Revista de la Facultad de Derecho de México
Tomo LXXI, Número 282, Enero-Mayo 2022
DOI:http://10.22201/fder.24488933e.2022.282.81937

Criptomonedas y delito: apuntes iniciales

Cryptocurrencies and crime: introductory notes

Marcelo A. Riquert*

Resumen: El trabajo pretende ofrecer una inicial reflexión acerca de la vinculación entre las monedas virtuales y el delito que presenta una doble faceta ya que tanto puede facilitar su realización (lavado de activos, financiación del terrorismo, defraudaciones, narcotráfico), como ser su objeto (apropiaciones indebidas). Asimismo, se da noticia de las primeras resoluciones judiciales en Argentina.
Palabras clave: criptomonedas; delito; jurisprudencia; lavado de activos; defraudaciones.

Abstract: The work aims to offer a reflexive approach on the link between virtual currencies and crime that has a double facet since it can both facilitate its realization (money laundering, financing of terrorism, fraud, drug trafficking), as well as its object (appropriations undue). Likewise, news is given of the first judicial decisions in Argentina.
Keywords: cryptocurrencies; crime; jurisprudence; money laundering; fraud.

* Abogado y Doctor en Derecho, UNMDP. Master en Derecho Penal, U. Salamanca (España). Director del Área Departamental Penal, Facultad de Derecho, UNMDP. Ex Presidente de la Asociación Argentina de Profesores de Derecho Penal. Contacto: riquertm@hotmail.com Fecha de recepción: 11/11/2021. Fecha de aprobación: 14/02/2022.

Revista de la Facultad de Derecho de México
Tomo LXXII, Número 282, Enero - Abril 2022
DOI:http://10.22201/fder.24488933e.2022.282.81937

I. Introducción

No parece necesario incursionar en mayores explicaciones acerca de la trascendencia de las modernas tecnologías de la información y comunicación en materia macroeconómica porque, justamente, ya no son tan nuevas y la percepción directa de su influencia modificando prácticamente todos los ámbitos de nuestra vida en sociedad contribuye a evitar tal sobreabundancia. Todos tenemos clara conciencia del pasaje de una economía "analógica" a otra digital o de las constantes modificaciones de tal fenomenología desde una clave microeconómica. Por dar un solo ejemplo, años atrás, los cambios en los modos de comercializar que se fueron imponiendo a partir de ofertas en sitios como "e-Bay", con sistemas de pago como "PayPal". En nuestro medio, la multiplicada presencia de unicornios tecnológicos con "Mercado Pago" a la cabeza.

Entonces, es claro estamos ante un fenómeno que ya no es novedoso y que, además, se ha acelerado producto de las medidas sanitarias que hubo de tomarse en todo el mundo por la pandemia del COVID-19.

Mínimo recordatorio, a comienzos de los noventa Carlo Sarzana apuntaba que el sistema electrónico de transferencias de fondos nos llevaba a una "cashless society" que, para expertos americanos, era una realidad y, por eso, tanto el gobierno como las entidades financieras estaban (y están) fuertemente interesadas en la protección de este sistema. Para fundar el aserto recordaba que el FBI y la CIA en el último semestre de 1985 habían detectado 1400 casos de fraudes graves contra este sistema[1]. Una década después, también desde el ámbito doctrinario italiano, Claudia Pecorella puso de resalto que la difusión de los abusos con tarjetas magnéticas de pago fue un fenómeno que se extendió a la vez que

[1] Sarzana, en su obra *Informatica e diritto penale*, Giuffré Editore, Milano, Italia, 1994, p. 21.

fuera popularizándose el uso de los cajeros automáticos, con las facilidades que aparejaron para poder operar bancariamente fuera del horario de atención tradicional[2].

El impulso hacia el reemplazo de la moneda metálica por las transacciones online es fuertemente incentivado, cuando no impuesto, no sólo desde el ámbito privado sino, en particular, desde el público. Así, da cuenta Faustino Gudín Rodríguez-Magariños que, en diciembre de 2012, el Consejo Italiano de Ministros votó afirmativamente el aumento del control de capital mediante la prohibición del uso de dinero efectivo en transacciones de más de mil euros, lo que al año siguiente se agudizó, limitando los pagos en metálico a 50 euros[3]. En síntesis, el dinero papel viene siendo suplantado intensamente por el dinero electrónico al punto que usar el primero empieza a considerarse indicio serio de delito (por ej., de evasión a la hacienda pública) o de su procedencia de origen delictivo (y el consecuente destino de "lavado" para su reincorporación a la economía formal). Esto sin que, a su vez, pase por alto las dificultades de control que pueden ofrecer los medios electrónicos de pago[4] o las consecuencias que podrían derivarse de una "caída" del sistema.

Más reciente, no puede dejar de advertirse la presencia que en la economía mundial y también en lo relativo a las defraudaciones y otros delitos como el lavado de activos o la financiación del

---

[2] Pecorella, en su obra *Il diritto penale dell'informatica*, CEDAM, Padova, 2000, p. 46.

[3] En su trabajo "La nueva era del dinero virtual y los nuevos tipos penales patrimoniales: Skimming, Carding, Phishing y Pharming", pub. en Donna, E.A. (dir.), *Revista de Derecho Penal*, Rubinzal-Culzoni editores, Buenos Aires/Sta. Fe, Tomo 2014-1 "Derecho Penal de los Negocios y de la Empresa – II", p. 245.

[4] Expone su inquietud Patricio N. Sabadini en su ponencia "Modernidad y crisis del Estado-Nación en la sociedad de riesgo. Una especial referencia a la seguridad en las nuevas tecnologías", pub. en AAVV "Informática y Delito", Infojus/AIDP Grupo Argentino, Buenos Aires, 2014, pp. 256-257.

