para hacer responder al sujeto por sus acciones. Por un lado tenemos la responsabilidad objetiva. En este caso, el sujeto responde porque su acción menoscabó un bien jurídico (el derecho pretende volver a equilibrar las relaciones de bienes que la acción desequilibró). Por otro lado, tenemos el caso de la responsabilidad subjetiva. Aquí, el sujeto responde porque la acción se le puede reprochar por haber actuado con voluntad de desconocer el mandato protector del bien jurídico (directamente ha querido violarlo o no atendió como debería de haberlo hecho a la posibilidad de violarlo). Aquí el reproche se presenta como fundamento o presupuesto de la sanción.

Por las circunstancias mencionadas precedentemente H. M. P. ha obrado, siendo culpable de tales acciones, trasgrediendo conductas prescriptas por la norma prohibitiva del tipo penal infringido la que conocía, predeterminándose a actuar en el sentido que lo hizo en un ámbito de libertad y autodeterminación personal, utilizando tecnología apropiada al cometido de las acciones ilícitas que consumó.

En función de ello afirmo que el reconocimiento de su autoría y participación en el hecho resulta legalmente válido y es producto de su voluntad, por lo que merece sanción penal. Así me expreso.

Sanción punitiva convenida: tipificados los hechos y definida ya la autoría responsable del imputado, cabe referirme ahora a la cuestión de la individualización de la pena a aplicar, teniendo en cuenta, en primer lugar, el hecho cuya sanción ameritara la procedencia del juicio abreviado y el encuadramiento legal que hace prever una escala sancionatoria en abstracto de un (1) mes —mínimo— a siete (7) años —máximo— de prisión.

Tal como lo impone la vía del juicio abreviado reglada en los arts. 426, 429, 1º párrafo y ccds. del Código de rito, debo cuantificar en esta sentencia el monto de la sanción a aplicar al justiciable, la que no podrá superar ni resultar más severa, de la acordada entre las partes. El Sr. fiscal convino con H. M. P. y su defensa técnica, por el hecho por el que fuera traído aquí a juicio y teniendo en cuenta los antecedentes penales condenatorios computables que pesan sobre el imputado (sentencia Nº 41 de fecha 19/05/2017, dictada por el Juzgado Correccional Nº 1 de esta ciudad en la causa Nº 18629/2015-1, caratulada: "P., H. M. s/ lesiones leves calificadas por el vínculo y el género", en la cual se lo condenó a la pena de seis meses de prisión en suspenso por considerarlo autor penalmente responsable del delito de lesiones leves calificadas por el vínculo y por haber sido cometidas en un contexto de violencia de género; arts. 89 en función con el 92 y 80, incs. 1º y 11, del CP, cuya condicionalidad se revocará), en la extensión del acuerdo realizado en el *visu*, la aplicación de la pena única conformada por el método de composición de dos (2) años de prisión de cumplimiento efectivo, como autor penalmente responsable del delito de defraudación informática en concurso real con violación de secretos y de la privacidad (acceso ilegítimo a un sistema informático) en concurso real con lesiones leves calificadas por el vínculo y por haber sido cometidas en un contexto de violencia de género (arts. 173, inc. 16, 55, 153 bis, 2º supuesto, 55, 89 en función con el 92 y 80, incs. 1º y 11, todo en función del art. 45 del CP), según la calificación legal contemplada en ambas causas respectivamente y las consideración precedentes. Expresamente interrogadas las partes han expresado su total conformidad con el monto de pena única determinado en el convenio pertinente, ampliado en esos términos en la audiencia *de visu* y, durante la audiencia de conocimiento personal que celebré, el imputado expresó su aprobación. Asimismo, no procede la declaración de reincidencia, por no darse los extremos previstos en el art. 50 del CP y los antecedentes de la modalidad de la pena que la primera condena adoptara respecto de la pena aplicada en la misma.

