Revista YACHAQ Nº 19
Centro de Investigación de los Estudiantes de Derecho (CIED)
Universidad Nacional de San Antonio Abad del Cusco
ISSN: 2707- 1197 (en línea)
ISSN: 1817–597 (impresa)
Fecha de recepción: 07/03/2025
Fecha de aceptación: 15/07/2025
[pp. 354-386]

Utilización de criptomonedas como objeto ilícito de lavado de activos en el contexto de ataques Ransomware: una "nueva" problemática

Use of cryptocurrencies as an illicit object of money laundering in the context of ransomware attacks: a „new" problem

Edson Arturo Arana Floriano[1]

Resumen

A través del presente artículo de investigación, el autor se aboca a problematizar el debate sobre las criptomonedas y su naturaleza como bienes, efectos o ganancias a la luz de la regulación peruana sobre el delito de lavado de activos, resolviendo bajo el principio de legalidad, concluyendo que sí es posible subsumirlas en dicho elemento normativo. Esto implicará, naturalmente, una reinterpretación del elemento normativo del tipo penal de lavado de activos antedicho a la luz de los aportes de la pragmática del lenguaje, con el fin de no provocar una infrainclusión de casos en el marco de las nuevas tecnologías. En segunda línea de desarrollo, luego de ofrecer una interpretación desde el principio de legalidad penal, analiza

1 Bachiller en Derecho por la Facultad de Derecho y Ciencia Política de la Universidad Nacional Mayor de San Marcos. Miembro egresado del Taller de Derecho Penal Económico y de la Empresa de la UNMSM. Asistente académico y legal en el Estudio Jurídico José Urquizo Olaechea S.A.C. Asistente de cátedra de Derecho Penal II y III en la Universidad Nacional Mayor de San Marcos. Correo electrónico: contactodp.edsonarana@gmail.com ORCID: https://orcid.org/0009-0003-7357-534X.

cómo se comporta el uso de ataques *Ransomware* por los ciberdelincuentes con el fin de exigir pagos mediante criptomonedas para no hacer inaccesibles de forma permanente los datos del usuario digital y si este supuesto se subsume en el delito de fraude informático como delito previo de lavado de activos, llegando a la respuesta de que concurren problemas de precisión y adecuación por desconexión con la dimensión de gravedad e injusto que emana de la propia conducta de secuestro informático. Las propuestas del autor se dividen en aspectos de *lege lata* y *lege ferenda*, para los problemas advertidos.

Palabras clave: Criptoactivos; blanqueo de capitales; secuestro informático; tipicidad; interpretación; fraude informático.

Abstract

In this research article, the author attempts to problematize the debate on cryptocurrencies and their nature as "*goods, effects or gains*" in the situation of Peruvian regulations on the crime of money laundering, resolving under the principle of legality, concluding that it is possible to subsume them in this normative element. In a secondary analysis, it examines how the use of Ransomware attacks by cybercriminals behaves in order to demand payments using cryptocurrencies in order not to make the data of the digital user inaccessible and whether this assumption subsumes in the crime of computer fraud as a prior crime of money laundering, arriving at the answer that there are problems of accuracy and adequacy due to disconnection with the dimension of seriousness and injustice emanating from the conduct of "cyber kidnapping". The author's proposals are divided into aspects de lege lata and lege ferenda, for the problems noted.

Keywords: Criptoactives, money laundering, cyber-kidnapping, typical, interpretation, computer fraud.

Introducción

No cabe duda de que uno de los tópicos de mayor contemporaneidad – pero, también, de un valetudinario tratamiento en nuestra comunidad jurídica nacional – concierne a la cibercriminalidad, por su entramado tan vegetante y, sobre todo, por la conjunción de elementos propios de la globalización digital, tecnologías de la información y derecho penal, como son el uso de programas informáticos maliciosos de secuestro de datos (*Ransomware*), la disposición de un tipo concreto de monedas digitales para liberar los datos del usuario criptomonedas y los actos concretos de recepción, ocultamiento o "traslado" de dichas monedas digitales a "monederos" digitales lavado de activos. Cada una de las variables aquí identificadas constituyen, por de contado, un contexto integral – y autónomo – de injusto: la comisión del delito de lavado de activos a través de la realización previa de un "secuestro informático" que genera un provecho económico traducido en una criptomoneda.

Así, este trabajo pretende desarrollar y problematizar la figura del lavado de activos y su posibilidad concreta de configuración típica en estos supuestos en el marco de la globalización digital y las Tecnologías de la Información (solución *a priori*); ello, mediante el uso de la interpretación gramatical, propia de la regla de competencia de la legalidad penal. Del mismo modo, en el marco de problemas concursales de delitos, se defiende que no existe posibilidad de aplicar concurso real entre atentado a la integridad de sistemas o datos informáticos y extorsión mediante el uso de ataques *Ransomware*, sustentado en la naturaleza especial que ostenta el merecimiento de pena para esta modalidad especial de impedimento de acceso a datos o sistemas informáticos. Finalmente, se recomienda una modificación de *lege ferenda* respecto de un tipo penal derivado del delito base de fraude informático (solución *a posteriori*).

Identificación del problema

"X" es un pirata informático, con una amplia presteza para la configuración de *malwares*; específicamente, *Ransomware*. Su propósito es esparcir este programa malicioso mediante internet para infectar múltiples sistemas operativos de usuarios y cifrar sus datos, para hacerlos inaccesibles y, en ese marco, solicitar al desventurado cibernauta la friolera de 0.0077 BTC que, al cambio, resultan $ 400 USD (cuatrocientos dólares americanos) a través de una pantalla emergente. Tal desembolso deberá realizarse en una billetera digital, cuyo enlace se adjuntará, disponiéndose solo del plazo de 72 horas para entregar el dinero por el rescate de la información y, a cambio, desencriptar los archivos, bajo la amenaza de hacer permanentemente inaccesibles los datos si no se cumple con dicho requerimiento. Con posterioridad, "X", quien no resulta el propietario de la billetera digital, sino "Y", ordenará – recibidos los $ 400 USD en Bitcoins – que dicho monto se ramifique a otras billeteras digitales ya creadas previamente, para dotarlas de mayor seguridad. Finalmente, "A" y "B", colegas de "X" e "Y", utilizarán dichos Bitcoins para otras actividades afines.

Como se puede colegir, subyacen al caso tres problemas de fuste: primero, si se trata de un supuesto imputable (por autoría o participación) que cumple con las condiciones para colmar el tipo penal de lavado de activos (el hecho cuenta como lavado de activos) y ser antinormativo y que el grado de injusto y severidad de la pena responde al derecho penal con implicancias en las nuevas tecnologías; segundo, si las criptomonedas pueden ser consideradas como "bienes, objetos o ganancias", con base en una interpretación *gramatical* de la ley penal o si, por el contrario, admitirlo implicaría una *analogía extensiva in malam partem*, proscrita bajo la lógica del principio de legalidad penal (*lex stricta*) y, finalmente, si el delito de "fraude informático" es lo suficientemente específico – en el sentido de naturaleza e intensidad de injusto – como para incluir dentro de sus supuestos a los casos de "secuestro de datos informáticos" mediante un *Ransomware* (juicio de interpretación y subsunción de un hecho a un tipo penal) – *applicatio legis ad*

factum – (Sánchez-Ostiz, 2008, p. 486; Hruschka, 2009, p. 15) y, por otro lado, si este mismo tipo penal podría consignarse como "delito previo" en la figura del lavado de activos.

Atiende entonces el lector que esta resultará una industria donde se conjuntarán tres elementos: dogmática penal, informática y monedas digitales. Visto y considerando que la legislación peruana – a diferencia de otras latitudes – no ha desarrollado con propiedad el tópico atinente a los delitos informáticos y posee aún solo destellos de regulación para los criptoactivos, resulta de precipua trascendencia esta investigación.

Análisis

Para resolver el problema que aquí concierne, se precisará de esquematizar bajo tres interrogantes lo expuesto: primero, ¿el delito de lavado de activos, en su configuración actual, es lo suficientemente preciso como para ser regla de comportamiento para casos como los de cibercriminalidad y uso de monedas digitales?; segundo, ¿es posible incluir mediante interpretación gramatical a las criptomonedas como objeto ilícito del delito de lavado de activos?; tercero, ¿tiene el delito "fraude informático", regulado en el artículo 8 de la Ley N.º 30096, un alcance preciso para determinar la entidad de injusto de los "secuestros informáticos" mediante utilización de *Ransomware* y, en ese marco, delitos previos para lavado de activos? A lo largo del trabajo se resolverá cada una de estas.

El delito de lavado de activos: ¿preciso ante la cibercriminalidad?