DOI:http://10.22201/fder.24488933e.2022.282.81937

terrorismo han adquirido las criptomonedas o monedas virtuales, cuyo surgimiento se remonta hasta hace apenas poco más de un década (2009), con la aparición de la más popular, Bitcoin, luego de la que se desarrollaron muchas más (centenares en realidad), como Ethereum[5], Ripple, Litecoin o Dogecoin[6]. Como indica Carolina Vanella estamos frente a productos complejos y volátiles,

[5] Sebastián Campanario señala que "ethereum" es la moneda virtual elegida por el municipio de Bahía Blanca para pagar subsidios culturales a músicos, pintores y otros artistas en el marco de un "contrato inteligente" que buscará darle más trasparencia sobre lo que cobrarán. Similares iniciativas se han registrado en Varsovia con "Userfeeds" y en USA con el "proyecto UJO", en procura de que los derechos de cantantes y compositores les lleguen directamente desde los consumidores, evitando la intermediación de plataformas como "Spotify" (en su nota "Criptomarketing. Monedas virtuales en el mundo del entretenimiento", pub. en diario *La Nación*, edición del sábado 28 de octubre de 2017, sección "Sábado", p. 9).

[6] La creación misma de Bitcoin está rodeada de misterio: para algunos fue obra de Craig Steven Wright (cf. María Belén Linares, en su trabajo "El uso de Bitcoins para lavar activos. Aproximación a una técnica delictiva", pub., Riquert, M.A. (dir.), Sueiro, C.C. (coord.), *Sistema Penal e Informática*, ed. Hammurabi, Buenos Aires, 2019, p. 136, nota al pie núm. 1). Otras fuentes indican que se debe a Satoshi Nakamoto. Así, Ezequiel Sallis, quien a inicios de 2017 señalaba que en ese momento ya existían aproximadamente unas 739 criptomonedas, enorme desarrollo si se atiende a que "bitcoin" fue creada y puesta a funcionar por Satoshi Nakamoto el 3 de enero de 2009 y que la primera transacción por un ítem físico utilizando bitcoins fue el 22 de mayo de 2010: una pizza en New York en momentos en que el cambio de bitcoins era de un bitcoin equivalente a 25 dólares (cf. su trabajo "Desafíos de la investigación de los delitos informáticos en la Deep & Dark Web", pub. en Dupuy, Daniela (dir.) Kiefer, Mariana (coord.), *Cibercrimen*, ed. BdeF, Buenos Aires/Montevideo, 2017, p. 611). En enero de 2017 un bitcoin valía 4000 dólares. Al momento de escribir estas líneas, fines de 2021, la cotización llegó hasta los 60.000 dólares por bitcoin. Finalmente, tampoco faltan quienes ponen en duda que Nakamoto exista, sino que sería un nombre de fantasía usado por un

que representan riesgos para su consumidor/inversor, que se justifican en los beneficios que con ellos se busca provocar, como llegar a los sectores no bancarizados, otorgar liquidez o activar el mercado, entre otros[7]. Ello, además de lo que para muchos operadores son las ventajas derivadas de la descentralización del sistema (se pueden hacer pagos internacionales entre privados sin la mediación de una autoridad central bancaria validándolo), con bajos costes (por eliminación aquella burocracia y la posibilidad de pactar comisiones bajas o incluso prescindir de ellas), la rapidez y flexibilidad de los horarios para las operaciones y la confidencialidad con que se efectúan, lo que deriva junto con la promesa/expectativa de alta rentabilidad en que haya un incentivo importante para querer invertir en criptoactivos.

II. Las monedas virtuales y su funcionalidad para el delito

Puede de inicio apuntarse que, si nos referimos al campo de lo penal, han proliferado trabajos que destacan su funcionalidad para servir a la concreción de distintas maniobras delictivas deriva de sus características definitorias. En tren de justificar el aserto, baste destacar que al realizarse las veloces transacciones por direcciones y no por personas, media una suerte de anonimato que facilita actividades como el lavado de activos de origen delictivo[8] (en nuestro Código Penal (CP), art. 303, que en lo básico pena al que "(…)

grupo de personas (tal la versión que informa "Wikipedia", puede consultarse en https://es.wikipedia.org/wiki/Satoshi_Nakamoto).

[7] Vanella, Carolina, "Los avatares del negocio con critomonedas y el peligro de estafa", pub. en *Erreius online*, ed. Erreius, Buenos Aires, setiembre de 2021, punto V. Disponible en <https://ius.errepar.com/sitios/ver/html/20210902102513352.html?k=criptomonedas%20y%20criminalidad>.

[8] Cfr. Linares, en "El uso…", *op. cit.*, pp. 142-146, donde explica la modalidad que puede asumir la maniobra delictiva en concreto.

convirtiere, transfiriere, administrare, vendiere, gravare, disimulare o de cualquier otro modo pusiere en circulación en el mercado, bienes provenientes de un ilícito penal, con la consecuencia posible de que el origen de los bienes originarios o los subrogantes adquieran la apariencia de un origen lícito (…)"[9]). Como apuntan Parma, Mangiafico y Álvarez Doyle, en síntesis, las actividades de lavado consisten en transformar bienes provenientes de un ilícito penal y darle apariencia lícita, siendo la consagración de este tipo penal una manifestación del objetivo político-criminal del Estado de controlar el flujo de fondos y financiamiento de actividades delictivas variadas y comúnmente asociadas a la existencia de estructuras de criminalidad organizada[10].