Siendo un deber de inexcusable contenido republicano en tanto: "El juicio previo establecido por el art. 18 de la Constitución Nacional como derivación del Estado de derecho no sólo exige que los jueces expresen las razones en que se encuentra fundada la responsabilidad o irresponsabilidad del procesado, sino también aquellas en que se apoya la naturaleza e intensidad de la consecuencia jurídica correspondiente (conf., entre otros, Fallos 314:1909)". CSJN, R.804.XL, recurso de hecho "Romano, Hugo E. s/ causa Nº 5315"; subordino a ello la tarea analítica de esta última cuestión, con especial consideración a la función y finalidad de la pena y sus parámetros de proporcionalidad y razonabilidad. A su vez por imperativo legal, y directriz derivada de los derechos esenciales que integran la personalidad de la imputada, he de merituar el monto de la pena a aplicar según pautas que emanan de los arts. 40 y 41 del CP, en función de la escala penal que en abstracto se prevé para los delitos respectivamente incriminados, en tanto la pena se individualiza teniendo en cuenta la magnitud del injusto y la culpabilidad, y como correctivo, la peligrosidad.

En tal sentido, considero para el caso de H. M. P., como circunstancias agravantes:

— La naturaleza del hecho con connotación negativa para la sociedad, utilizando equipamiento tecnológico apropiado y valiéndose de su experto conocimiento informático para el cometido de sus designios ilícitos, lo que determina su personal y menor vulnerabilidad social.

— La extensión del daño patrimonial ocasionado, lucrando con una actividad en la cual los sistemas operativos cuentan con resguardos especiales de seguridad, horadando la confianza pública que tales sistemas ofrecen a los usuarios, en su propio beneficio.

— La ausencia de motivos determinantes e insuperables que lo determinaron a delinquir, adoptando equipamiento especial para el cometido de sus designios.

— La existencia de antecedentes penales condenatorios computables en su contra, ésta no será su primer condena.

Como atenuantes a su favor valoro:

a) Las condiciones personales, un hombre joven, con 36 años de edad, con estudios universitarios incompletos, quien es comerciante. Con excepcionales conocimientos en sistemas operativos lo que es de esperar lo ayuden a utilizarlos para su supervivencia de manera lícita. Circunstancias de su vida personal que es de esperar que le permitirán readaptarse social y familiarmente ya que es padre de dos hijos menores de edad.

b) Su voluntad de someterse a la ley, en este proceso, admitiendo el disvalor que su conducta irregular significó para con la sociedad y las consecuencias personales acarreadas, solicitando al tribunal la implementación de un tratamiento específico para neutralizar la viciosa conducta derivada de su afección al juego, incluyéndose en un programa de tratamiento para la "ludopatía" que padece.

c) Su actitud durante la audiencia *de visu*; predispuesta a reflexionar sobre las consecuencias negativas para su vida que el hecho juzgado le ocasionara.

Dentro de ese conjunto, siguiendo los lineamientos valorativos y en mérito a los parámetros que he expuesto, donde también evalúo los efectos disgregantes que produce la pena, entiendo por ser justa, equitativa y proporcional, apropiada al reproche ilícito que le fuera endilgado, es que concuerdo plenamente con la condena al acusado de dos (2) años de prisión de cumplimiento efectivo. En orden al hecho cometido entre los días 14 y 16 de diciembre de 2017, en perjuicio de la empresa "Mercury Cash" y sus clientes, por el que fuera investigado y requerido a juicio por el Equipo Fiscal Nº 13, expte. Nº 17029/2017-1, caratulado: "P., H. M. s/ defraudación informática en concurso real con violación de secretos y de la privacidad", expte. Nº 40134/2017-1, expediente policial: E-21-2017-2142-E, sumario policial: 170-CSPJ/17.

