Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales

Diciembre/2021

El GAFILAT agradece la asistencia técnica brindada por la Cooperación Alemana para el Desarrollo, implementada por la Deutsche Gesellschaft für Iternationale Zusammenarbeit (GIZ) para la elaboración del presente documento que contó además con el apoyo de Hernán Blanco. El contenido de esta publicación es completa responsabilidad del Grupo de Acción Financiera de Latinoamérica (GAFILAT).

ÍNDICE

I. INTRODUCCIÓN

El desarrollo y la masiva adopción, a nivel global, del uso de Internet, de computadoras personales, dispositivos móviles, servicios y plataformas asociadas con aquellos, ha tenido un vasto impacto sobre la velocidad y naturaleza de las interacciones sociales, del que no están exentos las transacciones comerciales o financieras[1]. Una de las manifestaciones de la transición de la actividad humana desde el mundo físico al virtual ha sido el surgimiento de activos virtuales (AV), entendidos, conforme la definición del Grupo de Acción Financiera Internacional (GAFI), como una representación digital de valor que puede ser intercambiada o transferida digitalmente, y utilizada como forma de pago o instrumento de inversión[2]. En este escenario, el desarrollo más importante ha sido, sin dudas, la creación de las criptomonedas, que desde su nacimiento en 2008 -con la publicación del célebre "White paper" de Satoshi Nakamoto sobre el Bitcoin[3]- se convirtieron en uno de los mercados no regulados más grandes del mundo[4].

La aparición de las criptomonedas y de la tecnología de "libro mayor distribuido" (distributed ledger technology o DLT) subyacente (ejemplificada en la Blockchain), constituye un fenómeno que bien puede estar llamado a revolucionar positivamente muchos aspectos del sistema financiero. Sin embargo, como muchas innovaciones, también es susceptible de ser explotada para favorecer la actividad ilícita. Ello así, desde que el uso de bitcoins -o de las criptomonedas similares que surgieron con posterioridad, conocidas genéricamente como "Altcoins"- permite a cualquier persona -con independencia de si desarrolla una actividad lícita o delictiva- transferir valores casi instantáneamente a un costo muy bajo o inexistente, con mínimas barreras para el ingreso y sin dejar rastro en papel.

Los criminales, usualmente ágiles para adoptar nuevas tecnologías- advirtieron rápidamente que las particulares características del Bitcoin podían ser útiles para sus intereses. Esto derivó en que se recurriese a dicha criptomoneda para facilitar el surgimiento de mercados online en la "Red oscura" de la Internet, en los que hasta el día de hoy se intercambian bienes y servicios (en su mayoría) ilegales a cambio de bitcoins.

[1] Ver: European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses", Policy Department for Citizen's Rights and Constitutional Affairs, mayo 2018, pág. 21.
[2] De esta definición están excluidas las representaciones digitales de monedas fiduciarias ("Fiat currencies"), securities u otros activos financieros comprendidos en otros tramos de las Recomendaciones del GAFI.
[3] Ver: NAKAMOTO, Satoshi: "Bitcoin: A peer-to-peer electronic cash system", 2008.
[4] Con relación a esa cuestión, un trabajo académico publicado en 2019 destacó la aparición de más de 170 "criptofondos" (fondos de inversión dedicados exclusivamente a criptomonedas) con activos por encima de los 2.300 millones de dólares. Ver: FOLEY, Sean / KARLSEN, Jonathan R. / PUTNINS, Talis J.: "Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?", The Review of Financial Studies, Vol. 32, N° 5, 2019, págs. 1798/1853.

La adopción del Bitcoin como la principal moneda de cambio de la actividad criminal en el ciberespacio quedó de manifiesto a partir del cierre de Silk Road, el primer mercado ilícito online, por parte de las autoridades de los EE. UU. en el año 2013. Desde entonces, se han reiterado las menciones al uso de criptomonedas con fines ilícitos en documentos de distintas agencias u organizaciones dedicadas al cumplimiento de la ley. Así, los informes de Evaluación de Riesgo del Crimen Organizado en Internet de Europol (IOCTA, por sus siglas en inglés) puntualizaron la creciente adopción del Bitcoin como moneda de cambio preferida entre las organizaciones criminales, sustituyendo a otros AV[5]. En tal contexto, un estudio reciente estima que un 26% de los/las usuarios/as de Bitcoin y el 46% de las operaciones con esa criptomoneda están asociadas con la actividad ilegal[6].

En lo que respecta específicamente al lavado de activos y el financiamiento del terrorismo (LA/FT), una de las primeras alusiones a la posibilidad de utilizar bitcoins a tal efecto puede encontrarse en un reporte del FBI elaborado en 2012[7]. Desde entonces, numerosos documentos de organizaciones dedicadas a la prevención del delito en general y del lavado de activos en particular han confirmado la consolidación del recurso a las criptomonedas como método para reciclar fondos ilícitos provenientes no solo de actividades criminales en el ciberespacio (venta online de bienes y servicios ilegales, ramsonware, extorsión, sustracción de AV mediante hackeo, etc.) sino también de delitos cometidos en el mundo físico.

El GAFI ya había advertido sobre la posibilidad de que la evolución en las tecnologías de la información y la comunicación (TICs) generase nuevas vulnerabilidades y tipologías de LA/FT en su reporte sobre nuevos métodos de pago, publicado en 2006[8]. La cuestión fue revisitada en un informe de 2010[9] en el que se destacó el crecimiento del número de casos de uso ilícito de los nuevos métodos de pago reportado por los países miembros, a la vez que se puso de resalto la importancia de implementar medidas de debida diligencia del cliente (DDC) en los puntos de acceso a estas nuevas tecnologías, como vía para mitigar los riesgos de LA.

Posteriormente, las criptomonedas fueron adquiriendo cada vez mayor preponderancia entre los nuevos métodos de pago hasta ocupar un lugar central como moneda de cambio en las transacciones ilícitas. El GAFI se ocupó del tema en el reporte sobre "monedas virtuales" publicado en 2014[10], en el que analizó los riesgos de LA/FT vinculados a las criptomonedas, a las que

[5] Ver: European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses", Policy Department for Citizen's Rights and Constitutional Affairs, mayo 2018, págs. 15/18.
[6] Ver: FOLEY, Sean / KARLSEN, Jonathan R. / PUTNINS, Talis J.: "Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?", The Review of Financial Studies, Vol. 32, N° 5, 2019, págs. 1798/1853. Cabe destacar, no obstante, que desde el año 2016, la proporción de actividad en Bitcoin vinculada al tráfico ilegal ha ido declinando en forma constante, en gran medida debido al rápido crecimiento del interés especulativo en Bitcoin merced al incremento en el valor de esa moneda.
[7] Ver: Federal Bureau of Investigations (FBI): "Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity", Criminal Intelligence Section / Cyber Intelligence Section, abril 2012.
[8] Ver: GAFI: "Report on new payment methods", octubre 2006.
[9] Ver: GAFI: "Money laundering using new payment methods", octubre 2010.
[10] Ver: GAFI: "Virtual currencies. Key definitions and potential AML/CFT risks", junio 2014.

consideró particularmente vulnerables a la explotación para fines delictivos. Un año después, en su "Guía para un enfoque basado en el riesgo: monedas virtuales"[11], el GAFI fijó una serie de pautas para una mejor aplicación de las 40 Recomendaciones a efectos de minimizar los potenciales riesgos, destacando, una vez más, la conveniencia de centrar las medidas de ALA/CFT en la intersección entre el ecosistema de las criptomonedas y el de la moneda fiduciaria.

En estos reportes, el GAFI identificó como principales rasgos que incrementan el riesgo de LA/FT a los siguientes: a) el anonimato asociado al diseño de los AV (que incluso puede incrementarse mediante el recurso a herramientas como los "mezcladores" o "conmutadores" ("Mixers" o "Tumblers"); b) la posibilidad de que una misma persona controle múltiples "monederos virtuales"; c) el carácter descentralizado de la mayoría de las criptomonedas (que supone la inexistencia de un órgano de supervisión que pueda ser alcanzado por la normativa de ALA/CFT); y d) el alcance global de muchas de ellas, entre otros.

En atención a ello, en octubre de 2018 el GAFI actualizó la Recomendación 15, referida a las obligaciones fundamentales de los países miembros con respecto al enfoque basado en el riesgo (EBR) en orden a las nuevas tecnologías, para de clarificar su aplicación a los AV, las actividades relacionadas con los mismos, y a los proveedores de servicios de AV (o PSAV)[12]. Luego, en 2019, el GAFI adoptó una nueva Nota Interpretativa a la Recomendación 15 a fin de precisar aún más el modo en que deben aplicarse los estándares y las medidas para la regulación y supervisión de las actividades de los AV y PSAV.

Ese mismo año, el GAFI publicó una guía con recomendaciones para un EBR[13]. En dicha guía destacó los riesgos derivados de una aplicación inconsistente, a nivel internacional, de los parámetros del organismo en materia de obligaciones de ALA/CFT de los PSAV, señalando que, en atención al carácter inherentemente transfronterizo del Internet, un PSAV basado en una jurisdicción puede ofrecer sus productos y servicios a clientes localizados en cualquier otra, en la que esté sujeto a diferentes deberes y estándares de supervisión, lo cual es motivo de preocupación cuando el prestador se encuentra en una jurisdicción con controles débiles o inexistentes. Luego, en septiembre de 2020, el GAFI hizo pública una guía actualizada sobre indicadores de riesgo y alertas ("Red flags") en materia de AV[14].