No cabe duda de que el tipo penal de lavado de activos respondió a una necesidad de orden político-criminal para desbaratar la acrecencia de la delincuencia organizada, que veía en la introducción de las ganancias ilícitamente conseguidas mediante la comisión de un delito previo un método para promover y fortalecer

económicamente a la misma actividad criminal, constituyéndose entonces como un problema de fuste en la nueva era. Ello justifica cómo es que en diversas convenciones internacionales (Viena, de 1988, donde se vincula primigeniamente las organizaciones criminales y el narcotráfico; Estrasburgo, de 1990, donde se precisa normativamente por primera vez el tipo penal de lavado de activos al someterse a escrutinio las directrices de construcción dogmáticas de este delito y extender el marco de acción a "delitos graves" y asumir una posición en la teoría de la imputación subjetiva psicológico-volitiva (Sánchez-Málaga, 2016, pp. 221, 229, 243 y 248); Palermo, del 2000, donde se establecen tres Protocolos Facultativos que inciden sobre los delitos previos, que máxime se encuentren coligados con la participación en delitos de organización, sobre el extremo de la corrupción y sobre la obstrucción de la justicia; Mérida, del 2003, etc.) (Pariona, 2021, pp. 28-34) se trata con sumo aplomo la lucha frontal contra la criminalidad y la gestación de capitales maculados, hecho no ajeno a la propia mutabilidad de los fenómenos criminógenos que, con el tiempo y el avance de la tecnología, es cada vez más intensa.

En el mundo digital, es cada vez más habitual plantearse modalidades para lavar dinero de origen ilícito; verbigracia, a través de casas de apuesta o juegos en línea, por lo cual no resulta inocente afirmar que la transnacionalización y la globalidad han aportado enormemente a proliferar mecanismos de blanqueo del lucro surgido de ciberdelitos (Miró, 2012, pp. 83 y 239).

Es más: resulta especialmente interesante esta situación, toda vez que la dogmática penal tradicional se ha visto avasallada por este cambio social, manifestando cuatro posiciones – que se pueden ver reflejadas también en el propio tipo penal de lavado de activos –: a) se ha planteado que solo se trata de un problema de orden práctico, cuando en realidad se trata de un auténtico desplazamiento *sui generis* de la forma clásica de interpretar conductas penalmente relevantes – es decir, no nos encontramos ante hechos que se puedan atribuir al agente como artífice en tanto modificador de la realidad de forma libre

de manera *directa*, sino que a través de la utilización de un medio no humano, que en ocasiones es automático (como los ataques mediante *malware,* que solo exigen la programación del pirata informático para luego infiltrarse en el sistema operativo) se generan lesiones a bienes jurídicos inmateriales, con problemas ostensibles para la teoría de la tipicidad penal (Posada-Maya, 2022, p. 75 y 84)); b) se ha considerado que esta diatriba en la cibercriminalidad por la dogmática penal es de dandis, es decir, una moda de época – sin embargo, no es de extrañar que las corrientes de este estilo posean afinidad a la Escuela de Frankfurt, que asumía una posición minimalista y nuclear del derecho penal –; debe recordarse, como hace Alpaca (2022, p. 147) que la propia concreción de los bienes jurídicos implica un concepto material que subyace a las normas de comportamiento, como efectivas razones de legitimación para su creación, por lo cual influye mucho lo ontológico – como antaño lo diría Welzel – para encontrar el marco de limitación de la libertad de acción.

Sin embargo, si entendemos que la propia definición de bien jurídico se sostiene como "propiedad que, en cuanto exhibida por una persona, una cosa, una institución o en general un objeto (lato sensu) cualquiera, es valorada positivamente, en el sentido de que esa propiedad es valorada como buena" (Mañalich, 2022, p. 64), no cabe duda de que, en tanto un usuario exponga la propiedad inmutable, personal e intransferible sin consentimiento de sus datos o sistemas informáticos en la autopista digital, la libertad de terceros, en sus ámbitos de organización, debe regirse por la máxima *neminem laedere* (deber negativo no dañar a otro) y, en consecuencia, se valorará como positivo y reconocido, por tanto, esa propiedad de los datos informáticos exhibidos por los usuarios de un ordenador. Con todo, el bien jurídico supone una específica configuración de la realidad, vista desde lo jurídico-penal, en función de valores de la vida social o como "circunstancias dadas o finalidades útiles para el individuo", por lo cual no cabe duda de que disponer de un mecanismo interpretativo reduccionista anacrónico solo serviría para la impunidad de conductas que poseen una entidad

lesiva ostensible, infraincluyendo supuestos (Lascuraín, 2018, p. 114; Roxin; 1997, p. 56); c) se plantea la existencia de un cambio de paradigma en la dogmática penal, hecho que supusiese repensar los contenidos de la parte general al respecto de la naturaleza del injusto, los grados de intervención delictiva, la reformulación de los criterios de imputación, etc., pero sin abandonar los principios esenciales (Agustina, 2021, pp. 710-715); y d) al ser la tecnología informática una de cambios tan vertiginosos, la capacidad de rendimiento de una determinada teoría en el marco de la criminalidad deberá responder precisamente – por ejemplo, en el análisis del riesgo permitido– a las formas en que se comportan los usuarios sin alterar el objeto protegido por la norma de comportamiento sobre cibercriminalidad.

Toca delimitar, al fin, cuál es el objeto protegido del tipo penal de lavado de activos, pues dependerá en buena cuenta hasta dónde se interpreta adecuadamente un tipo penal y su objeto de protección inmediato (función de delimitación) (Lascuraín, 2018, p. 120). Sobre lo anterior, existe una avenencia más o menos marcada en la jurisprudencia; no obstante, una discrepancia insalvable en la doctrina. Así, la Corte Suprema de Justicia del Perú, en el Acuerdo Plenario N.º 3-2010-CIJ-116, esbozó que el lavado de activos tiene naturaleza pluriofensiva, esto es, tutela una variedad de bienes jurídicos, en atención de su naturaleza criminológica mutable. Autores como Pérez López (2019, p. 22) indican la razón de esta posición pluriofensiva: existe más bien un compromiso político-criminal de lucha contra la criminalidad abocada a la comisión del lavado *per se*. Otros profesores como Nieto Martín explican el motivo de cada bien jurídico tutelado: primero, la administración de justicia, en la medida que se vincula con los delitos de encubrimiento y los mecanismos de ocultación de los beneficios económicos obtenidos con la realización del delito previo que afectan la efectividad del sistema judicial. En segundo lugar, se analiza como bien jurídico el mismo que ya protege el delito previo, con lo cual se atendería a una premisa preventivo-general de la pena, mediante la que se busca desincentivar a la comisión de los injustos penales

precedentes. Con ello, se deduce, quedaría en evidencia la falta de autonomía dogmática y hermenéutica del lavado de activos, desplazándose como accesoria en función del merecimiento de pena que suponga el tipo penal precedente, siendo así que su construcción prescindiría de un objeto protegido inmediato y atentaría ostensiblemente contra el principio de lesividad (imprecisión del bien jurídico. Tercero, se proyecta como objeto protegido el orden socioeconómico y financiero. Al trasladarse cantidades de dinero o criptoactivos (en el caso de que se pueda concluir – como sí será – el alcance interpretativo de los artículos 1 y 2 del D.L. 1106) ingentes, se piensa que su comisión maniataría a sectores económicos completos o, más aún, de manejar una porción considerable de la economía de los países (Nieto, 2022, pp. 1273-1289).

Autores como García Cavero (2013, p. 75) sostienen, por su lado, que lo protegido es la expectativa normativa de un correcto tráfico de bienes a través de operaciones lícitas. La divergencia de opiniones –se puede advertir– se basa en dos factores clave: a) la comprensión de lo "protegido" por los tipos penales, y b) la naturaleza dogmática del tipo de lavado de activos.

De todo ello, se puede asumir que, cuanto menos, el objeto protegido del tipo de lavado es doble: primero, sobre la administración de justicia – tal y como en sus orígenes se constituyó, esto es, para "encubrir" otro delito y, segundo, sobre el delito precedente o previo, en la medida que dicho ocultamiento de ilicitud promueve genéricamente su masificación (Molina, 2017, p. 272), atentando solo accesoriamente al orden socioeconómico. Ambas fórmulas deben ser vistas de consuno, puesto que individualmente planteadas se enfrentarían a dificultades dogmáticas respecto de los principios limitadores del derecho penal. Tomar una posición que considere al orden socioeconómico como objeto protegido en el lavado de activos implicaría graves problemas para la inclusión de las criptomonedas como objeto ilícito del lavado, ya que se debería asumir, de buenas a primeras, que los criptoactivos se encuentran reconocidos actualmente en nuestra legislación como medio de cambio oficial; segundo, se debería reconocer de que, cuanto

menos, alguna institución financiera nacional o extranjera brinda soporte a las mismas y que, en ese sentido, la introducción de dichos criptoactivos maculados no garantiza las propiedades disposicionales exhibidas por el mercado y que el sistema jurídico valora como buenas: es decir, de competencia leal, justa, estable y libre (Villegas, 2018, pp. 254 y 256; Mendoza, 2022, p. 313).