Corresponde, asimismo, revocar la condicionalidad de la pena impuesta por sentencia Nº 41 de fecha 19/05/2017 dictada por el Juzgado Correccional Nº 1 de esta ciudad y unificar por composición la pena impuesta en la misma con la presente, fijando como pena única, conforme la extensión del acuerdo de juicio abreviado celebrado entre las partes, la de dos (2) años de prisión efectiva.

En cuanto a las expresiones del imputado en la audiencia *de visu* en función de su adicción a la "ludopatía" y su expresa voluntad de someterse a un tratamiento de control relacionado, solicitó que su implementación lo sea por un tiempo prolongado su defensa técnica. Considero al respecto que la "ludopatía" o juego patológico es: una enfermedad, un trastorno mental, una patología compulsiva y progresiva. Esta enfermedad se puede instalar en cualquier persona sea ésta joven, adulto, mayor, hombre o mujer. El juego patológico o ludopatía se caracteriza por la incapacidad de abstenerse y detenerse respecto del juego (*pinball*, máquinas tragamonedas, entre otros juegos de azar). Esta conducta generará una gradual alteración en las diferentes áreas de la vida del individuo: laboral, educativa, familiar, etc.

Advirtiendo que en el marco de las políticas de control de adicciones y de vida saludable que lleva adelante el Gobierno de la Provincia del Chaco, el Ministerio de Salud Pública y Lotería Chaqueña firmaron convenio para la implementación del Programa de Juego Responsable que apunta a la colaboración y al trabajo conjunto entre ambas instituciones para brindar atención a aquellas personas que presenten una patología adictiva, conocida como ludopatía.

El Programa Juego Responsable se implementó para asistir a quienes padezcan adicciones relacionadas al juego. Se trata de un servicio "gratuito y confidencial" que se brinda a través de un equipo profesional multidisciplinario, compuesto por psiquiatras, psicólogos, operadores sociales y terapéuticos, con capacitación específica en la problemática de las adicciones.

El día 13 de septiembre de 2018, el Dr. R. S. I., médico psiquiatra forense del Instituto Médico Forense, examinó a H. M. P. con el siguiente resultado: "se recomienda tratamiento psicoterapéutico para el imputado P., H. M., quien padece de ludopatía, según su propia referencia, en el programa de Juego Responsable de Lotería Chaqueña y/o en el servicio de Salud Mental del Hospital Perrando, con la Dra. E. K.".

En virtud de ello y atento lo manifestado por el imputado en la audiencia *de visu* respecto a su padecimiento de ludopatía, así como el consentimiento brindado para realizar el tratamiento respectivo y el dictamen del médico psiquiatra forense, Dr. R. S. I., corresponde disponer la incorporación de H. M. P. al Programa de Juego Responsable dependiente de Lotería Chaqueña y/o al Servicio de Salud Mental del Hospital Julio C. Perrando, a cuyos efectos ordénese el traslado del mismo a fin de efectuarse la entrevista inicial a la oficina sito en calle Santa Fe ... —piso 2º, oficina 5—, de esta ciudad, o al nosocomio en su Servicio de Salud Mental, tratamiento que se realizará durante el periodo de tiempo que dure su condena con los controles periódicos de su evolución por parte del órgano judicial de ejecución competente.

Todo ello teniendo en cuenta la finalidad de la sanción penal, el principio *pro homine* y la expectativa de que la aplicación del "Programa de Juego Responsable" resulta beneficioso para la vida del imputado comprometido con el tratamiento y su reinserción familiar y social tendiente a la

reflexión de su conducta respetando los derechos de terceras personas.

En cuanto a las costas, H. M. P. deberá oblar la suma de pesos ciento cincuenta (150) en concepto de tasa de justicia, por aplicación de la ley 4182 y sus modificatorias.