[11] Ver: GAFI: "Guidance for a risk-based approach: Virtual currencies", junio 2015.
[12] Definidos por el GAFI como una persona natural o legal (no alcanzada por alguna otra definición en las Recomendaciones), que lleve a cabo comercialmente una o más de las siguientes operaciones en beneficio de otra persona legal o natural: *i)* intercambio entre activos virtuales y monedas fiduciarias; *ii)* intercambio entre una o más clases de activos virtuales; *iii)* transferencia de activos virtuales (entendida como el desplazamiento de dichos activos de una dirección virtual o cuenta a otra); *iv)* custodia y/o administración de activos virtuales o de instrumentos que permitan el control de activos virtuales; y *v)* participación en o provisión de servicios financieros vinculados a la oferta y/o venta de activos virtuales por parte de los usuarios.
[13] Ver: GAFI: "Virtual assets and virtual assets service providers. Guidance for a risk-based approach", junio 2019. En octubre de 2021, el organismo publicará una actualización de la referida guía.
[14] Ver: GAFI: "Money laundering and terrorist financing red flag indicators associated with virtual assets", septiembre 2020.

Las vulnerabilidades resultantes de las divergencias regulatorias se acentúan debido al amplio rango de proveedores existentes en el ámbito de los AV y su presencia en múltiples jurisdicciones, que dificultan la determinación de qué entidades o personas (físicas o jurídicas) involucradas en esa clase de operaciones están sujetas a medidas de ALA/CFT y cuál o cuáles países son responsables de regular sobre la cuestión y supervisar su cumplimiento. Asimismo, en un reporte posterior referido a las "así llamadas monedas estables" ("so-called stablecoins")[15], el GAFI reconoció la existencia de idénticos riesgos en relación con esa clase de AV[16].

A nivel regional, el Grupo de Expertos para el Control del Lavado de Activos de la Organización de los Estados Americanos (OEA) destacó los riesgos de LA/FT asociados a las criptomonedas. En el continente europeo, la cuestión de las monedas virtuales fue analizada por primera vez en un reporte del Banco Central Europeo (ECB, por sus siglas en inglés) de 2012[17]. El siguiente año, la Autoridad Bancaria Europea (EBA) publicó una alerta a los consumidores con respecto a los AV[18], indicando que el uso ilícito de dichos activos podía poner en peligro sus fondos. A fin de mitigar dichos riesgos, recomendó incluir a las monedas virtuales en el alcance de la Directiva Europea Anti-Lavado (AMLD, por sus siglas en inglés). Luego, en una opinión emitida en 2014[19], la misma entidad identificó más de 70 riesgos asociados a las monedas virtuales, a la vez que reiteró la necesidad de regulación sobre la materia. La EBA reiteró esta postura en una opinión posterior, publicada en 2016[20].

Por otro lado, en el Análisis del Crimen Organizado en Internet (IOCTA, por sus siglas en inglés) de 2019 se resaltó el uso de criptomonedas para facilitar el crimen en la red, exhortándose a las agencias de orden público (AOP) a desarrollar, compartir y propagar conocimientos sobre como reconocer, rastrear, incautar y recuperar AV[21]. Más recientemente, un documento conjunto de Interpol, el Instituto para el Gobierno de Basilea y Europol también enfatizó la importancia de que los países o estados miembros establezcan marcos regulatorios y procesos claros para propender al registro y supervisión en materia de ALA/CFT de los PSAV, en línea con las recomendaciones del GAFI[22]. En igual sentido, tanto el Instituto para la Estabilidad Financiera como el Comité de Basilea sobre Supervisión Bancaria publicaron, en 2020, documentos poniendo de resalto la

[15] Así se autodenominan las criptomonedas que cuentan con el apoyo de grandes empresas tecnológicas o financieras, lo cual se pregona a su respecto una mayor estabilidad que las restantes criptomonedas.
[16] Ver: GAFI: "FATF report to the G20 Ministers and Central Bank governors on the so-called stablecoins", junio 2020.
[17] Ver: European Central Bank (ECB): "Virtual currency schemes", Frankfurt, octubre 2012.
[18] Ver: European Banking Authority (EBA): "Warning to consumers on cryptocurrencies", diciembre 2013.
[19] Ver: European Banking Authority (EBA): "EBA opinion on 'virtual currencies'", EBA-Op-2014-08, julio 2014.
[20] Ver: European Banking Authority (EBA): "Opinion of the European Banking Authority on the EU Commision's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (AAMLD)", EBA-OP-2016-07, Agosto 2016.
[21] Ver: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 2.
[22] Ver: INTERPOL / Basel Institute on Governance / EUROPOL: "Recommendations 4th Global Conference on Criminal Finances and Cryptocurrencies", noviembre 2020.

existencia de riesgos de LA/FT derivados del uso de cripto activos y la necesidad de una regulación adecuada[23].

Asimismo, durante la última década se ha acentuado la preocupación de los organismos internacionales con relación al posible uso de criptomonedas para facilitar la financiación del terrorismo, en especial como medio para canalizar en forma (semi) anónima donaciones o aportes hacia organizaciones terroristas. En esa dirección, el reporte del ECB sobre monedas virtuales de 2012 ya enfatizaba, en relación con el surgimiento del Bitcoin, que el grado de anonimato asociado a ese activo suponía un riesgo en orden al FT. A su vez, la EBA explicó, en 2014, que el riesgo de FT derivado del uso de monedas virtuales deriva de que los esquemas referidos a estos activos no están restringidos por límites jurisdiccionales, ya que son aceptados a través de las fronteras. Destacó, en esa dirección, que lo único que se requiere para operar con AV es una conexión a Internet; que la infraestructura subyacente se encuentra distribuida en derredor del globo, dificultando la interceptación de transacciones; y que éstas tienden a no ser reversibles[24].

Con posterioridad a los ataques terroristas ocurridos en Francia en 2015, la Comisión Europea propuso analizar las vulnerabilidades en las políticas de prevención del FT en ese continente, incluyendo las vinculadas a la adquisición y uso anónimo de monedas virtuales. A consecuencia de ello, en 2016 la Comisión Europea aceptó incluir medidas similares a las recomendadas por el GAFI y la EBA en orden a los AV en la 5ª Directiva Europea Anti-Lavado (5AMLD), que fue adoptada por el Parlamento Europeo en abril de 2018 y por el Consejo de Europa en mayo del mismo año.

Sin perjuicio de lo expuesto, un reporte del Parlamento Europeo de 2018 señaló, en relación con estos riesgos, que el número de extremistas que han recurrido a las criptomonedas (atraídos por la percepción de anonimato y su estructura descentralizada) todavía es menor. Se explicó, en tal sentido, que, en el corto plazo, el riesgo más significativo proviene de la posibilidad de utilizar AV para adquirir elementos ilegales (como armas o explosivos) en la Red oscura, o para reunir fondos mediante donaciones anónimas[25]. El reporte concluye, sin embargo, que por el momento los AV no proveen beneficios sustanciales para la mayoría de las organizaciones terroristas en comparación con las metodologías ya establecidas de FT[26].

El desafío que supone el mantenimiento de los estándares de ALA/CFT frente al nuevo escenario planteado por la generalización, a nivel global, del uso de criptomonedas como moneda de cambio (tanto en el marco de transacciones lícitas como ilícitas) no se agota en la actualización de los

[23] Ver: Basel Committee on Banking Supervision: "Prudential treatment of cryptoasset exposures", Bank for International Settlements (BIS) Consultative Document, junio 2021; y Financial Stabilty Institute (FSI): "Supervising cryptoassets for anti-money laundering", FSI Insights on Policy Implementation, N° 31, BSI, abril 2021.
[24] Ver: European Banking Authority (EBA): "EBA opinion on 'virtual currencies'", EBA-Op-2014-08, julio 2014, pág. 33 § 120.
[25] Al respecto, un reporte del GAFI del 2018 destaca un caso en el que una página web de propaganda de la organización terrorista ISIS fue explotada para solicitar donaciones en Bitcoin (ver: GAFI: "Financing of terrorism for recruitment purposes", octubre 2018).
[26] Ver: European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses", Policy Department for Citizen's Rights and Constitutional Affairs, mayo 2018, pág. 27.

marcos regulatorios para que las obligaciones de registro, información y reporte alcancen también a los AV y PSAV que continuamente se incorporan a los mercados financieros mundiales. Ello, toda vez que dadas las especiales características de los AV, su explotación con fines ilícitos puede incidir sobre la efectividad de las investigaciones patrimoniales y sobre la posibilidad de incautar o decomisar activos de origen o destino ilícito, ambos aspectos que han sido considerados por el GAFI como elementos centrales de los estándares de ALA/CFT y de los regímenes nacionales sobre la materia[27].

En efecto, la circunstancia de que la operatoria con criptomonedas y otros AV similares se desarrolle casi enteramente en un ámbito virtual y casi completamente desvinculado del mundo físico (el denominado "ciberespacio"), impone un cambio de paradigma en todo lo relacionado a las estrategias, métodos y herramientas utilizadas para investigar, perseguir y sancionar maniobras de LA/FT cometidas mediante AV, así como para la incautación y decomiso de los fondos involucrados en las mismas.