Gabriela Ulas recuerda como "leading cases" en materia de blanqueo de activos usando monedas virtuales a los que fueron periodísticamente conocidos como "The Silk Road" y "Liberty Reserve SA", ambos de comienzos de la década pasada. Sin necesidad de ingresar en detalle, la nombrada propone justamente en el marco del *"compliance criminal"* la elaboración de un manual de procedimientos para operaciones con criptomonedas[11].

Esta facilidad, además, se indica concreta en particular por su uso en la llamada "red profunda" ("deep web"[12]), a la que se accede

---

[9] He comentado dicha norma en Riquert, M.A. (dir.) *Código Penal de la Nación. Comentado y Anotado*, ed. Erreius, Buenos Aires, 2018, t. III (Artículos 186 a 316), pp. 2283-2294.

[10] Cfr. Parma, Carlos, Mangiafico, David y Álvarez Doyle, Daniel, *Derecho Penal. Parte Especial*, Hammurabi, Buenos Aires, 2019, pp. 744-745.

[11] Ulas, "Lavado de activos y criptomonedas: en busca de un compliance eficiente", pub. Riquert, M.A. (dir.) y Sueiro, C.C. (coord.), *Sistema Penal e Informática*, ed. Hammurabi, Bs.As., núm. 4, 2021, pp. 208-210.

[12] Por oposición a lo que sería la red tradicional que, entonces, consistiría en la "superficial" o "clear web", apuntando a la transparencia o claridad de su navegación carente de anonimato. Diego F. Migliorisi refiere a la deep web como otro de los canales de ciberespacio que es utilizado por los delincuentes informáticos, definiéndola como una suerte de sub-red de redes que por su

mediante software especializado en garantizar el anonimato de los usuarios (como es "TOR"[13]), lo que la transforma en el vehículo ideal para canalizar operaciones ilegales por la criminalidad organizada[14]. Esto último es destacado en el sitio web oficial de "In-

---

estructura informática no forma parte de la internet superficial, ni las páginas que la integran –que en general tienen contenidos ilegales- están indexadas por los motores de búsqueda (en su trabajo titulado "La problemática del cibercrimen", pub. en AAVV, *Informática y delito*, INFOJUS, Buenos Aires, 2014, p. 272.

[13] Se trata de la sigla correspondiente a "The Onion Router", proyecto cuyo fin es desarrollar una red de distribución de comunicaciones de baja latencia y superpuesta sobre internet a través de la que el encaminamiento de los mensajes intercambiados entre los usuarios anonimizados al no revelar su dirección IP, manteniendo además la integridad y el secreto de la información que viaja por ella. Como indica Ezequiel Sallis, el proyecto TOR surge en 2003 y en la actualidad lo usan millones de usuarios en todo el mundo como herramienta de acceso a internet (www.torproject.org), aunque hay otras herramientas de este tipo disponibles como L2P2, I2P, Freenet o TOX (cfr. *op. cit*, pp. 604 y ss., donde puede ampliarse sobre el particular).

[14] Así, María Verónica Díaz, en su ponencia "Incidencia de las criptomonedas en los delitos económicos. Transversalidad con la Deep Web", presentada y premiada durante el XVII Encuentro Argentino de Profesores de Derecho Penal-VII Jornadas Nacionales de Derecho Penal, organizado por la Asociación Argentina de Profesores de Derecho Penal y la Facultad de Derecho de la Universidad Nacional de Córdoba, celebrado en sede de la última el 14 y 15 de setiembre de 2017. Ccte.: Daniel Montero Zendejas, quien sostiene la existencia de una cibercriminalidad económica que se suma a una delincuencia organizada transnacional para llevar a cabo el blanqueo de capitales favorecidas por una moneda virtual como bitcoin (en su trabajo "La regulación digital frente a la cibercriminalidad económica. El reto de nuestro tiempo", pub. en Donna, E.A. (dir.), *Revista de Derecho Penal. Derecho Penal Económico*, Rubinzal-Culzoni editores, Buenos Aires/Santa Fe, Tomo 2017-1 "Delitos contra el orden económico y financiero (Título XIII del Código Penal)-V", p. 86).
El tema de las implicancias del anonimato en la red y el uso del software que

terpol" (que cuenta con un equipo especial sobre "Red Oscura y Criptomonedas"), donde se noticia que como institución colaboradora del proyecto "Titanium", financiado por la Unión Europea, ha participado en el desarrollo de "GraphSense", una herramienta de análisis de cadenas de bloques que permite rastrear las transacciones realizadas con criptomonedas. También están desarrollando otra herramienta analítica denominada "Darkweb Monitor" para recopilar datos cuyo posterior análisis permita identificar nuevas tendencias y recomendar actividades de prevención[15].

Otro aspecto que resulta decisivo es que para operar con criptomonedas solo se necesita habilitar un "monedero o billetera virtual" para su administración, sin que medien impedimentos vinculados a fronteras ni días u horas para negociar. La billetera puede consultarse sin necesidad de conexión con internet (offline, modalidad de "almacenamiento en frío"), lo que minimiza la posibilidad de robos informáticos, circunstancia que por contraposición se habilita y potencia cuando opera "online" (modalidad de "almacenamiento en caliente"), riesgo que se procura reducir a partir del uso de la criptografía de datos (como el caso del citado TOR) y uso de mezcladores para encubrir la personalidad del usuario (como Bixtmixer), dando anonimato a las transacciones[16].

Sin embargo, adviértase que la explicación precedente lleva ínsita la exteriorización de otra faceta: las monedas virtuales tie-

---

garantiza el anonimato, como TOR, desde una perspectiva positiva, como posible garante de la libre expresión en contexto de opresión política, lo hemos expuesto una década atrás, en la obra *Crisis Penal. Política criminal, globalización y derecho penal*, prol. Carlos J. Lascano, ed. Ediar, Buenos Aires, 2007.