Asimismo se regularán honorarios profesionales por la asistencia técnica del imputado en el presente proceso a los Dres. M. A. M. en la suma de pesos ... ($ ...) y G. F. C. en la suma de pesos ... ($ ...), respectivamente, acorde a la calidad, extensión, etapas en las que intervinieron y la labor realizada en el ejercicio de la defensa técnica del imputado. Igualmente en relación al apoderado de la parte querellante, Dr. D. G., en el monto de pesos ... ($ ...), todos a cargo de H. M. P., obligado al pago, a quien se lo intima a abonarlos en el término de diez días de quedar firme la presente. Intimándose a los profesionales a que en el plazo legal efectúen los aportes normados en la Ley de Caja Forense y disposiciones de la Administración Tributaria Provincial (ATP), en el monto proporcional pertinente si correspondiere, bajo apercibimiento de ley, según las pautas regulatorias de los art. 13, 3º y 4º de la ley 2011/76 y sus modificatorias leyes 2385, 3578 y 5532 de Honorarios de Abogados y Procuradores, a cargo de H. M. P., obligado al pago, a quien se lo intima de abonarlos en el término de diez días de quedar firme la presente. Intimándose a los profesionales a que en el plazo legal efectúen los aportes normados en la Ley de Caja Forense y disposiciones de la Administración Tributaria Provincial (ATP), en el monto proporcional pertinente si correspondiere, bajo apercibimiento de ley.

Con respecto al destino de los efectos secuestrados, corresponde disponer el decomiso de los siguientes efectos secuestrados a saber: una (1) libreta tipo cuero, color marrón, con anotaciones varias; un (1) trozo de papel color blanco escrito con tinta azul "*Only use by Mercury Cash December 28th 2017*"; una (1) una tarjeta de débito Visa BBVA Francés; (1) una tarjeta (...) Payments Association MasterCard; (1) una tarjeta Visa del Nuevo Banco del Chaco; (1) una tarjeta MasterCard del Nuevo Banco del Chaco; (1) una tarjeta MasterCard del Nuevo Banco del Chaco; (1) una tarjeta Tuya del Nuevo Banco del Chaco; (1) una tarjeta Visa del Nuevo Banco del Chaco; (1) una tarjeta de débito Maestro del Nuevo Banco del Chaco; (1) una tarjeta de débito Debit Card Visa todos a nombre de H. M. P.; (1) teléfono celular marca Samsung modelo Galaxy A7, año 2017 color dorado, pantalla táctil, IMEI Nº ... Serie Nº ...; (1) disco rígido interno con la capacidad de 1 TB, marca Sergate s/ Nº ..., ST: ...; (1) *router* marca Cisco, color negro, modelo DPC3828D, Wan Mac ..., con su respectivo cargador; por haber sido instrumento del delito, art. 23 primer párrafo del CP, remitiéndose los mismos a Sala de Armas y Efectos Secuestrados.

Restituir al condenado H. M. P. (1) un pasaporte color azul oscuro del Mercosur República Argentina, a nombre de H. M. P.; (2) dos tarjetas de la firma OSDE a nombre de P. S. A. y P. L. M.; y (1) un documento nacional de identidad a nombre de H. M. P.; conforme las previsiones del art. 522, primer párrafo, del CPP, los que se encuentran reservados en Secretaría del Tribunal.

Restituir al señor S. P. (1) *router* color negro, marca Hitron, modelo CGNV2; Cm Mac: ...; Mta Mac: ... con su respectivo cargador, con debida acreditación de propiedad, a cuyo fin remítase el mismo a Sala de Armas y Efectos Secuestrados.

Remitir a la Dirección de Archivo del Poder Judicial, adjunto al presente expediente los siguientes efectos secuestrados: un (1) DVD entregado por M. E. H.; un (1) DVD de la Div. Delitos Tecnológicos conteniendo imágenes de allanamiento; un (1) DVD correspondiente a informe pericial Nº 17/18 del Gabinete Científico del Poder Judicial, los cuales se encuentran reservados en Secretaría del Tribunal.