A este efecto, resulta importante el aporte de Lamas Suárez, quien ofrece una detallada explicación del ciclo de lavado con criptomonedas: colocación de criptoactivos mediante *exchanges, local traders*, mineros, etc.; ensombrecimiento de las criptomonedas a través de la característica difusa de la *blockchain* y la integración de las criptomonedas mediante intercambiadores, cajeros o tecnología *P2P* de conversión con la mezcla de activos no maculados (2024, pp. 173-176), que nos termina por sugerir que, incluso en contextos de cibercriminalidad, sí se puede ensombrecer el origen ilícito de activos digitales a través de la integración de estas con otros ingresos lícitos.

Con ello, hemos arribado a la respuesta de la interrogante planteada en el análisis: el delito de lavado de activos, en su configuración actual, sí mantiene un estándar de precisión interpretativo para incluir su transferencia

Las criptomonedas: ¿objetos ilícitos de lavado?

Se define las criptomonedas, criptodivisas o criptoactivos como activos en formato digital que disponen de mecanismos de criptografía, con el fin de realizar intercambios comerciales entre personas (naturales o jurídicas) a través de internet y asegurar las transacciones o transferencias de valor de aquellos que la usen, a través de la confianza entre usuarios (Cabrera y Lage, 2021, pp. 3 y 6). Como funcionan a través de internet, es necesario conservar su existencia mediante ordenadores que determinan su base de datos con el propósito de proteger los registros que se tenga de las operaciones, a través de métodos matemáticos (Pilacuán, Espinoza, Carreño y Palacios, 2021, pp. 177-178). El método de obtención primigenia de estas criptomonedas es a través del proceso

de “minado”, que realiza en sí misma las validaciones de transacciones en una red *peer to peer* (P2P) para consignar la unicidad de cada criptomoneda a través de procedimientos matemáticos complejos para construir nuevos bloques que se añadirán a la *cadena de bloques*, esto es, que una misma criptomoneda no haya sido usada dos veces, recibiendo el “minero” una ganancia en criptoactivo de ese procedimiento; pero, además, este conjunto de operaciones complejas permite sellar el bloque de transacción (Barroilhet, 2019, p. 44).

Existen dos elementos indispensables en la configuración de las criptomonedas, esto es, el sistema de transferencia electrónica (tecnología *peer to peer*) y el registro contable (mercado *blockchain*). Sobre lo primero, brinda la facilidad de realizar operaciones entre privados sin la necesidad de una autoridad central que lo apruebe, hecho que define en buena cuenta una de sus características centrales. Además, esta red usuario-usuario también brinda las llaves privadas con las que el receptor de la criptomoneda podrá abrir el archivo cifrado que contiene la criptomoneda en sí.

Sobre lo segundo, cabe detenerse un poco más: la *blockchain* o cadena de bloques es un software de registro digital autónomo, integrado, sincronizado e inalterable, que, a través de una red de “nodos”, sirve como garantía de la autenticidad de la transacción con criptomonedas y da contenido al anonimato de estas, en la medida que toda la información de los usuarios no es revelada porque, en principio, no se solicita identificación (Pilacuán, Espinoza, Carreño y Palacios, 2021, pp. 179-180). Aunque sean estos datos ocultos, lo que sí es de carácter público es la propia transacción, ya que los mismos usuarios en conjunto pueden comprobarlas (Pérez, 2016, p. 144). Tal elemento definirá la poca trazabilidad de las transacciones con criptomonedas y, en definitiva, los riesgos penalmente desaprobados para la configuración de lavado de activos como factor criminógeno (Prado, 2019, p. 165).

Resulta importante deslindar su concepto de otras figuras como son el dinero digital (todo medio de pago en forma digital), dinero electrónico (medio de pago

digital por el que surge un deber de entrega y un derecho de cobro de dinero corriente – como si de un título valor se tratase –) y moneda virtual (medio de pago sin regulación normativa ni sucedáneo físico, pero con eficacia en transacciones vía internet); ello, porque al poseer los criptoactivos características autónomas y mayor nivel de complejidad en la seguridad de transacción, pretende estar a caballo entre una moneda digital, dinero electrónico y una moneda oficial. Tomando en cuenta esto, se infiere que la función de las criptomonedas, tanto histórica (herramienta incorpórea de pago de aceptación entre un grupo de personas) (García-Ramos y Rejas, 2022, p. 4) como actual es la de ser medios de pago. Así, por ejemplo, nos informa Pérez (2016, p. 143) que ha sido reconocido por el Tribunal de Justicia de la Unión Europea. Sin embargo, es cierto que todo depende, en buena cuenta, de la postura del sistema económico donde se hable.

Las criptomonedas fungen como sucedáneos del dinero físico, aunque se diferencian del mismo por cuatro factores esenciales: a) su descentralización e independencia; b) su marcada volatilidad en el mercado; c) su anonimato o privacidad, y d) su ausencia de intermediarios.

Sobre la primera de sus características, al no hallarse respaldadas ni reguladas por una entidad bancaria internacional o nacional, no poseen un soporte regulatorio oficial, por lo cual dependen más del uso privado entre usuarios de internet (García-Ramos y Rejas, 2022, p. 3). Optar por dicha posición ha permitido a múltiples usuarios hacer agibles las transacciones, reducir los costos de comisión y prescindir de los requisitos que los bancos establecían (Fonseca y Tacuma, 2018, pp. 6-7), lo cual deriva en una mejor oferta de desarrollo comercial, con menores tiempos y costos (Álvarez, 2019, p. 133), a diferencia de lo que es utilizar los medios tradicionales de operación económica. Esta característica es lo que hace tan atractiva a la criptomoneda; pero, a la vez, lo que ha sugerido a cierto sector de la doctrina y legislación informática decantarse por la "licencia de transacción de criptomonedas" (García-Ramos y Rejas, 2022, p. 5), para poder combatir su uso delictivo por la criminalidad cibernética.

Algunos sectores, amparándose en su falta de respaldo de instituciones financieras y que la oferta de caudal dinerario es fija y con incrementos marginales decrecientes, la han reputado como una moneda deflacionaria (Cabrera y Lage, 2021, p. 11); no obstante, esto no podría ser totalmente cierto si es que se considera, como pudo advertirse, que el precio de las criptomonedas depende del modo en que los usuarios las empleen. En todo caso, más lógico sería atribuirles una condición de medio de pago con una liquidez tendiente a la incertidumbre o la especulación, en una relación triádrica entre usuario, producto y valor relacionado con alguna divisa legalmente admitida, y basada también en cierta medida en los hitos históricos suscitados por la humanidad.

La segunda de las características también trae consigo múltiples consecuencias; la central: las criptomonedas son inequívocamente volátiles y, en consecuencia, no son índice seguro de referencia monetaria estable. Todo ello, visto desde la experiencia: en sus inicios, entre el 2009 y 2010, el valor promedio anual en el mercado de la criptomoneda más conocida, Bitcoin (BTC) era de $ 0.001 y $ 0.1 USD (dólares americanos); en el 2017, su valor ascendió vertiginosamente hasta los $ 19 798 USD; con el inicio de la pandemia histórica del COVID-19 (marzo 2020 – enero 2023), se registró en su cierre un decrecimiento al valor de $ 6438.64 USD; luego, en octubre de 2021, alcanzó su ascenso histórico en dicho periodo con un valor de $ 61 318.96 USD[2]. Así, el gran atrenzo con las criptomonedas es la probable constitución de una burbuja especulativa en sus valores de cambio, toda vez que no hallan soporte ni en un metal precioso, valor específico real o por una entidad gubernamental (Egaña, 2018, p. 11).

Respecto de la tercera característica, al ser la transferencia de criptomonedas generada mediante criptografía que no exige a los tenientes de estos activos

2 Los datos aquí presentados fueron extraídos de la página dedicada al análisis bursátil de las criptomonedas "Yahoo! Finanzas", que posee registros de las alteraciones en la conversión de Bitcoin (BTC) a divisa estadounidense de distintos años. Véase: https://es-us.finanzas.yahoo.com/quote/BTC-USD/history/?period1=1577836800&period2=1729382400&interval=-1mo&filter=history&frequency=1mo&includeAdjustedClose=true.

digitales datos, se dificulta abiertamente la identificación o rastreo informático de autores de ciberdelitos (Prado, 2019, p. 166) que utilicen este medio para generar provechos; como dice, entonces, Pérez López, las criptomonedas se adecuan a estos caracteres de la delincuencia digital (2017, p. 177). Esta cualidad también afecta a los deberes de cuidado que impone el Grupo de Acción Financiera, en su Recomendación 10, a los usuarios digitales y las empresas para identificar la procedencia de los activos que ingresan al patrimonio pasibles de lavado o blanqueo.