15 Fuente: nota "La red oscura y las criptomonedas" (consultada el 4/11/2021), se aclara que entre los datos que se pretende recabar están las direcciones de las criptomonedas, claves PGP, direcciones IP, nombres de usuario y alias, direcciones electrónicas, dominios de los mercados de la red oscura, foros de la red oscura e historial de datos recopilados en la dark web desde 2015. Disponible en: <https://www.interpol.int/es/Como-trabajamos/Innovacion/La-red-oscura-y-las-criptomonedas>.

16 Cfr. Ulas, *op. cit*, p. 207.

nen un alto valor económico y esto las torna activos de interés como objeto de delitos patrimoniales que, por su naturaleza digital, se perpetrarán en forma de ataques a los sistemas informáticos de sus tenedores, sean empresas o individuos, con el objeto de tomar el control del sistema y transferir tales bienes digitales a cuentas de los apropiadores[17]. Entonces, no se trata solo de que las criptomonedas sean funcionales para perpetrar algunos delitos, sino que también son un codiciado objeto para ilícitas apropiaciones[18].

A nuestro propósito expositivo alcanza entonces con señalar que el de las criptomonedas es un sistema de intercambio basado en una unidad de medida o valor asignada por el propio mercado que la usa; no están reguladas por intermediarios; el sistema es descentralizado (un soporte digital sobre una base de datos distribuida entre los operarios con uso de criptografía y anonimato para ofrecer seguridad básica) y son independientes de la banca oficial. Se articulan sobre un sistema operativo P2P de código

---

17 Cfr. Chomczyk y Palazzi, "Primer caso argentino sobre 'apropición' de criptomonedas", pub. en *Checkpoint,* Ed. Thomson Reuters, Buenos Aires, p. 1; versión digital disponible en <https://economicas.unsa.edu.ar/afinan/afe_2/material_de_estudio/material/Primer%20caso%20argentino%20sobre%20apropiacion%20de%20criptomonedas.pdf>.

18 Chomczyk y Palazzi señalan que el primer caso conocido de apropiación de criptomonedas de repercusión internacional fue el ataque a "Mt. Gox", un exchange japonés, que involucró más de medio millón de bitcoins, en ese momento equivalente a más de 368 millones de dólares y dejó decenas de miles de perjudicados por todo el mundo (antes citados, p. 5, punto II.3). Puede agregarse que, al momento de la consecuente declaración de quiebra (el 24 de febrero de 2014 suspendió actividades), Mt. Gox concentraba el 70% del mercado de bitcoins (fuente: noticia titulada "Mark Karpelès: ¿Mt Gox fue un robo o un gran fraude?", pub. en el sitio *Criptonoticias*, disponible en <https://www.criptonoticias.com/seguridad-bitcoin/mark-karpeles-mt-gox-robo-fraude/> (28/04/2019)

DOI:http://10.22201/fder.24488933e.2022.282.81937

abierto y base de datos en cadena de bloques (blockchain[19]). De allí que se distingan dos tipos de usuarios, los "normales" y los "mineros". Mientras que los usuarios normales son los que compran y pagan bienes y servicios utilizando bitcoins (o la moneda virtual de que se trate), es decir, produciendo transacciones en el sistema, los llamados "mineros" son usuarios especiales, los que se dedican a validar nuevas transacciones creando bloques de estas[20].

Atendiendo a estas características Blanco Cordero ha definido al bitcoin (pero se trata de un concepto extensible a las demás monedas virtuales) como una unidad de cuenta compuesta de cadenas únicas de números y letras que constituye unidad de moneda y que tiene valor únicamente porque sus usuarios están dispuestos

---

19 La tecnología blockchain opera como una suerte de notario público, compartido por todos los usuarios, no modificable, de todo el sistema de transacciones. Evita que pueda falsificarse y da certeza a los pagos. Es inmutable y permanente. Hay una validación global por operadores con hardware especializado: para atacar el sistema se necesita el 51% del poder validador internacional. Siendo esto casi imposible, es lo que garantiza la seguridad del sistema.

Chomczyk y Palazzi (ya citados, p. 1, punto II) señalan que, simplificando, puede definirse a una blockchain como una base de datos mantenida a través de una red pública de servidores distribuidos por todo el mundo, que no confían entre sí para mantener un registro ordenado de movimientos de unidades, pero sí confían en las reglas fijadas por el software que usan para mantener funcionando esa red. El incentivo para participar en el mantenimiento de la red pública es la asignación por el software de nuevas unidades y comisiones. A las unidades que son registradas por una blockchain se las conoce como "token" y los hay de tres grandes categorías: 1) de pago o criptomonedas (se comportan como un medio de pago e imitan el comportamiento del dinero, ej: bitcoin); 2) de utilidad (empleados para los servicios asociados a las funcionalidades de una determinada moneda, ej.: ether); 3) de valores negociables (buscan replicar el funcionamiento de los valores negociables en el mundo de las blockchain, colectan fondos y representan una participación en un proyecto determinado, ej.: ICO).

20 Cfr. Ulas, *op. cit.*, p. 206.

a pagar por ella[21]. En orden a esto último, téngase presente que, como puntualiza Gabriela Ulas, el valor es muy volátil y se calcula a través de un algoritmo que mide la cantidad de movimientos y transacciones con bitcoin en tiempo real; el límite de emisión fue fijado en 21 millones de monedas (se lo alcanzaría probablemente en el año 2140), lo que provocaría que la moneda no se desvalorice ya que este tope emisivo provocaría una suerte de tendencia al alza permanente y, por lo tanto, mantendría constante el interés de los inversores[22].