Por todos los fundamentos expuestos, la Cámara Tercera en lo Criminal, en sala unipersonal falla: I. Condenando a H. M. P., ya filiado, como autor penalmente responsable del delito de "defraudación informática en concurso real con violación de secretos y de la privacidad (acceso ilegítimo a un sistema informático)" (art. 173, inc. 16, art. 153 bis, 2º supuesto, en función del art. 55 y 45 del CP) a la pena de dos (2) años de prisión efectiva. En orden a los hechos respectivamente cometidos entre los días 14 y 16/12/2017, en perjuicio de la empresa "Mercury Cash" y sus clientes, por el que fuera investigado y requerido a juicio por el Equipo Fiscal Nº 13, expte. Nº 17029/2017-1, caratulado: "P., H. M. s/ defraudación informática en concurso real con violación de secretos y de la privacidad", expte. Nº 40134/2017-1, expediente policial: E-21-2017-2142-E, sumario policial: 170-CSPJ/17. II. Revocando la condicionalidad de la pena impuesta por sentencia Nº 41 de fecha 19/05/2017 dictada por el Juzgado Correccional Nº 1 de Resistencia - Chaco. III. Unificando, por composición, la pena impuesta en la presente con la recaída en sentencia Nº 41 de fecha 19/05/2017 dictada por el Juzgado Correccional Nº 1, fijando como pena única la de dos (2) años de prisión efectiva por los delitos de "defraudación informática en concurso real con violación de secretos y de la privacidad (acceso ilegítimo a un sistema informático) en concurso real con lesiones leves calificadas por el vínculo y por haber sido cometidas en un contexto de violencia de género" (arts. 173, inc. 16, 55, 153 bis, 2º supuesto, 55, 89 en función con el 92 y 80, incs. 1º y 11, todo en función del art. 45 del CP). Con costas. IV. Disponiendo la incorporación de H. M. P. al Programa de Juego Responsable dependiente de Lotería Chaqueña, y/o al Servicio de Salud Mental del Hospital Julio C. Perrando, a cuyos efectos ordénese el traslado del mismo a fin de efectuarse la entrevista inicial a la oficina sito en calle Santa Fe Nº ... —piso 2º, oficina 5—, de esta ciudad, y/o al nosocomio en su Servicio de Salud Mental, tratamiento que se realizará durante el periodo de tiempo que dure su condena con los controles periódicos de su evolución por parte del órgano judicial de ejecución competente. V. Imponiendo al condenado H. M. P., el pago de pesos ciento cincuenta ($ 150), en concepto de tasa de justicia, por aplicación de la ley 4182 y sus modificatorias, suma que deberá efectivizar dentro de los cinco (5) días de quedar firme la presente. VI. Regulando los honorarios profesionales según las pautas regulatorias de los arts. 13, 3º y 4º de la ley 2011/76 y sus modificatorias leyes 2385, 3578 y 5532 de Honorarios de Abogados y Procuradores, por la asistencia técnica del imputado en el presente proceso a los Dres. M. A. M. en la suma de pesos ... ($ ...) y G. F. C. en la suma de pesos ... ($ ...) respectivamente; acorde a la calidad, extensión, etapas en las que intervinieron y la labor realizada en defensa del imputado. Igualmente en relación al apoderado de la parte querellante, Dr. D. G., en el monto de pesos ... ($ ...), todos a cargo de H. M. P., obligado al pago, a quien se lo intima de abonarlos en el término de diez días de quedar firme la presente. Intimándose a los profesionales a que en el plazo legal efectúen los aportes normados en la Ley de Caja Forense y disposiciones de la Administración Tributaria Provincial (ATP), en el monto proporcional pertinente si correspondiere, bajo apercibimiento de ley. VII. Decomisando los siguientes efectos secuestrados: una (1) libreta tipo cuero, color marrón, con anotaciones varias; un (1) trozo de papel color blanco escrito con tinta azul "*Only use by Mercury Cash December 28th 2017*"; (1) una tarjeta de débito Visa BBVA Francés; (1) una tarjeta (...) Payments Association MasterCard; (1) una tarjeta Visa del Nuevo Banco del Chaco; (1) una tarjeta MasterCard del Nuevo Banco del Chaco; (1) una tarjeta MasterCard del Nuevo Banco del Chaco; (1) una tarjeta Tuya del Nuevo Banco del Chaco; (1) una tarjeta Visa del Nuevo Banco del Chaco; (1) una tarjeta de débito Maestro del Nuevo Banco del Chaco; (1) una tarjeta de débito Debit Card Visa todos a nombre de H. M. P.; (1) teléfono celular marca Samsung modelo Galaxy A7, año 2017 color dorado, pantalla táctil, IMEI Nº ... Serie Nº ...; (1) disco rígido interno con la capacidad de 1 TB, marca Sergate s/ Nº ..., ST: ...; (1) *router* marca Cisco, color negro, modelo ..., Wan Mac ..., con su respectivo cargador; por haber sido instrumento del delito, art. 23, primer párrafo, del CP, remitiéndose los mismos a Sala de Armas y Efectos Secuestrados. VIII. Restituyendo al condenado H. M. P. de (1) un pasaporte color azul oscuro del Mercosur República Argentina, a nombre de H. M. P.; (2) dos tarjetas de la firma OSDE a nombre de P. S. A. y P. L. M.; y (1) un documento nacional de identidad a nombre de H. M. P.; conforme las previsiones del art. 522, primer párrafo, del CPP, los que se encuentran reservados en Secretaría del Tribunal. IX. Restituyendo, al señor S. P. (1) *router* color negro, marca Hitron, modelo CGNV2; Cm Mac: ...; Mta Mac: ... con su respectivo cargador, con debida acreditación de propiedad, a cuyo fin remítase el mismo a Sala de Armas y Efectos Secuestrados. X. Remitiendo a la dirección de archivo del Poder Judicial, adjunto al presente expediente los siguientes efectos secuestrados: un (1) DVD entregado por M. E. H.; un (1) DVD de la Div. Delitos Tecnológicos conteniendo imágenes de allanamiento; un (1) DVD correspondiente a informe pericial Nº 17/18 del Gabinete Científico del Poder Judicial, los cuales se encuentran reservados en Secretaría del Tribunal. Consentida que fuere la presente, dése cumplimiento a la ley 22.117, comuníquese a la División Antecedentes Personales. Practíquese cómputo de pena. Remítanse antecedentes al Juzgado de Ejecución Penal en turno para la ejecución del fallo. Oportunamente archívense los autos. — *María S. Gutiérrez.*