Finalmente, su cuarta característica reconocida es una consecuencia del propio hecho de trabajar en los márgenes de instituciones bancarias: no se necesita de un tercero para validar la transacción. En sí, esta cualidad también dota a las operaciones con criptoactivos de su carácter irreversible, ya que, para suplir la ausencia de un tercero, se generan "paredes blindadas" para evitar la reversión de estas, incrementando su anonimato e "irrastreabilidad" (Lamas, 2024, p. 173).

Respecto del análisis dogmático-penal que se pretende hacer, es relevante advertir las dificultades que encauza su anonimato y nivel de regulación ya explicados *supra*. Como expresa Prado Saldarriaga (2019, p. 166), la vinculación entre criptomonedas y derecho penal pueden acarrear tres factores criminógenos: anonimato en transacciones, dificultad en el rastreo para las operaciones vía internet y la regulación normativa lábil por parte de los países donde se registran operaciones con criptoactivos. No por nada una buena parte de países ha optado por la adopción de una tolerancia pasiva a este tipo de cambio, es decir, la no-adopción de medidas prohibitivas, pero sí de una política de desincentivo para transar con criptomonedas – como, por ejemplo, ha venido a postular el Banco Central de Reserva del Perú –. Sobre lo primero, debe considerarse que las criptomonedas trabajan a través de billeteras electrónicas; estas se pueden transferir como archivo y con una llave digital encriptada a otra billetera.

A través de esta puede advertir solamente el usuario receptor cuánto recibió y, si este desea enviar posteriormente a otra billetera un nuevo monto,

deberá generarse otra llave encriptada, que recibirá con el correspondiente archivo el novísimo usuario (Barroilhet, 2019, p. 41). Se genera así una cadena de transferencias privadas, cuyo rastreo es sumamente complejo, y aviene la posibilidad de ramificar un monto de criptomonedas de una sola billetera a otras, ensombreciéndose el camino por el cual transita. Todo esto sirve para analizar si una criptomoneda puede ubicarse dentro de los supuestos de "bienes, objetos o ganancias" como objeto ilícito, bajo un marco de interpretación gramatical del principio de legalidad.

Primero, debe decirse que, aun cuando no tengan un respaldo jurídico estricto, se puede colegir que estos activos poseen un valor económico referenciado en una moneda aceptada como divisa de cambio oficial por instituciones financieras (por ejemplo, el dólar) que, en cuyo caso, cuenta como medio de cambio para los usuarios que con ella transen y, en ese marco, puede generar provechos del cual se favorezcan los sujetos. Aquí se parte de una interpretación literal del término "ganancias", sostenida por el juego del lenguaje que los propios hablantes en su normatividad hacen del uso del término.

Segundo, tal posición se sostiene desde una perspectiva de la pragmática del lenguaje, que define los usos correctos e incorrectos a través del seguimiento de una regla implícita a partir de un compromiso de los hablantes con dicha regla, con base en la práctica social. Así, la interpretación consistiría en, básicamente, sustituir el contenido proposicional de la regla por otra que contenga lo mismo (Wittgenstein, 2014, p. 183) y, naturalmente, quienes realizan los contenidos de corrección de esta interpretación son los propios hablantes como seres sociales en comunidad, es decir, a través de la intersubjetividad.

Así, la interpretación literal podría definirse como la razón que– por práctica social – todos los hablantes sostienen en un contexto bajo un compromiso intersubjetivo que corresponde a las *formas correctas* de sustituir el contenido de una regla, sin que se tenga que pedir dicha razón por hallarse implícita en su propio uso por dominar la misma técnica. Sin embargo, cabe decir que la práctica

no se trata de una mera regularidad de actividades (el propio Robert Brandom (2005, p. 68), en su Hacerlo Explícito, descartaba la idea del *regularismo* porque, en todo caso, no habría sentido en la naturaleza *ontogenética* del hablante en potencia es decir, en la comprensión de lo que se hace), sino más bien de un "hacer" como una forma de vida (p.ej. un hablante que apunta con un arma a otro en la cabeza y aprieta el gatillo da una razón para que un hablante afirme que, intencionalmente, quiere que se produzca la muerte a otro y, en consecuencia, se activa la razón excluyente de la norma de comportamiento en tanto *evitar* dicha acción para cumplir la norma) (Mañalich, 2010, p. 173) que hace a la normatividad como "normalidad" (Cabanchik, 2015, p. 22).

Esa es la naturaleza por la que el principio de legalidad penal se constituiría como una regla de uso de la interpretación, por lo que sirve también como su límite. Por eso, la adscripción de un sentido para las palabras depende, en buena cuenta, de cómo usemos la expresión cotidianamente, es decir, si al decir dicha palabra esperamos una reacción concreta de los demás como acto perlocucionario. Lo último se refleja en que, para los filósofos analíticos, que algo sea "común" (y, por ende, "literal") se sostiene en su común aceptación por todos y en su funcionalidad comunicativa (esto es, su efectividad, lo que se quiere causar en terceros es lo que al final ocurre – justamente la definición de acto perlocucionario de John Austin –) (Camps, 1976, p. 63). Así, menciona Wittgenstein, en *Investigaciones Filosóficas,* en el parágrafo 340, sugiriendo que la forma de descubrir cómo funciona una palabra dependerá, en buena medida, de dar examen a su forma de aplicación y aprenderla (2014, p. 241), y eso se sujeta, obviamente, al uso de esta *para* sus hablantes.

Sin embargo, quizá podría ser necesario disponer de ciertos criterios para llegar a una conclusión sobre el uso literal del término criptomonedas. Así, Matthias Klatt, apelando a un juicio pragmático del lenguaje, ofrece el siguiente estándar argumentativo: se trata de apelar a relaciones inferenciales que llevan la siguiente premisa general: "para todos los objetos x es válido que: si x tiene las propiedades

M, entonces x ha de subsumirse bajo el concepto legal t" (2012, p. 241). Esto, naturalmente, debe poseer su basamento en los distintos principios limitadores del derecho penal, como son la proporcionalidad, culpabilidad, mínima lesividad, etc., es decir, ser una *razón correcta* en el marco de la normatividad de los intérpretes de la ley penal[3].

En tercer lugar, para interpretar si las criptomonedas pueden incluirse dentro de un objeto ilícito constitutivo de lavado de activos dependerá, en buena cuenta, de preguntarse por cómo se usa la criptomoneda en la comunidad de hablantes. Tal y como se dijo, se dispone de la misma como un *sucedáneo* del dinero, esto es, como un medio de pago para múltiples transacciones, mediante la *blockchain*, es decir, como una forma de efecto o ganancia para contratos. Así, los criptoactivos se han integrado de manera flexible a las actividades financieras de múltiples empresas alrededor del mundo en el mundo virtual (Álvarez, 2019, p. 131), transformándose bajo normatividad su uso como el propio de un medio de pago a través del hacer financiero cotidiano. Bajo esa premisa, la definición que ofrece el artículo 1 del Decreto Legislativo N.º 1106, de lavado de activos, no debe ser vista desde una lógica anacrónica, sino referenciada en el contexto de las tecnologías de la información digital que hoy nos envuelven. Gana más peso el argumento cuando se advierte que múltiples instrumentos internacionales ofrecen descripciones amplias y flexibles de la figura de los bienes, efectos o ganancias (Prado, 2019, p. 174).

Ahora bien, la mayor objeción que se puede efectuar a este respecto es que la interpretación de "efecto o ganancia" no podría alcanzar a las criptomonedas, puesto que, en todo caso, cualquier tipo de resultado, incluso indirecto, de un delito fuente, sería pasible de encajar en él, sobrepasando el "sentido literal posible" del mandato de *lex stricta*. Ello se alega desde la premisa de que el

3 Tal premisa se define en función de que estos principios sirven, en el plano del derecho penal, como límites para el poder punitivo, restringiendo determinadas medidas o interpretaciones que puedan vulnerar derechos constitucionales. No por nada buena parte de estos tienen su origen en el Estado social y democrático de derecho, de ribetes liberales.