Ello así, desde la existencia del ciberespacio conlleva a que el delito deje de ser territorial y que las fronteras se tornen irrelevantes para el que lo comete, lo cual favorece a los criminales y perjudica a las agencias encargadas del cumplimiento de la ley. El proceso de investigación y obtención de evidencia se ve drásticamente modificado, y obliga a recurrir a herramientas tecnológicas para llevar a cabo tareas con procedimientos ya establecidos. En tal contexto, se advierten complejidades en la persecución de los delitos, que se ve obstaculizada por factores tales como las dificultades en la procuración gubernamental de herramientas tecnológicas, el uso limitado de las TICs por parte de las AOP y ciertos prejuicios en la cultura de las AOP en torno a las necesidades y habilidades requeridas para el uso de nuevas tecnologías[28].

A fin de sostener la eficacia de las investigaciones patrimoniales en el ámbito virtual, con todos los desafíos que ello entraña, es preciso que las autoridades nacionales a cargo de la investigación, identificación, incautación y decomiso de AV adapten su enfoque a la nueva realidad tecnológica en la que debe desarrollarse su actividad. Esta adaptación demanda la adopción de nuevas estrategias de investigación que se adecuen al escenario creado por la evolución tecnológica de las últimas dos décadas, con un enfoque multidisciplinario y utilizando nuevas herramientas de investigación vinculadas a la informática, en línea con lo establecido en las Recomendaciones 30 y 31 del GAFI.

En este escenario, el propósito de esta *guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de AV* es ofrecer ideas, conceptos y buenas prácticas que resulten útiles para que todos los operadores de los países miembros del GAFILAT

[27] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 7, § 1.
[28] Ver: MCQUADE, Samuel: "Cybercrime", en TONRY, Samuel, *The Oxford handbook of crime and public policy*, Oxford University Press, 2011.

puedan procurar una mayor eficacia en las investigaciones vinculadas a maniobras delictivas con AV, su incautación y decomiso. En atención a las diferencias entre las distintas jurisdicciones nacionales en las que pueden llegar a aplicarse, las referidas ideas, conceptos y buenas prácticas se vuelcan con criterio general, quedando librado al criterio de las autoridades de cada país definir el modo en que corresponde adaptarlas a la realidad normativa, regulatoria, política, económica y social de su territorio.

RESUMEN EJECUTIVO

La presente "Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales" es el primer documento de buenas prácticas elaborado por el GAFILAT sobre la materia, con el objeto de fomentar el desarrollo y fortalecimiento de las habilidades para la identificación y localización de esa clase de activos por parte de los puntos de contactos de Red de Recuperación de Activos del GAFILAT (RRAG) y, por su intermedio, de las unidades especializadas del Ministerio Público Fiscal, las fuerzas de seguridad y otras agencias de investigación dedicadas a la identificación, incautación y decomiso de activos vinculados al LA/FT en América Latina. En esa dirección, el propósito de la guía es ofrecer ideas, conceptos y buenas prácticas que resulten útiles para que todos los operadores de los países miembros del GAFILAT puedan procurar una mayor eficacia en las investigaciones vinculadas a maniobras delictivas con AV, su incautación y decomiso. En especial, se propone contribuir para que puedan conciliarse las estructuras normativas, herramientas y estrategias actualmente en uso en orden a la investigación patrimonial y la recuperación de activos -concebidas para ser utilizadas respecto de operatorias de LA/FT desarrolladas en el mundo "físico" o "real"-, con el nuevo escenario que representa el surgimiento de los AV, cuyo ámbito específico es el ciberespacio.

Durante la última década, los AV, y en especial las criptomonedas, han pasado a ocupar un lugar central como moneda de cambio en las transacciones ilícitas realizadas, sobre todo, en los mercados ilegales que operan en Internet. El GAFI se ha referido a ellos en distintos documentos publicados a partir del año 2014, en los que identificó como principales rasgos que incrementan el riesgo de LA/FT al anonimato asociado al diseño de los AV, la posibilidad de que una misma persona controle múltiples "monederos virtuales", el carácter descentralizado de la mayoría de las criptomonedas y el alcance global de muchas de ellas, entre otros. La evolución de este fenómeno derivó en que el organismo actualizara la Recomendación 15 y desarrollara su Nota Interpretativa, referidas a las obligaciones fundamentales de los países miembros con respecto al EBR en orden a las nuevas tecnologías para clarificar su aplicación a los AV, las actividades relacionadas con los mismos, y a los PSAV.

Con relación a ello, la guía contiene un detallado análisis de la problemática inherente a la investigación, incautación y decomiso de AV de origen ilícito o utilizados para el LA/FT, reseñando tanto las tipologías asociadas a esa clase de activos, el contexto tecnológico en el que

se desarrollan, las herramientas con que cuentan los criminales para obstaculizar la acción de las autoridades y las consecuencias que se derivan de su uso; como los aspectos del nuevo ecosistema tecnológico que favorecen la actuación de las AOP, las nuevas estrategias y técnicas de investigación que pueden adoptarse y las herramientas tecnológicas disponibles a tal efecto.

Tomando como punto de partida el escenario descripto precedentemente, se enumeran en la guía una serie de recomendaciones vinculadas a la efectiva regulación de los operadores del ecosistema de AV (con especial énfasis en los que sirven de nexo entre la moneda fiduciaria y la virtual); las fuentes de información con que cuentan las AOP para alimentar las investigaciones patrimoniales sobre conductas de LA/FT involucrando AV; la identificación de "señales de alerta" sobre la posible configuración de esa clase de conductas; los elementos de la arquitectura tecnológica que sustenta el uso de AV que pueden explotarse para una mayor efectividad en las investigaciones; su combinación con las medidas de investigación tradicionales y las que han ido surgiendo a partir de la evolución de las tecnologías de la información y la comunicación (TICs) en las últimas décadas (en especial, las herramientas de vigilancia automatizada o electrónica, el agente encubierto informático y el uso de programas espías); y todo lo concerniente a la planificación y ejecución de la incautación o decomiso de AV, incluyendo el tratamiento de los mismos una vez que se encuentran en poder de las autoridades. También se incorporan recomendaciones referidas a la capacitación del personal y la cooperación internacional en orden a la investigación, incautación o decomiso de AV, incluyendo una nómina de las agencias u organismos internacionales a los que puede recurrirse a estos efectos.

Como complemento, la guía incluye un anexo con una síntesis de todas las recomendaciones contenidas en el documento principal, a los efectos de facilitar su análisis por parte de las AOP y/o unidades especializadas del MP, así como de los puntos de contacto de la RRAG, a quienes se dirige el presente documento. Asimismo, cuenta con un segundo anexo con legislación comparada en materia de regulación del uso de herramientas informáticas avanzadas de investigación o vigilancia, que puede ser de utilidad ya sea como referencia para su eventual incorporación en la normativa procesal de los países de la región o para su aplicación analógica, allí donde sea posible conforme los principios legales vigentes.

II. METODOLOGÍA

A. Punto de partida

1. En el marco de las conclusiones, recomendaciones y prioridades trazadas en la XVII Reunión General de los Puntos de Contacto de la Red de Recuperación de Activos del GAFILAT (RRAG), que tuvo lugar en el mes de noviembre de 2020, se planteó la posibilidad de desarrollar documentos de buenas prácticas o técnicos sobre temas de interés para los puntos de contacto y sus instituciones, incluyendo la investigación, identificación, incautación y decomiso de AV y la implementación de técnicas especiales de investigación.

2. En especial, se destacó que el desarrollo y fortalecimiento de las habilidades para la identificación y localización de AV constituye un desafío ineludible para los puntos de contacto de la RRAG. En esa dirección, los propios integrantes de la Red identificaron dicha problemática como un aspecto central para el desarrollo de sus tareas, y la señalaron como una prioridad.

3. Producto de ese reconocimiento es la presente "Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales", dirigida a los puntos de contacto de la RRAG y, por su intermedio, a las unidades especializadas del Ministerio Público Fiscal, las fuerzas de seguridad y otras agencias de investigación dedicadas a la identificación, incautación y decomiso de activos vinculados al LA/FT en América Latina.

4. El objetivo de esta guía es contribuir para que puedan conciliarse las estructuras normativas, herramientas y estrategias actualmente en uso en ora en a la investigación patrimonial y la recuperación de activos -concebidas para ser utilizadas respecto de operatorias de LA/FT desarrolladas en el mundo "físico" o "real"-, con el nuevo escenario que representa el surgimiento de los AV, cuyo ámbito específico es el mundo "virtual" o ciberespacio.

B. Alcance

5. En atención a los objetivos planteados para la guía, su alcance esta acotado al análisis de cuestiones que tienen incidencia práctica en la investigación de conductas de LA/FT con AV. Por consiguiente, queda excluido el estudio general del fenómeno conocido como "Fintech" (entendido como la confluencia entre la tecnología y la provisión de productos y servicios financieros), dentro del cual el surgimiento de los AV (y sobre todo las criptomonedas) representa tan sólo una de las múltiples variantes dentro de un universo mucho más vasto, que comprende un amplio rango de actividades que incluye a la provisión de servicios bancarios a través de vías digitales no asociadas a instituciones bancarias, la evaluación de crédito con base en datos alternativos, los préstamos

"par a par" ("peer-to-peer" o P2P) a personas no bancarizadas, el uso de tecnología de Blockchain para "contratos inteligentes" ("Smart contracts"), las monedas digitales emitidas por bancos centrales, las ofertas iniciales de monedas virtuales, y las estrategias de inversión mediante algoritmos, entre otras.