## EDICTOS

El Juzgado Nacional de Primera Instancia en lo Civil y Comercial Federal Nº 8, secretaría Nº 15, sito en Libertad 731 7º piso de esta ciudad, informa que JUAN ANDRES DUGARTE CAMACHO de nacionalidad venezolana con DNI 95.404.842 ha iniciado los trámites tendientes a obtener la ciudadanía argentina. Por ello cualquier persona que tuviere conocimiento de algún acontecimiento que estimara podría obstar a dicha concesión, deberá hacerlo saber a este Juzgado. Publíquese por dos días.

**Buenos Aires, 27 de diciembre de 2018**

Felipe J. Cortés Funes, sec.

**LA LEY: I. 10/04/19 V. 11/04/19**

---

El Juzgado Nacional de Primera Instancia en lo Civil y Comercial Federal Nº 9, a cargo de la Dra. Alicia Bibiana Pérez (Juez Federal Subrogante), Secretaría Nº 18, sito en Libertad 731, 6to piso, Capital Federal, en los autos caratulados: "TORO VILLARROEL, ISRAEL ALEJANDRO s/SOLICITUD DE CARTA DE CIUDADANÍA", Expte. Nº 2500/2018, hace saber que el solicitante dijo ser chileno, nacido el 11 mayo 1986 en Rancagua, Chile, con DNI 94.689.386. Se publica para que cualquier persona —a través del Ministerio Público— formule objeciones que pudiesen obstar al otorgamiento del beneficio. Publíquese por dos veces en el lapso de 15 días.