límite de interpretación de un texto es el propio texto, olvidándose que no se puede encontrar en cualquier proposición *x* los criterios de interpretación de *x*: básicamente supondría, como se niega al respecto de las normas, que la forma de aplicación de una de ellas se encuentra en sí misma (principio de no autorreferencialidad de las normas). Por ello, el límite debería ubicarse, en principio, en aquello que *sujeta* discursivamente a todos los *intérpretes* (quienes dan y exigen razones para actuar) dentro de las reglas de juego del lenguaje (jurídico), es decir, en aquello que los hace *convenir* que un término tiene un significado. Y, para ello, recordando que la legalidad es una *regla constitutiva* del sistema de usos lingüísticos jurídico-penales, no habría de limitar la interpretación literal a un uso único, sino a la forma en que los hablantes podrían disponer de ella (para significarla) (Flores, 2022, p. 276) en una cadena emisor-receptor-emisor[4] *justificada* en normas implícitas (basadas en el compromiso discursivo sobre la significación de *x* en el mundo lingüístico, por el que uno se hace responsable ante sí propio y ante los demás) (Brandom, 2005, pp. 254-255). Así, el juez penal – que hace las veces de intérprete de la contenido enunciativo de la norma penal como *acto perlocucionario*, esto es, asignador de significados – debe sujetarse al *telos* (esto es, al fin) de una decisión legislativa para poder adjudicar un sentido propio al texto, puesto que existe una relación asimétrica de reconocimiento recíproco entre el intérprete y el legislador. Esto significa que solo con arreglo a lo que *el texto* legislativamente producido se *puede* interpretar, lo que da legitimación a la interpretación, mas no atribuye significados (primer

4 La estructura triádrica que se expone viene dada por una relación de lenguaje donde todos los agentes han pasado, primero, por introducir a un hablante en las reglas de uso de un sistema lingüístico concreto a través de la práctica (esto es, cómo usan dichos hablantes el término en su cotidianidad y cómo asignan a los objetos sensibles o no sensibles significados) y, en segundo lugar, que al "nombrar" algo se siga expresamente aquello ya aprendido. Ello debe seguir los criterios de: a) intención (lo que el "emisor" quiere enunciar al receptor, produciéndole un concreto efecto, según esas reglas aprendidas, reconociendo dicho receptor lo que busca provocar en él, haciéndolo nuevamente emisor de dicha intención) y b) convención (aquello que se toma por "cierto" del efecto buscado con la emisión de un acto lingüístico, según el contexto de uso – como intención del hablante dentro de los actos de habla –, por el principio de expresabilidad de todo hablante) (Camps, 1976, pp. 70-96)

reconocimiento del juez al legislador). De allí que el legislador haya de atender a que las convenciones de interpretación judiciales son variables en el tiempo, dependientes del uso del término propuesto, y corregibles entre sí (Mañalich, 2024, pp. 75-77). Así, entonces, para aprehender un correcto enfoque de la finalidad legislativa en la semántica de los términos usados por el legislador es aquel que entiende a la literalidad como *significado convencional*, es decir, los usos consolidados y admitidos por quienes, en el momento de la interpretación, dan a las expresiones, teniendo en cuenta reglas semánticas, convenciones de otros lenguajes y contextos específicos de uso (Iturralde, 2014, p. 64).

Parece ser, entonces, que las criptomonedas tienen las propiedades de un bien, ganancia o efecto, por lo cual aquellas podrán considerarse como auténticos objetos ilícitos de lavado de activos. Si reparamos en la definición que ofrecen, por ejemplo, profesores nacionales como García Cavero (2016, p. 95) o Gálvez Villegas (2016 , pp. 48-56), atenderemos que la mayoría de supuestos de uso de criptomonedas para lavar activos se pueden ubicar en el marco de "efectos o ganancias", ya que estas vienen a ser producidas con posterioridad al acto delictivo; en el caso de esta investigación, al mismo acto de "secuestro informático" (si se trata de la recepción del criptoactivo a la billetera digital o si se trata del uso de este criptoactivo en una actividad económica posterior que generará, por ensalmo, rédito económico). De igual sentido también es Mendoza Llamacponcca, al enunciar a los efectos del lavado como "[...] objetos producidos mediante la acción delictiva (producto *sceleris*)" (2016, p. 306) y a las ganancias como "[...] ventajas patrimoniales o utilidades conseguidas a través del dinero, cualesquiera que fueran las transformaciones que hubieran podido experimentar" (2016, p. 303).

Con esto en mente, la presuposición de que las criptomonedas, como sucedáneos del dinero en la autopista digital, puedan ser ganancias o efectos – no bienes, dado que, como entendemos, se trataría de una asignación estrictamente normativa, basada en lo que el Código Civil reconozca, luego, como tal – no

estatuiría una vulneración a la prohibición de *analogía in malam partem*, toda vez que, en tiempos hodiernos, el uso que hacemos de "ganancias" se referiría a todo aquello que acrece el patrimonio personal, esto es, todo aquello que posea un valor específico intrínseco, sea o no reconocido como lícito, pertenezca esta o no a medios no físicos (véase, si se alega que el uso de dinero virtual en casas de apuestas puede ser pasible de reconocerse como objeto ilícito de lavado de activos, nada obsta a que lo no regulado por una entidad bancaria tampoco lo sea – una suerte de argumento *a fortiori* –). Esta definición también podría verse avalada con otra como la que ofrece Blanco Cordero, al acogerse a una postura de las *ganancias brutas* como objeto material de blanqueo de capitales, que propone bajo la idea de los tratados internacionales la asignación de sentido "producto" a "todo provecho económico derivado u obtenido directa o indirectamente de un delito", en virtud de que no se tiene derecho respecto de bienes que no han sido obtenidos de forma lícita (Blanco, 2012, pp. 252 y 262).

En nuestro país, no obstante, existe una suerte de escepticismo socavante respecto de la evolución criminógena de todos los activos virtuales, dado que, incluso con las modificaciones del Decreto Legislativo N.º 1106, no se priorizó un tratamiento específico de esta clase de formas para acrecer el patrimonio. Sin embargo, no se puede estar de acuerdo con Prado Saldarriaga (2023, p. 103) cuando sostiene que, *en principio* los activos virtuales (entre los que encuadran las criptomonedas) no podrían ser objeto de lavado de activos – ni bienes, efectos, dinero o ganancias –, puesto que no son monedas FIAT, cuando líneas posteriores reconoce el impacto negativo sobre una falta de regulación expresa de estas manifestaciones de activos digitales. Lo que sucede, en todo caso, es que existe una malcomprensión de la *legalidad penal* y de los límites de interpretación literal que, *ut supra*, se ha intentado esbozar con otra perspectiva líneas arriba. Desde la lógica del *convencionalismo semántico* y los *compromisos lingüísticos* que recaen sobre los juzgadores, no hay duda de que se puede llegar a cumplir con

las características de “ganancias” o “efectos” para las criptomonedas en tono de lo exigido por este elemento normativo del delito de lavado de activos.

Hay otro argumento que también sostiene la presente tesis, y es la que concierne al bien jurídico tutelado por este delito, que ya se pudo evaluar, supra, no es el orden socioeconómico (como bien jurídico instrumental), sino la administración de justicia – como un tipo especial de encubrimiento – y, conjuntamente, la evitación de masificación del delito fuente de lavado (que no es lo mismo que el bien jurídico tutelado por el propio delito fuente); así, como acuciosamente distingue Molina Fernández, el nivel de desvalor no se puede sostener única y exclusivamente en lo que al orden socioeconómico concierne (competencia igualitaria, tráfico de bienes adecuado o reglas regulativas de las mismas) o trae, sino más bien lo que, en lo profundo, termina por generar el propio acto de lavado, es decir, la proliferación de actividades criminales de índole lucrativa (2017, pp. 262-263), como en el caso que concierne al presente trabajo es la cibercriminalidad.

Se puede considerar, finalmente, que la pregunta base del presente apartado ha sido respondida afirmativamente: sí se puede tomar, dentro del alcance de objetos ilícitos constitutivos del tipo penal de lavado de activos, a las criptomonedas o criptoactivos.

Ataques Ransomware: ¿supuestos dentro del alcance de los delitos informáticos actualmente regulados y auténticos delitos previos?

Para entender la naturaleza de los *Ransomware*, debemos aclarar qué es un *malware*. Este último es un tipo de programa informático malintencionado que puede generar daños al sistema informático o a los datos contenidos en este que pertenecen a un usuario o, en otros casos, controlar lo modificar el propio sistema informático (Miró, 2012, p. 59). Su funcionamiento, en los más de casos, se da a partir de la apertura o ejecución de un programa infectado (véase, ejecutables

o archivos) (Mata y Guevara-Juárez, 2010, pp. 58-59) o, en otros casos, tener varios vectores de ataque, como son correos electrónicos – esparcimiento masivo por cuentas –, conexiones USB, plataformas web incorporadas con el programa malicioso, entre otras; de esto se desprende que el atacante posee una lista interminable de medios para dar acceso al programa maligno (Osorio-Sierra, Mateus-Hernández y Vargas-Montoya, 2020, p. 133).