6. El foco del análisis se centra en la problemática vinculada a los AV centralizados y descentralizados, con especial énfasis en el uso de criptomonedas para fines de LA/FT. Esto incluye también a las "así llamadas monedas estables" ("so called stable-coins"). Ello, toda vez que esa clase de activos presenta muchos de los mismos riesgos de LA/FT que se encuentran en otros AV, derivados de su potencial para el anonimato, el alcance global y su posible uso para la estratificación de fondos de origen ilícito. Estas vulnerabilidades se incrementan en caso de que estas monedas sean adoptadas masivamente, lo cual, si bien todavía no ha ocurrido, puede darse en un futuro cercano ante el lanzamiento de "monedas estables" auspiciadas por grandes compañías financieras, de tecnología o telecomunicaciones[29].

7. Asimismo, en lo que refiere a las criptomonedas, es importante tener presente que, aunque Bitcoin, Ethereum y Ripple son las más conocidas, en la práctica todas ellas son, en mayor o menor medida, susceptibles de ser explotadas para el LA/FT. Sin embargo, dada la inabarcable cantidad de AV de esta clase en circulación (al mes de marzo de 2020, existían 5.183 criptomonedas conocidas[30]) se hace foco sobre todo en el Bitcoin, que es la que ostenta un lugar preponderante en el mercado, como así también en Altcoins de uso generalizado, y en las denominadas "monedas privadas", como Monero y ZCash.

8. La presente guía ha sido concebida para ser aplicada en los 17 países que integran el GAFILAT, que representan una variedad geográfica, política y social, de lo que se deriva a su vez en una gran diversidad en punto a la realidad normativa imperante en cada jurisdicción, así como a la integración y funcionamiento de los organismos encargados de la investigación, incautación y decomiso de activos vinculados al LA/FT. Por consiguiente, tanto el análisis como las recomendaciones se efectúan con criterio general, a fin de que sean los propios destinatarios de la misma los que adapten sus postulados al contexto específico de cada país en que vayan a ser aplicados.

C. Metodología

9. El análisis efectuado a los efectos de la elaboración de esta guía comprendió las siguientes cuestiones: a) el funcionamiento de los AV, los riesgos de LA/FT asociados a los mismos y la consecuente necesidad de una regulación eficaz, a nivel internacional, dirigida a mitigarlos; b) las

[29] Ver GAFI: "Report to the G20 finance ministers and central bank governors on so-called Stablecoins", junio 2020, apartados §§ 1 y 4.
[30] Ver: ALLEN, Franklin / GU, Xian / JAGTIANI, Julapa: "A survey of Fintech research and policy discussion", Federal Reserve Bank of Philadelphia Research Department, Worgking Papers 20-21, junio 2020, pág. 18.

especiales características que presenta la investigación de delitos cometidos en el ámbito virtual (incluyendo a las conductas de LA/FT con AV), los inconvenientes que de ellas se derivan a los efectos de la identificación de los/las responsables, la reconstrucción de las transacciones y el decomiso o incautación de los fondos involucrados; y c) las nuevas herramientas tecnológicas con las que cuentan las AOP para lograr una mayor eficacia en las investigaciones patrimoniales referidas a la materia.

10. En tal contexto, se elaboró un diagnóstico sobre la situación de América Latina en relación con el tratamiento de los AV, la supervisión de las personas o entidades que prestan servicios referidos a los mismos (los PSAV), y la posible implementación de nuevas estrategias y herramientas tecnológicas en procura de una mayor efectividad en las investigaciones patrimoniales referidas a conductas de LA/FT con AV.

11. A tal efecto, se llevó a cabo un relevamiento de la realidad normativa y regulatoria de la región por medio de un cuestionario dirigido a los países del GAFILAT, además de a los puntos de contacto de la RRAG. Este relevamiento puso el énfasis en dos cuestiones centrales:

a) En primer lugar, la situación en orden al cumplimiento de los estándares establecidos en la Recomendación 15 del GAFI y su nota interpretativa (así como de las guías y reportes del organismo con relación a la materia) en orden a la regulación de los deberes de ALA/CFT en materia de AV y PSAV. Ello, toda vez que el grado de adecuación que presentan no sólo repercute en la eventual generación de alertas sobre operaciones sospechosas de LA/FT involucrando esa clase de activos, sino también en la posibilidad de que las agencias encargadas en la investigación, identificación, incautación y decomiso de AV cuenten con una fuente de información precisa y detallada acerca de las personas físicas o jurídicas que operan con esa clase de activos, que puede resultar de capital importancia para el éxito de las investigaciones patrimoniales que los tengan por objeto.

b) En segundo, la identificación de los recursos con que cuentan las AOP o unidades especializadas de los Ministerios Públicos en América Latina para investigar, identificar, incautar y decomisar AV. En tal contexto, se procuró determinar cómo es la situación normativa en la región en términos de la posible adopción de las técnicas y herramientas tecnológicas de investigación reseñadas precedentemente, que resulta imprescindible para una detección y persecución eficaz de maniobras de LA/FT vinculadas a criptomonedas.

12. El resultado de este relevamiento constituyó el insumo fundamental para la elaboración de un diagnóstico sobre la situación de la región frente al nuevo escenario que supone la creciente adopción del uso de AV y su potencial de explotación para el LA/FT. No obstante ello, también se analizó, a tal efecto, la información obtenida por el GAFILAT en el marco de la 4ª Ronda de

Evaluaciones Mutuas sobre cumplimiento con los estándares del GAFI, particularmente a la Recomendación 4 y 38, al igual que la recolectada por el Grupo de Expertos para el Control del Lavado de Activos de la OEA como resultado de un estudio sobre criptomonedas acordado en la reunión de dicho grupo en el año 2016, en cuyo marco se hizo circular un cuestionario entre los años 2017 y 2018.

13. Por añadidura, se tomaron en consideración otros insumos tales como:

- Entrevistas con funcionarios de la Organización de Estados Americanos (OEA), CARIN, Banco Mundial e ICAR.

- Documentos publicados por distintos organismos internacionales, comenzando por los reportes y guías del GAFI y siguiendo por documentos de Interpol, Europol, Instituto de Basilea sobre Gobernanza, el Comité sobre Supervisión Bancaria de Basilea, el Instituto para la Estabilidad Financiera (FSI), CARIN, la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS), el Banco Central Europeo (ECB), la Autoridad Bancaria Europea (EBA), el Parlamento de Europa y el FBI, entre otros (así como en numerosas publicaciones académicas sobre la materia) en los que se reflejan los riesgos de LA/FT asociados a los AV y la consecuente necesidad de una regulación eficaz, a nivel internacional, dirigida a mitigarlos.

- Documentos de organismos internacionales y material académico referido al funcionamiento de los AV en general y las criptomonedas en particular, reflejando tanto los obstáculos que ello supone para una investigación patrimonial, como a las posibilidades que dicho funcionamiento ofrece para la obtención de evidencia y/o información relevante para la identificación y persecución de conductas de LA/FT con AV. Como así también en lo referido a la incautación y/o decomiso de esa clase de valores. Se destacan, en tal sentido, las guías publicadas sobre la materia por el GAFI, UNODC, el Consejo de Europa y el Centro de Información Regional sobre Criminalidad Organizada (ROCIC, por sus siglas en inglés).

- Documentos de organismos internacionales y material académico sobre el impacto de los avances tecnológicos en la investigación de ciberdelitos, y la necesidad de adoptar nuevas estrategias e implementar el uso de nuevas herramientas para poder combatir eficazmente esa clase de criminalidad. Por ejemplo, los documentos publicados por el Grupo de Trabajo en Delito Cibernético de la OEA, el Instituto de Gobierno de Basilea, el Parlamento Europeo, Interpol, Europol, la Asociación Internacional de Jefes de Policía (IACP, por sus siglas en inglés) y el Foro Ejecutivo Policial de Investigación (PERF, por sus siglas en inglés).

- Los instrumentos internacionales referidos a la implementación de herramientas novedosas de investigación de ciberdelitos, entre los que cabe enumerar al Convenio del Consejo de Europa sobre Cibercriminalidad (Convención de Budapest); los Textos Legislativos Modelo de la Comunidad del Caribe (ITU/CARICOM/CTU Model Legislative Texts), el Proyecto de Convención de la Unión Africana (Draft African Union Convention), la Ley Modelo del Commonwealth (Commonwealth Model Law), el Proyecto de Directiva de la Comunidad Económica de los Países de África Occidental (ECOWAS Draft Directive) y la Convención de la Liga de Estados Árabes (League of Arab States Convention). También ejemplos de regulación específica del uso de nuevas técnicas de vigilancia o investigación tecnológica en España, Francia, Inglaterra, Países Bajos y Polonia.

D. Proceso de elaboración

14. El proceso de elaboración de la guía se dividió en cuatro fases o etapas, a saber: 1. Etapa preparatoria; 2. Etapa de estudio; 3. Etapa de diagnóstico e informe preliminar; y 4. Etapa final.

15. La etapa preparatoria comprendió la compilación y análisis de reportes de organismos especializados y material académico sobre las cuestiones comprendidas en la temática de la guía, así como la elaboración, en coordinación con la Secretaría Ejecutiva del GAFILAT y la Cooperación alemana para el desarrollo implementada por GIZ, del proyecto de cuestionario dirigido a los países del GAFILAT y a los puntos de contacto de la RRAG a fin de obtener información sobre: a) regulación local sobre criptomonedas; b) regulación local de ALA/CFT en relación con los PSAV; c) normativa local sobre incautación y decomiso; y d) normativa procesal local sobre técnicas de investigación tecnológica y/o informática.