III. Entre fraudes, pedidos de regulación y prohibiciones

En el marco expuesto, se observa hoy que median pedidos de regulación del mercado de criptomonedas y se verifican situaciones totalmente contrapuestas, mientras El Salvador se ha transformado en el primer país del mundo que les ha dado curso legal[23], en Turquía, luego de varios fraudes gigantescos en abril de 2021 (Thodex[24] y Vebitcoin[25]) se prohibieron las criptomonedas a partir

21 Cfr. M.B. Linares, en *"El uso…"*, *op. cit.*, p. 136.

22 Ulas, *op. cit*, pp. 206-207.

23 Fuente: noticia publicada el 7/9/21 en el sitio web oficial en español de la BBC con el título *"Bitcoin: El Salvador se convierte este martes en el primer país del mundo en adoptar la criptomoneda como divisa de curso legal"*. Disponible en <https://www.bbc.com/mundo/noticias-america-latina-58441561>.

24 Thodex es una plataforma de criptomonedas con base en Turquía y, a mediados de abril de 2021, frenó sus operaciones mientras su CEO huía a Albania. Se afectaron los activos de 390.000 usuarios involucrando 4.000.000 de dogecoins (con un valor equivalente a unos 2000 millones de dólares). En el operativo judicial/policial se detuvieron a 70 empleados. La empresa alegó ser víctima de un incidente de piratería informática.

25 Vebitcoin es una casa de cambios de criptomonedas con sede en Turquís que a mediados de abril de 2021, como consecuencia del fraude "Thodex",

del 1° de mayo pasado[26]. Similar decisión adoptó el Banco Central de China, en el marco de una serie medidas enérgicas contra las actividades ilegales de comercio de criptomonedas, prohibiendo que las bolsas extranjeras brinden servicios a inversores de China continental a través de Internet. También prohibirá a las instituciones financieras, las empresas de pago y las empresas de Internet facilitar el comercio de criptomonedas, y fortalecerá el monitoreo de los riesgos de tales actividades. En su comunicado, la autoridad bancaria señaló que "Todas las criptomonedas, incluidas Bitcoin y Ether, no son moneda fiduciaria y no pueden circular en el mercado", subrayando que "Ponen en peligro seriamente los haberes de la gente"[27].

En cuanto a las defraudaciones más comunes con criptomonedas (en general, suele servir de "anzuelo" que se ofrece una renta del 8 a 15% mensual), se concretan básicamente a través de casas de cambio falsas, grandes estafas piramidales (clásicos "esquemas de Ponzi"), ofrecimiento de criptomonedas falsas[28], así como variantes que incluyen cartas nigerianas y uso de malware. En orden

---

sufrió retiros masivos de fondos (operaba unos 60 millones de dólares diarios, 50% en bitcoins), dejando una importante cantidad de inversores sin poder recuperar su dinero.

[26] Fuente: noticia publicada el 16/4/21 en la versión virtual del diario "Ámbito Financiero" con el título *"Turquía prohíbe las criptomonedas y golpea a Bitcoin, que cae 4% hasta los u$s60.000"*. Disponible en: <https://www.ambito.com/negocios/bitcoin/turquia-prohibe-las-criptomonedas-y-golpea-que-cae-4-los-us60000-n5184955>.

[27] Fuente: noticia publicada el 24/09/21 en el periódico virtual "El Marplatense", con el título *"El Banco Central de China declaró ilegales todas las transacciones con criptomonedas"*, disponible en: <https://elmarplatense.com/2021/09/24/el-banco-central-de-china-declaro-ilegales-todas-las-transacciones-con-criptomonedas/>.

[28] Un argumento usual es señalar al eventual inversor que ya es tarde para invertir en Bitcoin y, por eso, se ofrece otra moneda alternativa como "Onecoin", con la que se perpetró una estafa valuada en 500 millones de euros.

a las primeras, mínima expresión de la dimensión que pueden alcanzar, en 2019 fueron el 92% de los casos e involucraron 4300 millones de dólares. La mayor ha sido la de la firma "Plustoken", con sede en la isla Vanuatu (microestado de 1750 km2 en Oceanía, compuesto por 83 islas e islotes de los que sólo 1/3 está habitado, su capital es Port Vila, que concentra la mayoría de los 300.000 habitantes del archipiélago), que dejó 3 millones de damnificados. En España, el 26/5/21 la Audiencia Nacional abrió la investigación de una estafa piramidal en criptomonedas: el caso "Arbistar 2.0 SL". En principio, se individualizaron 1127 damnificados por un importe de unos 4 millones de euros. Se proyectaba a partir del avance de la investigación que habría unos 32.000 perjudicados por un total de 100 millones de euros.

En cuanto al uso de malware, tampoco es difícil encontrar algún ejemplo. Recientemente, la empresa de ciberseguridad ESET puso en alerta a la comunidad informática luego de que se detectara una aplicación falsa que, bajo la promesa de realizar criptominado, distribuye un virus que permite robar información personal y espiar a los usuarios. La compañía explicó que se trata de un malware que ingresa a los teléfonos por medio de una falsa app a través de la plataforma "Discord" que atrae a los usuarios con la promesa de minar la criptomoneda "Safemoon"[29].

Claro está que muy distinta es la situación en la que, sencillamente, la inversión en criptomonedas no tuvo el resultado esperado por los inversores participantes. Así se notició lo entendió la Sala V de la Cámara Nacional en lo Criminal (jueces Hernán

[29] Fuente: noticia publicada en el diario Ámbito, edición digital del día 28/9/21 con el título "La peligrosa aplicación que roba información y que los expertos recomiendan desinstalar". Disponible en <https://www.ambito.com/tecnologia/virus/la-peligrosa-aplicacion-que-roba-informacion-y-que-los-expertos-recomiendan-desinstalar-n5288785>.