De este género, se puede hablar del *Ransomware*, que es una especie de *malware* que tiene como principal objetivo secuestrar los datos informáticos del usuario y, en consecuencia, hacerlos inaccesibles. Sin embargo, esta modalidad de ataque se puede separar en dos. En primera línea, los Cripto-Ransomware disponen de un proceso de encriptación para cifrar datos informáticos, lo que va más allá de la propia accesibilidad del sistema informático que se use, es decir, en caso de que se logre eliminar el malware, los archivos seguirán encriptados porque dicho estado es autónomo de cualquier programa. En segundo término, aparecen los locker-Ransomware, que apuntan estrictamente a anular las terminales del arranque del sistema informático, bloqueando el acceso integral al dispositivo por parte del usuario. A diferencia de su similar, el estado de inaccesibilidad al sistema depende en estricto de la presencia del *malware*, por lo que, si se le elimina, se volverá a conseguir dominio de este o, en su defecto, bastará con la sola traslación del dispositivo de almacenamiento a otro equipo para hacer ineficaz la extorsión de la que se vale el pirata informático (Ávila, 2023, pp. 97-98). Se ha precisado de forma general los tipos de Ransomware; sin embargo, existen otros más que se van distinguiendo por su modo de ataque, la exigencia del atacante o el dispositivo al que se dirige (Ávila, 2023, p. 100).

Tal clase de ataques partió, se sabe, de pequeña a gran escala; del usuario informático común a grandes empresas o instituciones públicas contra las que se dispone un ataque *Ransomware* para poder obtener ganancias estratosféricas por su amplia capacidad operativa. No por nada, como bien menciona Pérez López, existió durante el año 2012 un cúmulo de más de 1000 denuncias vinculadas

a ataques Ransomware con resabios de otros mecanismos como *phishing* obtuvieron múltiples códigos prepago de proveedores de dinero electrónico que luego distribuían mediante "mulas" para retirar dinero en cajeros (2017, pp. 184-185), siendo así un problema de ciberseguridad prioritario para los Estados, con necesidades marcadas de inversión económica para su prevención (González, 2010, p. 94). No obstante, quizá el caso más famoso de un ataque *Ransomware* fue el producido contra la empresa Telefónica por el conocido "WannaCry" en el año 2017, y que también se propaló por más de 170 países. Este malware se aprovechaba de una vulnerabilidad del sistema operativo Windows (de amplio uso en el mundo). En la actualidad, las formas de utilizar estas herramientas maliciosas han mutado, hasta el punto de crear modelos de negocios denominados *Ransomware-as-a-Service* (RaaS), que consiste en contratar los servicios de operadores de Ransomware para efectuar ataques a víctimas y lograr el cifrado de archivos, como afiliados, enviando comisiones a dichos propietarios del RaaS (10 % a 30 % de la ganancia) (Paniagua, 2022, p. 14) como parte de un servicio.

Habida cuenta de estas problemáticas que afectan tanto a usuarios, instituciones, estados o, también, a escala global, fue celebrado en Budapest, en el año 2001, el Convenio sobre la Ciberdelincuencia, con el propósito de integrar y brindar a todos los países miembros lineamientos para una legislación contra la ciberdelincuencia, así como establecer regímenes de cooperación internacional. (Kiefer, 2018, p. 315). El Perú adoptó estos lineamientos y sirven como base para jueces y fiscales que tienen en sus manos casos vinculados a este orden.

Ahora bien, ¿qué distingue al *Ransomware* de otros *malware*? En estricto, la solicitud dineraria que se hace para revertir el estado de inaccesibilidad de los datos informáticos o de todo el sistema informático secuestrado. Habitualmente, se exige un pago (Bitcoins u otra moneda digital) a una billetera digital, con el fin de obtener el rédito económico mediante actos de transformación a dinero físico o mediante adquisiciones. Ya habiendo desentrañado que las ganancias mediante criptomonedas son definidas como "objeto ilícito" de lavado de activos,

y las conductas de conversión, transferencia o recepción de estos "bienes, efectos o ganancias", constitutivas de lavado, queda desentrañar en qué tipo penal se puede subsumir el "secuestro extorsivo" de datos informáticos y si este es ubicable como "delito fuente" de lavado.

Las dos primeras aproximaciones sobre el baremo de medición que hay que utilizar se ubican en los artículos 3, 4 y 8 de la Ley N.º 30096, Ley de Delitos Informáticos, publicada el 22 de octubre de 2013. Así, la caracterización típica de ambos es:

> "Artículo 3. Atentado a la integridad de datos informáticos
> El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, [...]."
> "Artículo 4. Atentado a la integridad de sistemas informáticos
> El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, [...]
> "Artículo 8. Fraude informático
> El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante [...], alteración, borrado, supresión, clonación de datos informáticos, [...] o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, [...]
> [...].»

Cada uno de estos tipos penales recurren, para su configuración, a las modalidades "deliberada e ilegítimamente", esto es, sin autorización o consentimiento del titular del objeto protegido, que es la intangibilidad informática como propiedad exhibida por el usuario al hacer uso de dichos datos o sistemas informáticos en su control (Espinoza, 2024, p. 79), que pueden ser desglosadas en otras cualidades más precisas, conforme el Convenio de Budapest:

"confidencialidad, integridad y disponibilidad de datos y sistemas informáticos" (Elías, 2014, p. 13). Sin embargo, el interés tutelado varía en el supuesto del artículo 8, ya que se puede considerar su pluriofensividad al afectar tanto a la misma intangibilidad informática (como medio) como el patrimonio del usuario, en la medida que el sistema o datos informáticos tengan un valor patrimonial autónomo o que, producto de dicho medio típico, se consiga un provecho económico (Pérez, 2019, p. 158). Tal apreciación resulta de importancia bentónica, toda vez que una ciberextorsión ataca de manera directa o intencionada a un usuario mediante su propalación (esto es, conocimiento de la situación típica que le determinaba en el momento relevante para la decisión su no-acción u no-omisión por la concreción pragmática de la norma de comportamiento –dolo–), impidiendo accesos que sin ella serían comunes (Lamas, 2024, p. 151).

Autores como Villavicencio Terreros, en el Perú, ha catalogado el artículo 3 como uno de mera actividad (puesto que no exige para su configuración un cambio de estado de cosas jurídico o material [cibernético] que vaya más allá de la conducta de borrado, daño, alteración o inaccesibilidad de los datos), mientras que a los artículos 4 y 8 materia de comentario, como de resultado (esto es, que para la realización del tipo no solo se debe inutilizar o perturbar la actividad del usuario, sino que esta actividad debe resultar en un cambio de estado de cosas avenido al impedimento del acceso o imposibilidad del funcionamiento, como ocurre en el ataque *Ransomware*; pero, además, en el fraude informático del artículo 8 se requiere la producción de un perjuicio patrimonial a tercero) (2014, pp. 292-293 y 297). Sin embargo, ya desde este punto, podemos observar que ni el tipo regulado en el artículo 3 y 4, ni tampoco el del artículo 8, copan las condiciones de realización antinormativa que deja exhibir un "secuestro informático".

De aquí surgen los primeros problemas cuando atendemos a las cualidades específicas de un ataque *Ransomware*: como se dijo, se hace inaccesible el dato (Cripto-Ransomware) o el sistema informático (locker-Ransomware) mediante el programa maligno, pero se exige, vía una amenaza de inaccesibilidad permanente

unido a un plazo para el envío de las criptomonedas. Estos casos terminan por emparejarse insólitamente a casos de extorsión, solo que ubicadas en el mundo digital: así como en este tipo penal los elementos de la conducta típica (Robles y Pastor, 2018, p. 280) se desglosan en el uso de violencia o intimidación (advertencia de bloqueo permanente de los datos), coacción sobre el sujeto pasivo (usuario) para un hecho fuera de su voluntad libre (dar criptomonedas) y la ejecución del mismo titular del bien jurídico de un acto jurídico con efectos patrimoniales que implican una idónea conducta de perjuicio (envío de criptomonedas como medio de cambio).

Sin embargo, nadie se atrevería a subsumir estas conductas como constitutivas de extorsión en un sentido estricto; básicamente, porque la naturaleza de este tipo penal es entendida desde su materialidad: amenazas o violencia contra la persona *de* forma directa o indirecta en el mundo real, mas no en la digitalidad. Aunque el propio artículo 8 utilice una figura de amplia extensión interpretativa cuando dice cualquier interferencia o manipulación (Espinoza, 2024, p. 97), el ataque *Ransomware* tiene cualidades lesivas especiales que no se pueden encuadrar específicamente allí. Sin embargo, es interesante cómo otra parte de la doctrina, bajo la premisa de que se trata de un *medio* para la comisión de extorsión, ubica la conducta del ataque informático como parte de su *iter criminis*, apelando a un concurso de leyes (Kiefer, 2018, pp. 341-342). Esta también se resolvería como una solución, pero se encontrará ante cuestionamientos vinculados a la naturaleza casi común en doctrina sobre lo que representa "violencia o intimidación" en sentido estricto.