16. Durante la etapa de estudio se desarrolló el Plan de Trabajo junto con la SE del GAFILAT, que coordinó la distribución de los cuestionarios. Luego, se recopilaron y sistematizaron las respuestas recibidas, y finalmente se sostuvieron entrevistas con representantes de la OEA, CARIN, el Banco Mundial e ICAR.

17. En la etapa de diagnóstico se llevó a cabo, con base en la información recopilada durante las fases previas, una evaluación sobre la situación regional en relación con la regulación, investigación, incautación y decomiso de AV, identificando las fuentes de información y las herramientas legales previstas en la normativa, así como el margen de acción para la implementación de nuevas medidas de investigación tecnológica.

18. En la etapa final, y tomando como punto de partida dicho diagnóstico, se elaboró un informe preliminar centrado en la identificación de estrategias para el aprovechamiento eficaz de los puntos de contacto entre el universo “virtual” y el “físico” en las investigaciones patrimoniales,

como así también de métodos y herramientas investigativas adecuadas a la realidad del ciberespacio y al contexto tecnológico actual.

19. El último paso consistió en la redacción del documento final y su aprobación por parte de la Secretaría Ejecutiva del GAFILAT.

E. Estructura

20. La presente guía está estructurada de la siguiente manera: a continuación de la introducción (Sección I) y de esta reseña sobre la metodología empleada (Sección II), se encuentran las definiciones sobre los términos técnicos empleados en la guía (Sección III); el análisis de la información obtenida en orden a la problemática de la investigación patrimonial, incautación y decomiso de AV, con especial referencia al contexto regional (Sección IV); y, por último, las recomendaciones y pasos apropiados para la investigación, identificación, incautación y decomiso de AV (Sección V).

21. Como **Anexo I** se incluye una reseña de buenas prácticas para la investigación, identificación, incautación y decomiso de AV vinculados a fondos de origen ilícito y, como **Anexo II**, un análisis de la legislación comparada en materia de implementación de herramientas tecnológicas de investigación.

III. DEFINICIONES

Referidas a los activos virtuales

22. **Activo virtual (AV):** conforme la definición del GAFI, es una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar para pagos o inversiones. Los AV no incluyen a las representaciones digitales de moneda *fiat*, valores y otros activos financieros que ya están cubiertos en otras partes de las Recomendaciones del GAFI.

23. **Dinero fiduciario:** alude a la moneda o dinero real (no virtual), o moneda nacional. Se diferencia de la moneda virtual porque éste funciona como la moneda y el papel moneda de un país, designado como dinero de curso legal; que circula, se utiliza y acepta como medio de intercambio en el país emisor.

24. **Activo virtual convertible (o abierto)**: es el que tiene un valor equivalente en moneda fiduciaria y puede ser convertido desde o hacia esa clase de moneda. Ejemplos: Second Life Linden Dollars o WebMoney.

25. **Activo virtual no convertible (o cerrado):** es el que pretende ser específico para un dominio o mundo virtual en particular, como los creados en el seno de los "Juegos de rol multi-jugador masivos en línea" (MMORPG, por sus siglas en inglés) o en Amazon.com; motivo por el cual las reglas que regulan su uso prohíben intercambiarlos por moneda fiduciaria. Ejemplos: Project Entropia Dollars, Q Coins y World of Warcraft Gold. Esto no implica que los AV no convertibles puedan ser negociados por moneda fiduciaria (o por criptomonedas) en un mercado secundario, conducta que puede estar sujeta a sanciones por parte del administrador. Todos los activos virtuales no convertibles son centralizados.

26. **Activos virtuales centralizados**: son los que responden a una única autoridad central (administrador), que es una tercera parte que controla el sistema. El/la administrador/a emite el AV, fija las normas para su utilización, mantiene un libro de contabilidad central de pagos, y tiene autoridad para canjear la moneda (retirarla de la circulación). Ejemplos: Second Life "Linden dollars", PerfectMoney, WebMoney "WM units", y World of Warcraft gold.

27. **Activos virtuales descentralizados**: son activos virtuales distribuidos, de fuente abierta y "par-a-par" sin una autoridad central de administración, monitoreo y supervisión. Los principales exponentes de los AV descentralizados son las criptomonedas.

28. **Criptomonedas:** son AV de código abierto, convertibles y descentralizados, que funcionan en una red de pares distribuida que aplica principios matemáticos y criptográficos para dotar de seguridad al sistema. Las transferencias entre los/las usuarios/as se llevan a cabo "par a par", sin intermediarios, a partir del juego de claves criptográficas públicas y privadas, y requieren de ser firmadas criptográficamente para concretarse. La transparencia del sistema se garantiza mediante el registro de las transacciones en una suerte de "libro mayor" distribuido (denominado Blockchain en la mayoría de las criptomonedas), llevado por una red de partes mutuamente "desconfiadas" (llamadas "mineros" en el ecosistema del Bitcoin y otras criptomonedas) que elaboran los bloques criptográficos de la cadena y son recompensados por ello con tarifas pagadas por los/las usuarios/as.

29. **Bitcoin**: lanzado en 2009, fue el primer AV convertible descentralizado, y la primera criptomoneda. Los bitcoins son unidades de cuenta compuestos de secuencias alfanuméricas únicas que constituyen unidades de moneda (divisibles, a su vez, en unidades más pequeñas, llamadas Satoshis) y que tienen valor sólo porque usuarios individuales están dispuestos a pagar por ellos. Los bitcoins se comercian digitalmente entre los usuarios en forma parcialmente anónima (las personas o entidades que intervienen en cada transacción se identifican solo con pseudónimos alfanuméricos llamados "Direcciones Bitcoin" -Bitcoin adresses-) y pueden ser intercambiados por moneda fiduciaria o por otras criptomonedas. El software requerido para enviar, recibir y almacenar bitcoins o para monitorear las transacciones puede ser descargado gratuitamente. Los/las usuarios/as también pueden obtener sus direcciones Bitcoin (que funcionan como cuentas) en plataformas de intercambio de Bitcoin o en servicios de monederos online. Las

transacciones (flujos de fondos) se consignan en un registro público compartido (la cadena de bloques o "Blockchain"), en el que se las identifica por medio de las direcciones Bitcoin.

30. **Altcoin:** el término refiere a cualquier moneda virtual convertible descentralizada fundamentada matemáticamente distinta al Bitcoin—la original. Actualmente, existen miles de Altcoins. Entre las principales, cabe mencionar a las siguientes:

a) **Litecoin (LTC)** fue lanzada en 2011. Fue una de las primeras Altcoins posteriores al Bitcoin. Si bien se asemeja a esta última en muchos aspectos, la generación de bloques es más veloz, lo que aumenta la rapidez en la confirmación de las transacciones.
b) **Ethereum (ETH)**: Es una plataforma de software descentralizada que permite la ejecución y desarrollo de "Contratos inteligentes" ("Smart contracts") y aplicaciones distribuidas (DApps) sin interferencias de terceros. Ether es el token criptográfico con el que corren las aplicaciones basadas en Ethereum.
c) **Dash (DASH)**: Conocida originalmente como Darkcoin, es una versión más privada de Bitcoin. Ofrece un nivel mayor de anonimato, ya que funciona en una red descentralizada que dificulta la trazabilidad de las transacciones.

31. **Ripple (XRP)**: Es una red global de compensación de pagos que ofrece la posibilidad de transferencias instantáneas, ciertas y de bajo costo. Su registro no requiere minado (lo que lo distingue de la mayoría de las criptomonedas), lo que reduce el uso de capacidad computacional y la latencia (demora) en la red.

32. **Bitcoin Cash (BCH)**: Es una derivación de Bitcoin, cuya principal diferencia reside en que permite un flujo mayor de transacciones por segundo, lo que a su vez deriva en tasas más bajas.

33. **"Así llamadas monedas estables" ("So-called stablecoins")** son AV que indican mantener un valor estable en relación con uno o más activos de referencia (que pueden ser monedas fiduciarias, otros activos virtuales, securities, commodities o activos inmobiliarios). El término no responde a una clasificación legal o regulatoria, sino que es utilizado en general como un término publicitario. Dependiendo del diseño del AV de que se trate, puede ser clasificado como una moneda o como un "activo financiero" (como las securities) conforme los estándares fijados por el GAFI.

Referidas a las tecnologías asociadas a los activos virtuales

34. **Dirección de AV o de criptomonedas (Ej.: dirección Bitcoin):** es un código alfanumérico que identifica el lugar virtual asociado a una determinada cantidad de AV, necesaria para poder enviar o recibir criptomonedas. Funciona como una cuenta bancaria en el sistema financiero tradicional para recibir o enviar transferencias. Por ejemplo, las direcciones Bitcoin tienen una longitud de entre 26 y 32 caracteres. Empiezan por el número 1 para direcciones estándar y por el

número 3 para las direcciones de multi firmas. Otras criptomonedas tienen sus propios sistemas para representar sus direcciones. Las direcciones de AV también pueden representarse por medio de códigos QR.

35. **Códigos QR:** son una representación gráfica creada por un algoritmo hash gráfico, lo que significa que siempre proporciona el mismo gráfico si se introduce la misma información. Cuando se lo utiliza en relación con las criptomonedas, permite compartir la dirección Bitcoin más fácilmente, puesto que el código puede ser escaneado usando la cámara de un smartphone.