López y Ricardo Pinto), en resolución del 2/6/2021, cf. art. 336 inc. 3° del CPPN[30], confirmando el decisorio de primera instancia.

Comentándolo, señala Carolina Vanella que la denuncia se formuló el 17/04/2019 por quien mantenía un vínculo social con el denunciado, que es quien lo acercó al negocio de las criptomonedas ya que conocía un "trader" que ofrecía una rentabilidad bimestral, proponiéndole participar del negocio de compra de bitcoins, diciéndole que no era riesgoso y que él respondería si mediara alguna contingencia, aportando quien luego fuera querellante dinero en dólares estadounidenses en varias ocasiones hasta febrero de 2019. El imputado no le devolvió la rentabilidad pactada bajo diversas excusas hasta que cesó el contacto y, por eso, acumuló una deuda que según el querellante ascendió a 86.800 dólares[31].

En lo medular, la Cámara señaló que no se vislumbró la existencia de un ardid o engaño para inducir al querellante en error y lograr así una disposición patrimonial perjudicial de su parte, sobre todo teniendo en cuenta el riesgo propio de la actividad comercial emprendida por ambas partes. Se destacó que el denunciante sabía con quién operaba, que era alguien inscripto en dos plataformas de intercambio de criptomonedas con las que había registrado catorce operaciones, lo que descartaba una artimaña sobre este tópico. La conclusión del tribunal fue que *"no se aprecia en el caso un supuesto con aristas delictivas… sino una inversión con alto riesgo dado por su carácter virtual y la falta de regulación legal"*, que se trató de un actuar voluntario guiado por la ganancia del negocio que impidió estimar la presencia de una modalidad fraudulenta[32]. Creo que lleva razón la comentarista cuando apunta que la intromisión penal en los negocios de estructura especulativa no puede olvidarse el principio pro-

30 La resolución fue en causa "G.T. s/Estafa", disponible en *Erreius on line*, ref.: IUSJU006060F. La referencia periodística corresponde a la noticia publicada en el diario "Ámbito", edición digital del 11/06/2021, titulada "Para la justicia, las criptomonedas no son una estafa", disponible en: <https://www.ambito.com/economia/criptomonedas/para-la-justicia-las-no-son-una-estafa-n5200305>.

31 Vanella, en "Los avatares…", punto II.

32 Cfr. Vanella, *op. cit.*, punto IV.

pio de "mínima intervención", que debe ser defendido singularmente en este tipo de casos[33].

IV. Consideración legal en Argentina

En cuanto a la consideración legal de las criptomonedas en nuestro país, si bien se comportan como monedas, no puede considerárselas tales en sentido jurídico en tanto no se ajustan al art. 30 de la Carta Orgánica del Banco Central de la República Argentina (BCRA), de allí que –como destacan Chomczyk y Palazzi- escapan a la normativa de tal autoridad central relacionada con el mercado único y libre de cambios y la necesidad de cursar las operaciones de compraventa derivadas. Al presente, 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. Lo que resulta incuestionable es que tienen un valor patrimonial para quien las posee y, por eso, forman parte de su patrimonio. De allí que concluyan los nombrados que se trata de bienes (arts. 15 y 16 del Código Civil y Comercial de la Nación CCyCN), de carácter patrimonial con soporte inmaterial, creado por un sistema informático, de emisión privada y que suele utilizarse como medio de pago o intercambio. Por eso, atendiendo a su naturaleza, son factibles de estar involucradas en los delitos clásicos contra la propiedad que prevé el CP[34].

---

33 Cfr. Vanella, *op. cit.*, punto X.

34 Ya citados, págs. 2/3, puntos II.2. y II.3. Brindan varios ejemplos, como el acceso no autorizado a la billetera virtual de la víctima (que tipificaría en el art. 153 bis del CP), apropiarse de las criptomonedas, cambiar claves, excluir al titular (posibles infracciones a los arts. 162, 172 o 173, idem), desencriptar archivos a cambio de pago (art. 183, 2do. párr., ibídem) o requerirlo para volver a acceder (extorsión del art. 168).

A) Algunas referencias generales

En mayo de 2014, el citado BCRA había emitido un comunicado en el que alertaba al público respecto de los riesgos que involucra el uso" de las monedas virtuales. En particular, destacó que las monedas virtuales *"no son emitidas por este Banco Central ni por otras autoridades monetarias internacionales, por ende, no tienen curso legal ni poseen respaldo alguno"*. Asimismo, en cuanto a su valor, destacó que *"no existen mecanismos gubernamentales que garanticen su valor oficial"* y se puso de relieve que *"Las llamadas monedas virtuales han revelado una gran volatilidad hasta el momento, experimentado veloces y sustanciales variaciones de precios"*[35]. Al mes siguiente, la Unidad de Información Financiera (UIF), en su Res. 300/14 alertó sobre el riesgo de lavado y financiación del terrorismo por la dificultad que reviste la trazabilidad nominativa de las operaciones. Además, se indicó que siendo un fenómeno de operaciones interjurisdiccionales, pueden involucrar a otras que no tienen controles de prevención (como las "Recomendaciones" del GAFI) y, por lo tanto, dificultan que los obligados a informar detecten las operaciones sospechosas y puedan emitir los respectivos reportes (ROS).