Si como dice Sánchez-Ostiz (2008, p. 472) el juicio de aplicación de la ley al hecho es un juicio de carácter realizativo, porque afirmamos que *x* constituye *y*, por principio de legalidad, no sería enteramente competente decir, por defecto, que solamente se trata de un fraude informático, sino de un "probable" concurso de fraude, atentado a la integridad de datos informáticos o de sistemas informáticos y coacciones (artículo 151 del Código Penal peruano). Sin embargo,

como bien enuncia García Cavero, el fundamento del concurso es permitir al juzgador determinar que la(s) conducta(s) del agente en la situación concreta definen una concreción o adecuación a tantos otros tipos penales aplicables al mismo tiempo, siendo una especial forma de aparición del hecho punible (García, 2019, p. 862); por lo cual, se puede deducir que entre cada tipo penal existe una autonomía que otro tipo penal, por especialidad, absorción o accesoriedad, no conduce. Asimismo, si se asumiese como adecuada la postura de concurso entre los delitos de atentado a la integridad de datos o sistemas informáticos (arts. 3 y 4, Ley N.º 30096) y extorsión, también se suscitan problemas de subsunción: si la extorsión en sí se caracteriza por ejecutar un acto violento o intimidatorio sobre otra persona para realizar un desprendimiento patrimonial (Serrano Gómez et. al., 2017, p. 292), el atentado contra datos o sistemas informáticos termina más bien convirtiéndose en una modalidad del tipo, por lo cual se estaría sancionando dos veces el hecho de provocar el desprendimiento patrimonial (por la intimidación y por la propia inaccesibilidad), vulnerando el principio de ne bis in ídem (Velásquez, 2023, p. 94). Aquí nos encontramos ante un caso de tales ribetes, que tal y como va regulado, no respeta los contenidos de proporcionalidad cardinal que von Hirsch postulaba para definir la severidad de las penas en función de la gravedad del hecho lesivo (expresión de desaprobación por la comunidad como razón fuerte para sancionar), es decir, si se admitiese la sanción que, por ejemplo, plantean cada uno de los delitos aquí analizados, diríase que el marco de anclaje punitivo con otros tipos penales de la parte especial del Código Penal no se encuentra debidamente coligado, porque el ataque *Ransomware* genera un estado de zozobra en el usuario que ve en la incertidumbre del estado de sus datos informáticos el motivo medular por el que accede a la exigencia del atacante informático (1998, pp. 45-46), considerando entonces un mayor desvalor de la acción (la conducta extorsiva digital) y de resultado (el perjuicio patrimonial) siendo pluriofensivo (Mayer y Oliver, 2020, pp. 174-175). Así, la única solución –más o menos– a largo plazo estimable es la de construir un tipo penal derivado

del fraude informático que establezca los supuestos concretos de "secuestro informático", para definir de forma precisa la entidad lesiva de su comisión y pueda encontrarse una armonización con las bases de la legalidad penal y la interpretación.

Existen problemáticas en el ámbito de la tipicidad de los ataques *Ransomware* con el delito de "fraude informático", como actualmente se regula. Así, la pregunta que fue formulada al inicio del trabajo no puede ser respondida con total certeza de manera afirmativa, aunque no quepa la menor duda de que, por su naturaleza, el propio tipo penal de fraude informático es un delito que puede generar ganancias ilegales, como bien exige el artículo 10 del propio Decreto Legislativo N.º 1106, sobre lavado de activos.

Propuesta de solución

Con todo lo expresado, las soluciones se pueden ampliar en dos frentes generales: primero, de *lege lata*, la interpretación literal desde una perspectiva pragmática y analítica del derecho penal permite incluir a las criptomonedas dentro de los supuestos de "bienes, efectos o ganancias" constitutivos de lavado de activos, incluso aunque no sean estas reconocidas. Asimismo, el tipo penal de lavado de activos, así tipificado, no genera problemas sustanciales de tipicidad para adecuarse a los nuevos entornos de cibercriminalidad y posee una capacidad de rendimiento admisible desde criterios de dogmática penal. No obstante, el problema de configuración típica del delito de fraude informático para los ataques *Ransomware* produce una incertidumbre en los criterios para utilizar dichos supuestos como *delitos previos* de lavado, aunque

De *lege ferenda*, sin embargo, tal y como, por ejemplo, ya efectuó Europa a través del Reglamento de Mercado de Criptoactivos [MiCA] – puesta en marcha desde el 2023 –, debe pensarse a futuro en una regulación nacional sobre las formas de transar con las criptomonedas existentes o por existir, partiendo de sus peculiaridades y modos de obtención. Para ello, quizá, podría atenderse a

la Resolución N.º 02648-2024, de la SBS, como primera aproximación a una regulación sectorial para una de índole nacional.

Finalmente, sobre el aspecto vinculado a la tipicidad de los ataques *Ransomware*, lo más preciso será que el legislador peruano apele a un juicio de tipificación necesario en este contexto de los "secuestros informáticos" en la Ley N.º 30096, sancionando con una pena privativa de libertad que se encuentre a caballo entre el tipo penal de extorsión (no menos de 10 ni más de 15 años) y el fraude informático (no menos de 4 ni más de 8) al que, mediando amenaza de hacer inaccesibles los datos o sistema informáticos del usuario a través de un ataque *Ransomware*, obligue a otro a otorgar un provecho económico, a través de cualquier sistema o plataforma de pago y con cualquier activo (sea digital o físico).

Conclusiones

No cabe duda de que la inmersión de la sociedad contemporánea en las nuevas tecnologías de la información, la actividad digital y la globalización han iniciado disquisiciones intensas en la dogmática penal; sobre todo, porque implican una mutación conceptual de las reglas de imputación y valoración o medición que debe realizar el intérprete de la ley. Asistimos como espectadores privilegiados a una nueva forma de entender el derecho penal, no solo desde lo meramente teórico o formal, sino también desde las formas pragmáticas de comprender la cibercriminalidad. Tales retos requieren, por supuesto, respuestas desde ambos flancos – como bien se ha propuesto –: de lege lata, para manejar con correctitud la interpretación de los tipos penales de que ahora disponemos para adscribir responsabilidad penal por la utilización de *Ransomware* con la finalidad subjetiva de medrar patrimonialmente al usuario informático – a través de una interpretación ciertamente insuficiente, pero necesaria, por ahora, del artículo 8 (fraude informático) de la Ley N.º 30096 que se constituiría como delito fuente de lavado de activos; de *lege ferenda*, una apuesta normativa por incluir de forma

taxativa a las criptomonedas como medios de pago con respaldo financiero, que deslinden cualquier posibilidad de negación interpretativa y, además, la configuración de un tipo penal autónomo de "secuestro informático" que permita delimitar con precisión la dimensión de injusto que esta conducta traería para los intereses merecedores de tutela en la era digital. Valgan verdades, este ya no se puede considerar un problema del futuro, pues ya es un gran atrenzo del presente, y la legislación peruana no puede negarse (ya) al cambio de paradigma.

Bibliografía

Agustina, José. (2021). Nuevos retos dogmáticos ante la cibercriminalidad: ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma? *Estudios penales y criminológicos, 42*, 705-777. https://doi.org/10.15304/epc.41.7433

Alpaca Pérez, Alfredo. (2022). *Teoría de las normas e injusto penal*. (1° ed.). Madrid: Marcial Pons.

Álvarez Díaz, Luis. (2019). Criptomonedas: Evolución, crecimiento y perspectivas del Bitcoin. *Población y Desarrollo, 25*(49), 130-142.

Ávila Niño, Fredy (2023). Ransomware, una amenaza latente en Latinoamérica. *Intersedes. Revista electrónica de las sedes regionales de la Universidad de Costa Rica, 24*(49), 92-119. https://doi.org/10.15517/isucr.v24i49.50765

Barroilhet Díez, Agustín. (2019). Criptomonedas, economía y derecho. *Revista chilena de derecho y tecnología, 8*(1), 29-67. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842019000100029

Brandom, Robert (2005). *Hacerlo explícito: Razonamiento, representación y compromiso discursivo*. (1° ed.). Barcelona: Herder.

Blanco Cordero, Isidoro. (2012). *El delito de blanqueo de capitales*. (3° ed.). Navarra: Thomson Reuters-Aranzadi.

Cabanchik, Samuel. (2015). La gramática de la acción: Wittgenstein y el pragmatismo. En P. Quintanilla & C. Viale (Eds.), *El pensamiento pragmatista en la actualidad: Conocimiento, lenguaje, religión, estética y política*. Lima: Fondo Editorial Pontificia Universidad Católica del Perú, 15-26

Cabrera Soto, Marian, & Lage Cordorniu, Carlos. (2021). Criptomonedas: ¿Qué son y qué pretenden ser? *Economía y Desarrollo, 166*(1), 1-21. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0252-85842022000100008

Camps, Victoria. (1976). *Pragmática del lenguaje y filosofía analítica*. (1° ed.). Alicante: Ediciones Península.

Egaña Huertos, Javier. (2019). *Criptomonedas: Pasado, presente y ¿futuro?* [Trabajo de fin de grado Universidad de Sevilla]. Sevilla: Depósito de Investigación Universidad de Sevilla.