36. **Blockchain:** es una forma de registro o "libro mayor" utilizada por Bitcoin y la mayoría de las criptomonedas, y funciona encadenando bloques de datos. Cada uno de estos bloques contiene información acerca de la operación que se están realizando. Los elementos iniciales y finales del bloque se relacionan, respectivamente, con el bloque anterior y posterior. De este modo, la modificación del bloque corrompería la cadena al completo, aunque es prácticamente imposible su alteración. Además, la tecnología basada en cadenas de bloques funciona de modo distribuido, con múltiples computadoras que operan simultáneamente con la cadena, lo cual hace extremadamente difícil comprometerla mediante un ataque informático. Cada criptomoneda tiene su propia Blockchain.

37. **Tecnología de registro distribuido (Distributed ledger technology o DLT):** es una estructura de datos que se distribuye geográficamente, de modo tal que la información de la base es procesada en simultáneo por múltiples servidores, sin que exista un/a administrador/a principal. Se trata, en esencia, de una base de datos gestionada por un colectivo de participantes, cada uno de los cuáles dispone de una copia del registro, de modo que las eventuales variaciones son fáciles de detectar, toda vez que las actualizaciones de la base solo pueden concretarse mediante consenso de todos los partícipes.

38. **Juego de claves pública/privada:** las principales criptomonedas, como Bitcoin, están construidas a partir de la tecnología de criptografía asimétrica, que recurre al juego de claves pública y privada. La primera puede ser conocida por cualquiera, la segunda es confidencial. En el ecosistema Bitcoin, la clave pública deriva de la privada a través de una función criptográfica de única vía conocida como "Multiplicación de curva elíptica" ("Elliptic curve multiplication").

39. **Clave privada ("private key")**: es un número aleatorio que funciona como clave secreta, generado a través de un proceso de criptografía asimétrica, y se utiliza para resguardar la propiedad y el manejo de las criptomonedas. Durante el proceso de creación de un monedero de AV, la clave privada se genera en primer término y luego, a partir de ella, la clave pública, que está relacionada matemáticamente con la anterior. El proceso, sin embargo, es imposible de concretar en sentido inverso (deduciendo la clave privada a partir de la pública), lo cual brinda un alto nivel de seguridad. La clave privada es la que asigna al/la titular el control de los fondos asociados a una determinada dirección de AV.

40. **Clave pública ("public key")**: es un identificador que se puede compartir para permitir la transferencia de AV a terceros. Es una de las dos partes que forman el conjunto de claves creadas por la criptografía asimétrica para compartir secretos de forma segura.

41. **Monederos (Wallets) de criptomonedas:** son aplicaciones de software que permiten interactuar con la Blockchain de las AV a fin de generar y/o almacenar las direcciones de criptomonedas y sus correspondientes juegos de claves público/privada. Es una interfaz que permite a los/las usuarios/as administrar, transferir o recibir AV. Existen varias clases de monederos de AV.

42. **Monederos alojados o en custodia (Hosted / Custodial wallets):** son monederos virtuales que están alojados en un servidor externo (es decir, en "la nube"), y se ofrecen a través de proveedores de servicios de monedero de AV Su denominación refiere a que las claves privadas no están en poder del/la titular de las AV, sino "en custodia" del prestador del servicio.

43. **Monederos híbridos (hybrid wallets)**: son monederos alojados, pero no "en custodia", toda vez que, aunque están alojados en los servidores de un proveedor de servicios, el/la usuario/a mantiene el control sobre la/las clave/s privada/s.

44. **Monederos sin custodia o auto alojados (Self-custody/ Self Hosted)**: son los monederos que los/las propios usuarios/as de criptomonedas mantienen en su poder, para uso propio de los AV asociados a las direcciones almacenadas en los mismos. Estos monederos pueden ser virtuales o físicos.

45. **Monederos virtuales (Software wallets)**: son aplicaciones descargables, de escritorio o móviles, que pueden mantenerse en una computadora de escritorio o en un dispositivo móvil (un teléfono inteligente o smartphone) para permitir el almacenamiento seguro de las claves en el dispositivo.

46. **Monederos físicos (Hardware wallets)**: son aplicaciones de monedero alojadas en dispositivos físicos como pendrives o USB, que le permiten al/la usuario/a almacenar sus claves offline, en dispositivos físicos portátiles como pendrives.

47. **Monederos de papel (paper wallets)**: se trata de planchas de papel o de otro material en el que se imprimen, mediante un programa de monedero de AV, las direcciones de criptomonedas y el juego de claves pública/privada con las que se gestiona el intercambio de criptomonedas, ya sea en formato plaintext o en forma de código QR. Se recurre a las mismas para el almacenamiento y resguardo de fondos que no van a ser utilizados o movidos en mucho tiempo, ya que ofrecen un nivel mayor de seguridad, al no ser susceptibles al robo cibernético.

48. **Almacenamiento en frío (Cold storage)**: alude a los monederos que no están conectados a Internet, como los monederos físicos o de papel. La finalidad de las variantes de "almacenamiento en frio" es ofrecer protección contra el hackeo o robo de las criptomonedas.

49. **Almacenamiento en caliente**: en contraposición con el anterior, se refiere a los monederos de AV que funcionan online, es decir, con conexión a Internet. Debido a ello, esta forma de almacenamiento es más vulnerable a la piratería/robo que el almacenamiento en frío.

50. **Monederos de firma multiple (multi-signature wallets):** son aplicaciones que brindan un nivel de seguridad adicional al requerir el uso de múltiples claves privadas para autorizar una transacción, reduciendo de ese modo el riesgo de robo de criptomonedas si se compromete una única clave privada.

51. **Monederas controladas por el Estado**: se trata de un monedero (de cualquier clase) que está bajo control de una autoridad gubernamental (puede ser una agencia estatal especializada en el manejo de activos incautados, una agencia de cumplimiento de la ley, una fiscalía, un órgano jurisdiccional o incluso una compañía privada colaborando con el Estado), a la cual se transfieren los AV que se incautan o decomisan.

52. **Las "palabras semilla" o "frase semilla" ("Seed words" o "Seed phrase")**: son utilizadas por muchas aplicaciones de monedero de AV para generar claves privadas a partir de una única "semilla", que toma la forma de un mnemónico conformado por una secuencia de entre 12 y 24 palabras en distintos idiomas (inglés, japonés, coreano, español, chino, francés e italiano), que funcionan como un respaldo (back up) para el monedero, permitiendo que en caso de pérdida de control sobre el mismo (por ejemplo, debido al robo, pérdida o desperfecto técnico del dispositivo en el que se encuentra almacenada), sea posible recrearlo introduciendo en la aplicación correspondiente las palabras en el orden provisto originalmente.

53. Un **Mnemónico o nemónico** es, en informática, una palabra o frase que sustituye a un código de operación (lenguaje de máquina), con lo cual resulta más fácil la programación.

54. **Videojuegos de rol multijugador masivos en línea (Massively multiplayer online role-playing games o MMORPGs)**: son videojuegos que permiten a miles de jugadores introducirse simultáneamente en un mundo virtual a través de Internet e interactuar entre ellos.

Referidas a los actores del ecosistema de activos virtuales

55. **Usuario/a:** es la persona o entidad que obtiene un AV y lo utiliza para adquirir bienes o servicios físicos o virtuales, o para transferirlos a otra persona, o para mantenerlo en su poder como inversión. Los AV pueden obtenerse de diversas maneras. A saber: (1) adquiriéndolos a cambio de moneda fiduciaria (ya sea en una plataforma de intercambio de AV o, si se trata de

activos centralizados, directamente del administrador o emisor); (2) llevando a cabo tareas que se recompensan mediante pagos en AV; y/o (3) en el caso de los AV descentralizados -como el Bitcoin-, autogenerando unidades de la criptomoneda a través de la participación en el proceso de "minado".

56. **Minero/a:** es una persona o entidad que interviene en la red descentralizada de una criptomoneda utilizando un software especial para resolver algoritmos complejos dentro del sistema de "prueba de trabajo" empleado por el sistema para validar las transacciones.

57. **Administrador/a:** es la persona o entidad dedicada comercialmente a la emisión (puesta en circulación) de AV centralizados, que también se encarga de fijar las reglas de uso y mantener el registro central de pagos, además de ostentar la autoridad para retirar de circulación los activos en cuestión.

58. **Proveedores/as de servicios de activos virtuales (PSAV)**: conforme la definición del GAFI, comprende a cualquier persona física o jurídica que no esté cubierta en ningún otro lugar en virtud de las Recomendaciones y que, como negocio, realiza una o más de las siguientes actividades u operaciones para/en nombre de otra persona física o jurídica:

i. intercambio entre activos virtuales y monedas *fiat*;
ii. intercambio entre una o más formas de AV;
iii. transferencia de AV;
iv. custodia y/o administración de AV o instrumentos que permitan el control sobre AV; y
v. participación y provisión de servicios financieros relacionados con la oferta de un emisor y/o venta de un AV.

59. **Plataformas de intercambio de AV/criptomonedas (cryptocurrency exchanges)**: son las operadas por personas o entidades que se dedican comercialmente al intercambio de criptomonedas por moneda fiduciaria, fondos, metales preciosos u otras criptomonedas (o viceversa), a cambio de una tarifa (comisión). Por lo general aceptan una amplia variedad de métodos de pago (efectivo, transferencias, tarjetas de crédito u otras criptomonedas) y son utilizados para depositar o extraer fondos de cuentas de AV.