**Buenos Aires, 18 de abril de 2018**

Miguel Augusto Álvarez, sec. int.

**LA LEY: I. 10/04/19 V. 10/04/19**

---

El Juzgado Nacional de Primera Instancia en lo Civil y Comercial Federal Nº 8, secretaría Nº 15, sito en Libertad 731 7º piso de esta ciudad, informa que WILLIAN ALEJANDRO ARCAYA RIVAS de nacionalidad venezolana con DNI 95.429.333 ha iniciado los trámites tendientes a obtener la ciudadanía argentina. Por ello cualquier persona que tuviere conocimiento de algún acontecimiento que estimara podría obstar a dicha concesión, deberá hacerlo saber a este Juzgado. Publíquese por dos días.

**Buenos Aires, 20 de febrero de 2019**

Felipe J. Cortés Funes, sec.

**LA LEY: I. 10/04/19 V. 11/04/19**

---

El Juz. Fed. Civ. y Com. Nº 1, Sec. Nº 1 de la Cap. Fed., hace saber que BELKYS MACHIN PEREZ de nacionalidad cubana, DNI 93.606.721, ha solicitado la concesión de la Ciudadanía Argentina. Se deja constancia que deberán publicase por 2 (dos) veces dentro del plazo de quince días en el Diario LA LEY.

**Buenos Aires, 13 de julio de 2017**

Ana Laura Bruno, sec.

**LA LEY: I. 10/04/19 V. 10/04/19**

---

El Juzgado Nacional de 1ra Instancia en lo Civil Nº 109, Secretaría única, comunica por dos días en autos: PASJALIDIS, DIEGO ERNESTO c/GODOY, LAURA ANDREA s/EJECUCIÓN HIPOTECARIA", Expte. 60.446/14, que el Martillero Miguel A. M. Soaje subastará el 16 de abril de 2019 a las 11,30 horas en punto, en la sede de la calle Jean Jaures 545 de esta Ciudad, el inmueble ubicado en la calle Araujo 463/467, entre Ercilla y Ulrico Schmidl, planta baja, Unidad Funcional 3, matrícula FR 1-3317/3, N.C.: C. I, S. 60, M. 73, P. 5, de C.A.B.A.; Partida 1337420; que adeuda: AYSA $ 82,77 al 20/4/15 (fs. 80/1); Aguas Argentinas $ 8.811,31 al 15/4/15 (fs. 124/126); GCBA $ 3.023,10 al 16/4/15 (fs. 88); sin deuda de OSN al 13/4/15 (fs. 83/84); el inmueble no posee administración, y por ende no paga expensas (fs. 115, pto. 3). Del informe del Martillero surge que el inmueble se encuentra ocupado por la Sra. Paula Gómez (DNI 3.227.314) en calidad de inquilina de la propietaria. Se trata de la unidad funcional 3, vivienda identificada como departamento 2 con entrada exclusiva por Araujo 463, ubicada al fondo del pasillo descubierto de ingreso, accediendo a un patio con galería cubierta con un techo de chapa rebatible y plegable, compuesto de un living-comedor, dos dormitorios, baño completo, cocina y patio en el fondo. Todo en regular estado de uso y conservación por falta de mantenimiento y humedad. Esta venta se realiza al contado y al mejor postor, base $ 1.000.000, seña 30%, comisión 3%, sellado de ley (1%) y arancel (Acordada 20/2000) 0,25%, todo en dinero en efectivo en el acto de la subasta, debiendo el comprador constituir domicilio dentro del radio de la Ciudad de Buenos Aires, bajo apercibimiento de dar por notificadas las sucesivas providencias en la forma y oportunidad previstas por el art. 133 del C.P. Rendirá cuentas dentro de tres días de realizado el remate, bajo apercibimiento de multa, debiendo depositar el importe correspondiente en la Sucursal Tribunales de la Nación Argentina, a la orden del Juzgado y como perteneciente a estos autos. Se hace saber que el adquirente en subasta judicial no deberá hacerse cargo de las deudas que registra el bien por impuestos, tasas y contribuciones devengadas antes de la toma de posesión, en caso de que no existiere remanente suficiente. Exhibición: los días 11 y 12 abril de 14,30 a 16,30 horas.