Elías Puelles, Ricardo. (2014). Luces y sombras en la lucha contra la delincuencia informática en el Perú. *Hiperderecho*, 2-24. https://hiperderecho.org/2014/07/luces-y-sombras-de-la-delincuencia-informatica-en-peru/

Espinoza Calderón, Victor. (2022). *Delitos informáticos y nuevas modalidades delictivas*. (1° ed.). Lima: Instituto Pacífico.

Fonseca Pérez, Robinsson, & Tacuma Amador, John. (2018). El impacto de las criptomonedas en el Perú. En *Fundación Universitaria de la Cámara de Comercio de Bogotá* (pp. 1-19). http://hdl.handle.net/11520/26876

Flores Zerpa, Allen. (2022). La legalidad como regla constitutiva para la aplicación de la ley penal. En A. Flores Zerpa & J. Urquizo Olaechea (Dirs.), *Código Penal del Bicentenario: Estudios de derecho penal actual*. (Tomo II). Lima: Gaceta Jurídica.

García Cavero, Percy (2013). *El delito de lavado de activos*. Lima: Jurista Editores.

García Cavero, Percy (2019). *Derecho Penal: Parte general*. (3° ed.). Lima: Ideas Solución Editorial.

García-Ramos Lucero, Miguel, & Rejas Muslera, Ricardo (2022). Análisis del desarrollo normativo de las criptomonedas en las principales jurisdicciones: Europa, Estados Unidos y Japón. *Revista de los estudios de Derecho y Ciencia Política, 35*, 1-13. https://raco.cat/index.php/IDP/article/view/n35-garcia-ramos

Gálvez Villegas, Tomás (2016). *Autonomía del delito de lavado de activos: Cosa juzgada y cosa decidida*. (1° ed.). Lima: Ideas Solución Editorial.

González Cussac, José. (2010). Estrategias legales frente a las ciberamenazas. En: Ministerio de Defensa. *Ciberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio*. (Núm. 149), 85-127.

Hruschka, Joachim. (2009). *Imputación y derecho penal: Estudios sobre la teoría de la imputación*. (2.ª ed.). Montevideo/Buenos Aires: BdeF.

Iturralde Sesma, Victoria. (2014). *Interpretación literal y significado convencional. Una reflexión sobre los límites de la interpretación jurídica*. Madrid: Marcial Pons.

Klatt, Matthias. (2012). El límite del tenor literal. En J. P. Montiel (Ed.), *La crisis del principio de legalidad en el nuevo Derecho penal: ¿decadencia o evolución?* Madrid: Marcial Pons.

Kiefer, Patricia. (2018). Daño informático. En D. Dupuy (Dir.) & M. Kiefer (Coord.), *Cibercrimen: Aspectos de Derecho penal y procesal penal, cooperación internacional, recolección de evidencia digital, responsabilidad de los proveedores de servicios de Internet*. (Tomo I). Montevideo/Buenos Aires. BdeF.

Lamas Suárez, Gerardo. (2024). *Lavado de activos y criptoactivos*. Lima: Instituto Pacífico.

Lascuraín Sánchez, Juan. (2018). *Pena, principios y empresa: Estudios sobre los principios penales y sobre los delitos de empresa*. Lima: A&C.

Mañalich Raffo, Juan Pablo. (2010). Norma e imputación como categorías del hecho punible. *Revista de Estudios de la Justicia, 12*, 169-190. https://repositorio.uchile.cl/handle/2250/126658

Mañalich Raffo, Juan Pablo. (2022). ¿La salud pública como bien jurídico colectivo? Una (nueva) contribución a la teoría general de la parte especial. En A. Flores Zerpa & J. Urquizo Olaechea (Dirs.), *Código Penal del Bicentenario: Estudios de derecho penal actual*. (Tomo II). Lima: Gaceta Jurídica.

Mañalich Raffo, Juan Pablo. (2024). La interpretación de la ley penal bajo la "prohibición de analogía". Una reconstrucción desde el pragmatismo semántico. *Revista Chilena de Derecho*, vol. 51, n.° 3, 63-91.

Mata Villalpando-Becerra, Isaac, & Guevara-Juárez, Oscar. (2010). Virus informáticos, todo un caso, pero no perdido. *CienciaUAT, 4*(4), 56-61.

Mendoza Llamacponcca, Fidel. (2022). *Lavado de activos y criminalidad empresarial*. (1° ed.). Lima: Jurista Editores.

Mendoza Llamacponcca, Fidel. (2016). El delito fuente en el lavado de activos. En J. Hurtado Pozo (Dir.) & F. Mendoza Llamacponcca (Coord.), *Temas de derecho penal económico: empresa y Compliance. Anuario de Derecho penal 2013-2014*, n.° 19, Fondo Editorial PUCP, 293-358.

Nieto Martín, Adán (2022). Blanqueo de capitales: Extraterritorialidad y doble incriminación. En V. Gómez Martín et al. (Dirs.), *Un modelo integral de derecho penal: Libro homenaje a la profesora Mirentxu Corcoy Bidasolo*. Madrid: Boletín Oficial del Estado, 1273-1289.

Osorio-Sierra, Andrés, Mateus-Hernández, Milton, & Vargas-Montoya, Hector. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *Revista UIS Ingenierías, 19*(3), 131-142. https://doi.org/10.18273/revuin.v19n3-2020013

Paniagua Soza, Ramón. (2022). *Anatomía del Ransomware*. [Trabajo de fin de máster en Seguridad de las Tecnologías de la Información y de las Comunicaciones, Universitat Oberta de Catalunya]. Repositorio Institucional Universitat Oberta de Catalunya. http://hdl.handle.net/10609/145831

Pérez López, Jorge. (2019). *Delitos regulados en leyes penales especiales*. (1° ed.). Lima: Gaceta Jurídica.

Pérez López, Xesús. (2017). Las criptomonedas: Consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y española. *Revista de Derecho Penal y Criminología, 3ª* época (18), 147-181. https://revistas.uned.es/index.php/RDPC/article/view/24454

Pilacuán Cadena, Johana, Espinoza Herrera, Xavier, Carreño Llaguno, Steven, & Palacios Alcivar, Baltazara. (2021). Criptomonedas: Funcionamiento, oportunidades y amenazas. *Res non verba: Revista científica, 11*(2), 174-193. https://doi.org/10.21855/resnonverba.v11i2.604

Posada-Maya, Ricardo (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: De una realidad física a una realidad virtual. *Revista Nuevo Foro Penal, 13*(88), 72-112.

Prado Saldarriaga, Víctor. (2019). Lavado de activos mediante criptomonedas en el Perú: Problemas y alternativas. *Lex, 24*, 161-178. https://revistas.uap.edu.pe/ojs/index.php/LEX/article/view/1815/1983

Prado Saldarriaga, Víctor. (2023). *Lavado de activos virtuales. Nueva tipología del crimen organizado en el Perú*. Lima: Gaceta Jurídica.

Roxin, Claus (1997). *Derecho penal: Parte general*. (Tomo I, 1° ed.) (3° reimpresión). Madrid: Civitas.

Robles Planas, Ricardo, & Pastor Muñoz, Nuria. (2018). Tema 12. Delitos contra el patrimonio (III). En J. Silva Sánchez (Dir.) & R. Ragués i Vallés (Coords.), *Lecciones de derecho penal: Parte especial*. (5.ª ed.). Barcelona: Atelier.

Sánchez Málaga, Armando. (2016). *Una teoría para la determinación del dolo: Premisas teóricas e indicadores prácticos*. (1° ed.). Montevideo/Buenos Aires. BdeF.

Sánchez-Ostiz, Pablo. (2008). *Imputación y teoría del delito: La doctrina kantiana de la imputación y su recepción en el pensamiento jurídico-penal contemporáneo*. (1° ed.). Montevideo/Buenos Aires, BdeF.

Serrano Gómez, Alfonso et al. (2017). *Curso de derecho penal: Parte especial*. (4° ed.). Madrid: Dykinson.

Velásquez Velásquez, Fernando. (2023). *Fundamentos del derecho penal: Parte general*. (4° ed.). Valencia: Tirant lo Blanch.

Villavicencio Terreros, Felipe. (2014). Delitos informáticos. *Revista Ius et Veritas, 49*, 284-304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Villegas Paiva, Elky. (2018). Determinación del objeto de protección (bien jurídico penal) en el delito de lavado de activos. En: Urquizo Olaechea, J. et al. *El delito de lavado de activos*. Lima: Gaceta Jurídica, 225-262.

Von Hirsch, Andrew. (1998). *Censurar y castigar*. Madrid: Trotta.

Wittgenstein, Ludwig. (2014). *Investigaciones filosóficas (Die philosophische Untersuchungen)*. Madrid: Gredos.