Para diciembre de 2017 la Comisión Nacional de Valores (CNV), en lugar de una resolución, se limitó a emitir un comunicado de prensa advirtiendo a los inversores destacando el avance de las ofertas iniciales de monedas virtuales (ICO: Initial Coin Offering) y definió a las ICO como la forma de recaudar fondos del público a través de la oferta inicial de monedas virtuales o tokens, mencionando una serie de riesgos, entre los que uno de los más significativos es la falta de una regulación específica. No

[35] Fuente: noticia publicada el 28 de mayo de 2014 en el sitio *Infotechnology*, titulada "El Banco Central argentino considera riesgoso operar con bitcoins". Disponible en: <https://www.infotechnology.com/internet/El-Banco-Central-argentino-considera-riesgoso-operar-con-bitcoins-20140528-0003.html>.

obstante dejó abierta una puerta al señalar que, de existir solicitudes de oferta pública, la CNV podría evaluar la pertinencia del otorgamiento de autorización[36].

No obstante todas estas prevenciones, en 2017, por vía de la Ley 27430 se ha dispuesto que las rentas provenientes de las monedas virtuales queden gravadas con el impuesto a las ganancias. Conforme su reglamentación, aclara Ferrero, se paga el 5% de las ganancias derivadas de inversiones que se realicen en moneda nacional sin cláusula de ajuste y 15% por las utilidades acumuladas en moneda extranjera o en moneda nacional con cláusula de ajuste, equiparándolas a títulos públicos y obligaciones negociables[37]. Entiende asimismo el nombrado que, por vía de una interpretación global del funcionamiento del sistema impositivo argentino, también alcanzaría a las monedas virtuales el impuesto a los bienes personales[38].

Alrededor de un año atrás, el 11/11/20, ha ingresado a la HCD el primer proyecto de *"Ley Regulatoria de Transacciones y Operaciones civiles y comerciales de Criptoactivos"*. Vanella refiere que habría otros dos proyectos más en danza (uno de julio de 2021[39]) y que habría anuencia entre oficialismo y oposición en avanzar con la idea de que la "Autoridad de Aplicación" en materia "cripto" sea la Comisión Nacional de Valores (CNV), siendo las cuestiones

---

36 Cfr. Ferrero, Mariano, "Regulación legal de las monedas virtuales en la Argentina", Camps, Carlos E. (coord.) y Quadri, Gabriel H. (ed.) *Derecho, Innovación y Tecnología*, ed. Erreius, Buenos Aires, 2020, p. 179.

37 *Ibidem*, p. 180.

38 *Ibidem*, p. 182.

39 Se indica que se trataría de habilitar que los trabajadores que prestan servicios en el exterior puedan elegir el cobro total o parcial de sus salarios en bitcoins, ya que no se les considera divisas extranjeras. Se buscaría con ello ofrecer un mecanismo moderno para conservar el poder adquisitivo del salario frente al acuciante problema inflacionario. Se trata de una iniciativa minoritaria que difícilmente pueda prosperar (Vanella, *op. cit.*, punto X y nota al pie número 24).

centrales planteadas la protección del consumidor, la prevención del fraude y otros delitos, la promoción de la competencia privada con una regulación clara y la innovación tecnológica para fomentar beneficios privados y sociales[40].

Es decir, puede advertirse se avanza en el sentido que, pocos años atrás, propiciaba Linares, cuando sostuvo que "El Estado no puede ignorar la existencia de la BTC, debe reaccionar y esforzarse, sin sofocar la innovación, en comprender su funcionamiento y adoptar las medidas orientadas a mitigar los riesgos de lavado de activos que puedan asociarse a su uso"[41].

No hay dudas que es el camino a seguir cuando las criptomonedas continúan popularizándose a partir de una intensa campaña de difusión que incluye propaganda en los más diversos medios y se multiplican los operadores que las ofrecen como modalidad de inversión[42]. Incluso es notable cómo se multiplica su aceptación y facilita su uso en redes sociales. Así, recientemente "Twitter" informó que permitirá a los usuarios enviar y recibir propinas utilizando bitcoin como parte de un impulso más amplio para ayudarlos a ganar dinero con el servicio. Se indicó, además, que la empresa está estudiando la posibilidad de autenticar los "tokens no fungibles" de los usuarios (NFT, por sus siglas en inglés), es decir, bienes digitales que van desde obras de arte hasta las más diversas imágenes digitales. Se hace notar que algunos usuarios ya exhiben sus NFT en sus perfiles, pero no hay una manera fácil de autenticar si la persona que muestra una imagen realmente es dueña de ella[43].

---

40 Cfr. Vanella, *op.cit.*, punto X.

41 Linares, en *"El uso…"*, *op. cit.*, p. 148.

42 Son muchos los operadores nacionales, pudiéndose mencionar entre los más populares a Ripio, Satoshi Tango o Binance.

43 Fuente: noticia en *Perfil*, versión digital, tomada de *Bloomberg* y disponible desde el 24/9/21, con el título "Twitter abre las propinas para todos y permite pagos en bitcóin". Consultarse en <https://www.perfil.com/noticias/

Otro ejemplo de inserción, Mastercard anunció que facilitará que los bancos ofrezcan recompensas en criptomonedas con sus tarjetas de crédito y débito como parte de la reciente adopción de las monedas digitales por parte de la red de pagos. Firmó un acuerdo con Bakkt, la empresa de criptomonedas que se separó de Intercontinental Exchange a principios de 2021. Mastercard también facilitará que los consumidores gasten en criptomonedas las recompensas que obtienen a través de los millones de minoristas en la red de la empresa[44].

B) Primeras repercusiones en la jurisprudencia penal

Según fuera anticipando, aunque todavía ciertamente escasa, ya comienza a advertirse la llegada de la fenomenología delictiva vinculada a las criptomonedas a nuestros tribunales. Ya referimos un caso reciente en el que se negó la pretensión de la querella de haber sido estafada (causa *"G.T. s/Estafa"*, res. de la Sala V de la CNCyCorr.), en lo que sigue se presentarán sintéticamente otros en los que mediaron sentencia condenatoria o, al menos, procesamiento.