60. **Proveedores de servicios de monedero de criptomonedas:** también comprendidos en la definición de PSAV del GAFI, son personas o entidades que ofrecen como servicio la provisión de monederos (ya sea alojados "en custodia" o híbridos). Cuando lo que se ofrece son monederos "en custodia", esta clase de proveedores facilita la participación en el ecosistema de AV al simplificar la realización de transacciones para los/las usuarios/as. Se encargan de mantener el balance de los clientes y por lo general ofrecen también seguridad respecto del almacenamiento y las transacciones con criptomonedas. En esa dirección, pueden proveer servicios tales como

encriptación, back up o "almacenamiento en frío" de los monederos, protección mediante firmas múltiples o mezcladores.

61. **Mezcladores (Mixers)**: Son plataformas que ofrecen a los/las usuarios/as de criptomonedas la posibilidad de oscurecer la cadena de transacciones en la Blockchain mediante el recurso a herramientas informáticas de anonimato que vinculan múltiples transacciones a una única dirección de AV y las envían en conjunto de un modo que hace aparecer como que provienen de una dirección diferente. El mezclador o conmutador (Tumbler) interviene cuando recibe la instrucción del/la cliente de enviar fondos a una determinada dirección. A fin de ocultar el origen y destino de dicha transacción, el mezclador la combina con una serie compleja y semialeatoria de transacciones ficticias, de modo tal de impedir que la transferencia al destino final pueda ser asociada con la dirección de origen. Ejemplos de mezcladores son Bitmixer.io, SharedCoin, Blockchain.info, Bitcoin Laundry, Bitlaunder, Easycoin.

62. **Plataformas de comercio**: funcionan como mercados, conectando a compradores y vendedores al ofrecerles una plataforma en la que pueden hacer y recibir ofertas por sus criptomonedas. Las operaciones entre los/las usuarios/as de estas plataformas se llevan a cabo en formato "par a par", esto es, sin intermediación de la plataforma. No están incluidas en la definición de PSAV del GAFI.

63. **Sistemas Par-a-par** ("peer-to-peer" o P2P), son los sistemas de comunicación o intercambio de archivos (incluyendo criptomonedas) en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos como intermediarios, sino mediante una serie de nodos que se comportan como iguales ("pares") entre sí.

64. **Sistema de Cambio Local (LETS, por sus siglas en inglés)**: es una organización económica implementada a nivel local que permite a sus miembros intercambiar bienes y servicios con el resto del grupo. Las LETS usan una moneda creada localmente para denominar unidades de valor que pueden ser objeto de comercio o intercambio a cambio de bienes o servicios. Teóricamente, los bitcoins podrían ser adoptados como moneda local utilizada dentro de un LETS. Ejemplos: Ithica Dollars o Mazacoin.

Referidas a herramientas de anonimato o anti forenses

65. **Anonimizadores o programas/herramientas de Anonimato**: son herramientas informáticas y/o servicios, tales como las redes oscuras o los mezcladores, que han sido diseñados para ocultar el origen de una transacción de AV y/o para facilitar el anonimato de los/las usuarios/as de Internet.

66. **Herramientas anti forenses**: son herramientas informáticas que han sido diseñadas o pueden ser explotadas para imposibilitar o entorpecer la ejecución de medidas de investigación por parte de las agencias de orden público o autoridades del Estado.

67. **Monederos oscuros (dark wallets)**: son monederos virtuales que funcionan como extensiones de los navegadores (disponibles en Chrome y potencialmente en Firefox) a efectos de garantizar el anonimato de las transacciones con criptomonedas mediante la incorporación de las siguientes funciones: autoanonimizador (mezclador), comercialización descentralizada, plataformas de micromecenazgo ("Crowdfunding"), plataformas de valores, e información y acceso a mercados online en la "Red oscura" (Dark web).

68. **Salto de cadenas (Chain hopping)**: es un método utilizado para entorpecer la trazabilidad de transacciones con AV, que consiste en "saltar" de una criptomoneda a otra (y, por consiguiente, de una Blockchain a otra) utilizando distintas plataformas de intercambio de AV.

69. **Intercambios atómicos (Atomic swaps):** son una variante del "salto de cadenas" a través de contratos inteligentes digitales, que permiten intercambiar una criptomoneda por otra sin recurrir a intermediarios centralizados, como las plataformas de intercambio de AV. Se llevan a cabo entre monedas que operan con diferentes blockchains, y pueden concretarse "off-chain", esto es: por fuera de la Blockchain de cada criptomoneda. El contrato requiere que ambas partes confirmen la recepción de los fondos dentro de un lapso predeterminado mediante una función hash criptográfica. Si dentro del período establecido una de las partes no confirma la transacción, la misma es anulada y los fondos no son intercambiados.

70. **Combinación o mezcla de monedas (CoinJoin o Coin Mixing)**: es una técnica de anonimización que se concreta mediante un contrato inteligente digital en el que las partes acuerdan comprometer sus AV en una nueva transacción, en la que cada una termina con la misma cantidad de criptomonedas con la que ingresó, pero en la que las direcciones utilizadas se entremezclan para dificultar la trazabilidad.

71. **Firma de círculo (Ring signature):** es un método de anonimización que consiste en el uso de una modalidad de firma digital grupal, conforme la cual cada miembro del grupo cuenta con su propia clave, pero al utilizarla no puede saberse cuál de todas ellas se usó para confirmar una determinada transacción con AV.

72. **TOR (The Onion Router):** es una red distribuida de computadoras en la Internet que se utiliza para ocultar las verdaderas direcciones IP (y, por consiguiente, la verdadera identidad) de los/las usuarios/as, enrutando las comunicaciones a través de múltiples nodos (elegidos aleatoriamente para cada comunicación) en todo el mundo y resguardando los paquetes de datos que indican el origen y destino de la comunicación en varias capas de encriptación.

73. **Dirección IP (Internet Protocol):** es un código único que identifica a una determinada computadora conectada a la Internet ante el resto de los equipos con los que se conecta. Las direcciones IP son asignadas por el proveedor de servicios de Internet (PSI) del/la usuario/a, al cual se le asignan determinados bloques de direcciones correspondientes a la región geográfica en la que se encuentran. No pueden existir en el mismo momento dos equipos informáticos conectados a Internet con la misma dirección IP.

74. **Red oscura (Dark web o Dark net)**: se trata del ámbito de la Internet ocupado por el contenido online al que sólo puede accederse mediante un software de anonimización especializado como el TOR.

75. **Servicios ocultos (Hidden services)**: son páginas web localizadas en la "Red oscura", a las que sólo puede accederse mediante el uso de sistemas de comunicación anónima como TOR. Ello impide que su verdadera ubicación (dirección IP) pueda ser identificada, toda vez que se encuentra enmascarada por el enrutamiento "en capas" provisto por el TOR. La comunicación entre estas páginas y sus usuarios/as tiene lugar a través de un "punto de encuentro" ("rendezvous point") que ofrece una capa adicional de protección frente al análisis de tráfico.

76. **Red privada virtual** ("virtual private network" o VPN) es una tecnología de red de computadoras que permite establecer una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se concreta estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, encriptado de los datos o la combinación de ambos métodos. Al igual que el sistema TOR, los VPN ocultan la verdadera dirección IP de los usuarios, asignándoles direcciones IP al azar para conectarse con sus sitios de destino.

77. **Encriptación:** es un método de cifrado de datos que consiste en codificar los contenidos usando una fórmula o algoritmo matemático que los desordena, de manera tal que si no se cuenta con la correspondiente clave (denominada "llave criptográfica") aquellos lucen como un conjunto de caracteres alfanuméricos sin sentido ni lógica de lectura.

78. **Encriptación "fuerte"** es aquella que utiliza claves criptográficas lo suficientemente complejas como para tornar matemáticamente imposible que sean descifradas mediante un "ataque de "fuerza bruta". Esto se logra, en términos informáticos, añadiendo bits a las claves criptográficas para volverlas más complejas, lo cual aumenta exponencialmente la dificultad para descifrarlas probando cada una de las posibilidades. Así, la adición de un único bit a la llave criptográfica incrementa mínimamente el trabajo requerido para encriptar los datos, pero duplica el esfuerzo computacional necesario para atacar el algoritmo. A modo de ejemplo, una llave de 128 bits contiene 2^{128} (340,282,366,920,938,463,463,374,607,431,768,211,456) posibles

claves, mientras que una de 256 bits contiene 2^{256}, es decir un número con el doble de dígitos que el anterior. Por ende, un ataque informático exitoso a las claves criptográficas de 128 o más bits resulta inviable.

79. **Ataque de "fuerza bruta"**: es aquél en el que se utiliza un gran poder computacional para descifrar una contraseña probando todas las combinaciones posibles.

80. **Encriptación punto a punto** ("End to end") es un mecanismo de encriptación en el cual el mensaje con su contenido es cifrado en el dispositivo del emisor mediante una clave propia, generada aleatoriamente para esa comunicación, que acompaña al mensaje en tránsito y llega al dispositivo del destinatario, siendo descifrada en ese momento sólo para las personas involucradas en esa conversación.