**Buenos Aires, 3 de abril de 2019**

Pilar Fernández Escarguel, sec.

**LA LEY: I. 09/04/19 V. 10/04/19**

---

5511/2016 GARCES SALAS, JESUS DAVID s/SOLICITUD DE CARTA DE CIUDADANIA. El Juzgado Nacional de Primera Instancia en lo Civil y Comercial Federal Nº 3, interinamente a cargo del Dr. José Luis Cassinerio, Secretaría Nº 6, a cargo de la Dra. María Florencia Millara, sito en Libertad 731, piso 4to., de esta ciudad, hace saber que JESUS DAVID GARCES SALAS, D.N.I. Nº 95.136.146, de nacionalidad colombiana ha solicitado la declaración de la "Ciudadanía Argentina". Cualquier persona que conozca algún impedimento para la concesión de dicho beneficio podrá hacerlo saber a través del Ministerio Público, dentro del plazo de quince días. Publíquese por dos días.

**Buenos Aires, 4 de julio de 2018**

María Florencia Millara, sec. fed.

**LA LEY: I. 09/04/19 V. 10/04/19**

---

El Juzgado Nacional de 1ra. Instancia en lo Civil Nº 17 a cargo del Dr. Marcelo Luis Gallo Tagle secretaría Única a cargo de la Dra. Mariel Roxana Gil, sito en Avenida de los Inmigrantes 1950 piso 5to de la Ciudad Autónoma de Buenos Aires, en "PALACIO WALTER RAUL EMIGDIO c/BIANCHI LEONARDO GABRIEL y OTRA s/DAÑOS Y PERJUICIOS" expte. Nro. 93540/2016, ha ordenado la publicación de este edicto por dos días en el diario "La ley", citando a SILVIA ESTER GRUNEWALD y LEONARDO GABRIEL BIANCHI para que dentro del plazo de 15 días comparezcan a estar a derecho bajo apercibimiento de nombrar al Defensor de Pobres y Ausentes para que los represente. Publíquese.

**Buenos Aires, 6 de marzo de 2019**

Mariel Roxana Gil, sec.

**LA LEY: I. 9/04/19 V. 10/04/19**

---

El Juzgado Nacional de Primera Instancia en lo Civil Nº 95 a cargo del Dr. Maximiliano Luis Caia secretaría Única a cargo de la Dra. María Laura Ferrari sito en calle Talcahuano 550 piso 6to de esta Ciudad, en los autos "URQUIZA SERGIO AGUSTIN c/GRAMAJO SERGIO EMMANUEL y OTRO s/DAÑOS Y PERJUICIOS" expediente 86740/2017, cita por quince días a SERGIO EMANUEL GRAMAJO para que comparezca a tomar intervención en autos en los términos de los arts. 338 y 339 del Código Procesal bajo apercibimiento de designar al Defensor Oficial. Publíquese por 2 días en el diario "La Ley".

**Buenos Aires, 14 de marzo de 2019**

María Laura Ferrari, sec.

**LA LEY: I. 09/04/19 V. 10/04/19**

**PROPIEDAD DE LA LEY S.A.E. e I. -** Administración, Comercialización y Redacción: Tucumán 1471 (C. P. 1050 AAC) Teléfono: 54-11-4378-4765 - Bs. As. Rep. Arg. - Registro Nacional de la Propiedad Intelectual Nº 5074180
Impreso en La Ley, Rivadavia 130, Avellaneda, Provincia de Buenos Aires.