Chomczyk y Palazzi refieren el primer fallo condenatorio por apropiación de moneda virtual, sentencia del 21/11/2018 de la Sala III de la Cámara Tercera en lo Criminal de la provincia de Chaco, causa *"P., H.M. s/defraudación informática en concurso real con violación de secretos y de la privacidad"*, que impuso tras un juicio abreviado la pena de dos años de prisión de efectivo cumplimiento por infracción a los arts. 173 inc. 16, 153bis 2°

---

bloomberg/bc-twitter-abre-las-propinas-para-todos-y-permite-pagos-en-bitcoin.phtml>.

[44] Fuente: noticia en diario *Perfil*, versión digital, tomada de *Bloomberg* y disponible desde el 26/10/2021, con el título "Mastercard permitirá tarjetas de débito y crédito criptográficas". Consultado en <https://www.perfil.com/noticias/bloomberg/bc-mastercard-permitira-tarjetas-de-debito-y-credito-criptograficas.phtml>

supuesto y 55 del CP. Recuerdan que los hechos sucedieron entre el 14 y el 16 de diciembre de 2017, cuando H.M.P. realizó un ataque informático al exchange "Mercury Cash", logrando acceder a los sistemas de la empresa y tomar su control, lo que le permitió cursar transferencias de un total de 500 "ethers" (criptomoneda asociada al blockchain de Ethereum), a cuentas propias que tenía en otras plataformas, luego de lo que las descargó en una billetera de su titularidad y dominio almacenada en un teléfono celular. A la fecha del hecho equivalían a 434.352 dólares estadounidenses. Las medidas de seguridad de la empresa y la colaboración de otros exchanges permitieron ubicar las direcciones IP desde las que se concretó el ataque[45].

En cuanto a la mentada funcionalidad de las criptomonedas como técnica para el lavado de activos de origen delictivo, se ha pronunciado la Sala 1 de la Cámara Federal de San Martín, confirmando un procesamiento en causa *"Rodríguez Córdova, Max y otros s/legajo de apelación"*, resolución del 27/11/2017, tratándose de un caso vinculado a la actividad de narcotráfico que tuvo mediática repercusión como "Bovinas blancas" y ha recibido comentario de María B. Linares[46]. En el marco de un múltiple procesamiento con diverso grado de participación de varios imputados mexicanos y argentinos por el delito de tráfico de estupefacientes en modalidad de almacenamiento, agravado por el número de personas intervinientes, concurriendo idealmente con el de tentativa de contrabando, uno de los procesados fue considerado autor del delito de lavado de activos de origen ilegal que se habría

[45] Ya citados, p. 6, punto III.1. Formulan allí un comentario en líneas generales favorable del fallo, explicando su concordancia con varios de los fundamentos de la sentencia.

[46] Linares, María B., "Bitcoins: su empleo como técnica para lavar activos ilícitos. Nota a fallo", pub. Borinsky y Schurjin Almenar (dirs.), *Temas de Derechos Penal y Procesal Penal*, Erreius, mayo de 2019, pp. 243 y ss. Disponible en "Erreius on line", en <https://ius.errepar.com/sitios/ver/html/20190422103025021.html?k=criptomonedas%20y%20criminalidad>.

concretado a través de diversas operaciones financieras internacionales entre México y Argentina con bitcoins, adquiridos mediante pagos de sumas en efectivo, evitando canales legales y, por lo tanto, la emisión de los correspondientes reportes de operación sospechosa (ROS)[47].

V. Colofón

Aunque resulte una obviedad, desde una mirada ceñida a lo penal, lo primero a destacar es que las criptomonedas no deben ser, por decirlo gráficamente, demonizadas como si no fueran otra cosa que un vehículo para delinquir. De hecho, hemos señalado que teniendo en cuenta su alto valor económico, resultan a la vez singularmente atractivas como objeto para perpetrar diversos delitos contra la propiedad de naturaleza informática afectando a sus legítimos tenedores.

En línea con el problema señalado al inicio, como tantísimas otras creaciones, tecnológicas informáticas o de cualquier otra naturaleza, pueden ser utilizadas para perpetrar una conducta delictiva, pueden ser funcionales para la realización de actos disvaliosos (que pueden ser graves como el financiamiento del terrorismo o el blanqueo de dinero de origen ilícito), pero nada más (ni menos) que eso. Estos iniciales apuntes o primaria aproximación a la problemática no han pretendido otra cosa que resaltar esta última mirada.

Es claro que se aprecian día a día noticias que dan cuenta de usos desviados de las monedas virtuales y, en todo caso, se tratará en el futuro inmediato de ver el mejor modo de lograr un marco regulatorio que controle y desaliente tales ilícitos. En el mismo camino, es notoria la necesidad de brindar adecuada información a sus eventuales usuarios e inversores, indicarles las medidas de

47 Cfr. Linares, en "Bitcoins…", *op. cit.*, punto IV.

DOI:http://10.22201/fder.24488933e.2022.282.81937

seguridad que deben rodear a sus operaciones para evitar su fácil victimización.

En un mundo en el que la condición de alfabeto parece no satisfacerse más con la capacidad de lecto-escritura, en que tornó imprescindible la capacitación en el uso de las tecnologías de la comunicación e información para las cosas más sencillas del quehacer diario, es fácil advertir que hay sujetos singularmente vulnerables a las defraudaciones informáticas y deben promoverse adecuadas campañas para reducir y, si fuera posible, eliminar dicha vulnerabilidad.