81. **"Perfect forward secrecy" (secreto perfecto hacia adelante)**: es un protocolo de manejo de llaves criptográficas que asegura que las llaves de sesión no puedan ser comprometidas incluso si la llave privada del servidor lo es. Ello, mediante la generación de una clave única para cada sesión iniciada por el usuario (a diferencia de los sistemas de encriptación más antiguos, en los que todas las sesiones se cifraban con una única clave que, en caso de ser comprometida, otorgaba acceso total). Es el sistema utilizado para proteger las comunicaciones en los principales servicios de mensajería por Internet, como Whatsapp o Telegram.

82. **PGP (Pretty Good Privacy):** Es un software de encriptación basado en el protocolo Open PGP diseñado para proporcionar privacidad, seguridad y autenticación para los sistemas de comunicación en línea. Creado originalmente para proteger mensajes de correo electrónico, su uso se ha extendido para incluir también las firmas digitales, la encriptación de disco completo y la protección de la red. PGP funciona con una clave (contraseña) pública y una privada. La clave pública o clave de sesión se utiliza para encriptar la información en formato plaintext que se pretende proteger, y la privada para desencriptarlo. A tal efecto, el receptor del mensaje le proporciona una clave pública (que se genera aleatoriamente para cada sesión de comunicación PGP) al emisor, que la utiliza para encriptar los datos. Luego, una vez transmitidos en forma encriptada tanto el texto del mensaje como la clave de sesión, el receptor utiliza su clave privada para descifrar la clave de sesión, que luego se usa para devolver el texto a formato plaintext.

83. **Voice over IP/VoIP (Voz sobre protocolo de internet):** agrupa a distintas aplicaciones para transmitir en tiempo real a través de la Internet información de audio como la voz humana, emulando el servicio telefónico tradicional. Sin embargo, a diferencia del sistema tradicional del Red Telefónica Pública Conmutada, las comunicaciones mediante sistemas de VoIP se realizan "par a par", sin intermediarios, lo que impide la interceptación de las comunicaciones mediante los sistemas habitualmente utilizados. Además, por lo general los paquetes de datos conteniendo las comunicaciones están protegidos por encriptación mientras se encuentran "en tránsito" por la Internet.

84. **Red Telefónica Pública Conmutada (Public Telephone Switched Network o PTSN)**: es aquella en la que todas las llamadas telefónicas son establecidas a través de un conmutador central que es el que dirige la llamada saliente hacia su destino buscado (el teléfono del receptor de la llamada, identificado por su número de línea).

85. **Encriptación de disco completo (Full-Disk Encryption o FDE)**, es el proceso mediante el cual se encripta la totalidad del disco duro de una computadora (incluyendo al sistema operativo), permitiendo el acceso a los datos contenidos en el mismo sólo a partir de una autenticación exitosa (mediante el ingreso de la correspondiente contraseña) en el producto FDE. Esto implica que ninguna persona que carezca de la contraseña (incluyendo a las empresas fabricantes del producto FDE) puede acceder a la información contenida en el dispositivo. Existen productos FDE para computadoras personales, laptops y dispositivos de almacenamiento (TrueCrypt, BitLocker y PGP, entre otros). Además, los smartphones de las principales compañías tecnológicas mundiales (Apple y Google) están protegidos por FDE, imposibilitando el ingreso si no se cuenta con la contraseña numérica o biométrica para abrir el teléfono.

En referencia con nuevas herramientas tecnológicas de investigación

86. **Análisis de la Blockchain (Chain analysis):** es el proceso de inspección, identificación, segmentación y elaboración de modelos para la representación visual de los datos públicos contenidos en la Blockchain, a fin de obtener información útil sobre quienes llevan a cabo transacciones con criptomonedas. Este análisis por lo general es llevado a cabo por compañías privadas que utilizan algoritmos propios para mapear las transacciones efectuadas por los/las usuarios/as de criptomonedas y vincular a unos con otros.

87. **Dusting attack:** consiste en el envío de rastros o trazas de criptomonedas (denominadas “dust” -polvo) a miles (a veces cientos de miles) de direcciones, con el objeto de monitorear su actividad y desanonimizar a sus verdaderos titulares. Los rastros o trazas de criptomonedas pueden encontrarse en la mayoría de las blockchains públicas, incluyendo Bitcoin, Litecoin, Bitcoin Cash y Dogecoin, entre otras.

88. **Inteligencia de fuente abierta (Open Source Intelligence u OSINT)**: denominación que alude a la recolección, procesamiento y análisis sistemático de información de acceso abierto. Esto es: la información disponible para el público en general sin restricciones (en redes sociales, páginas web, buscadores, portales de noticias, registros públicos, etc.).

89. **APIs (Application programming interfaces):** son una serie de requisitos que gobiernan el modo en que las aplicaciones se comunican entre sí, para lo cual se “expone” en forma limitada una parte de las funciones internas de un determinado programa. Esto permite que las aplicaciones compartan datos entre sí y lleven a cabo acciones en beneficio de las otras sin que sea necesario

compartir el código completo del software. Las APIs logran esto limitando el acceso exterior solo a un conjunto específico de funciones, por lo general las relacionados con pedidos de distintos tipos de información.

90. **Spyware:** es un tipo de malware (programa malicioso) diseñado para funcionar en forma subrepticia dentro de un sistema informático y registrar información en secreto. Puede supervisar y copiar lo que se escribe ("registrador de teclas" o "keylogger"), lo que ingresa o egresa del sistema, capturar la información almacenada o incluso activar los micrófonos o cámaras del equipo.

91. **Vulnerabilidad:** es un defecto o debilidad en el código de un sistema informático que puede ser manipulada por un atacante para exponer total o parcialmente dicho sistema.

92. **Exploit:** es el método (código informático) utilizado para obtener acceso no autorizado a un sistema vulnerable. Los exploits pueden ser programas, o simplemente un conjunto de comandos o acciones diseñados para "explotar" una vulnerabilidad del sistema.

93. **Spear phishing:** es un método para lograr el acceso subrepticio a un sistema informático basado en el engaño de los/las usuarios/as legítimos/as del mismo mediante técnicas de "ingeniería social", como por ejemplo la creación de un mensaje de correo electrónico o SMS que parezca provenir de una fuente confiable para el objetivo, el cual contiene un "llamado a la acción" (acto requerido, que puede consistir en conectarse con un link o abrir un archivo adjunto).

94. **Ingeniería social (Social ingeneering):** el término alude a la práctica de obtener información confidencial o la realización de una determinada acción a través de la manipulación de usuarios legítimos. Consiste en el uso de engaños a fin de conseguir la entrega de información relevante, acceso o privilegios en sistemas de información, que permitan al atacante concretar algún acto que perjudique o exponga a la persona u organismo objeto de ataque.

95. **Ataque de abrevadero (Watering hole attack):** es aquél en el que el atacante toma el control de un servidor o una página web y lo/la manipula de modo tal que descargue un spyware en el sistema de los/las usuarios/as que accedan al/la misma o lleven a cabo alguna clase de acción mientras se encuentren conectados.

96. **Ataque de cadena de suministro (Supply chain attack):** es aquél en el cual se explotan los puntos débiles en la cadena de suministro de una organización, aumentando las posibilidades de éxito sacando provecho de la confianza de los miembros de la organización en los productos originados en dicha cadena. Un ejemplo de este ataque consiste en introducir el spyware en actualizaciones de software, de modo tal que sean instaladas y ejecutadas por los/las clientes/as de la organización a partir de la relación de confianza con la entidad emisora.

97. **Paquet sniffers (Olfateadores de paquetes de datos):** se trata de programas para fines de monitoreo de red, específicamente diseñados para identificar, dentro del tráfico de Internet que fluye a través de un punto de intercepción, paquetes de datos que cumplan con distintos parámetros fijados por el/la usuario/a.

Referidos a la evidencia electrónica o digital

98. **Evidencia electrónica (o digital):** es la información generada, almacenada o transmitida mediante dispositivos electrónicos que puede ser utilizada como prueba ante un tribunal.

99. **Evidencia sobre contenido:** es la que atañe a la sustancia de una comunicación, esto es: la parte que representa lo que el/la emisor/a desea comunicarle al/la receptor/a de dicha comunicación.

100. **Evidencia de envoltorio, relativa a datos o "no de contenido"**: comprende a toda la información vinculada a la comunicación, salvo el contenido. Por ejemplo, la fecha y hora de la comunicación, su duración, los números telefónicos o direcciones IP de las personas que intervinieron, las celdas de telefonía celular involucradas en la comunicación, etc.

101. **Evidencia en tránsito:** es la evidencia digital que es capturada en tiempo real mientras se encuentra en movimiento a través de la red. Puede tratarse de evidencia de contenido, de envoltorio o ambas.

102. **Evidencia almacenada:** es la que, al momento de ser recolectada, no se encuentra en movimiento sino almacenada en algún servidor (interno o externo). Al igual que la anterior, puede tratarse de evidencia de contenido, de envoltorio o ambas.

103. **Evidencia de localización:** es la que se refiere a la ubicación de un determinado dispositivo de comunicación en un momento dado y, por consiguiente, también de la persona que lo estaba utilizando en ese momento. No es evidencia de contenido.

104. **Metadatos:** son "datos sobre datos". No se trata de información creada por el usuario ("datos activos" o "active data") sino información sobre la información: fecha de creación de los documentos, autor, cambios efectuados, datos sobre el sistema o equipo con el que fueron creados, datos de transmisión, etc.; a la que por lo general se puede acceder solo operando digitalmente (esto es: no aparece por defecto en las pantallas).

105. **Almacenamiento en la nube (o computación en nube):** es el servicio ofrecido por determinadas compañías que permite al/la usuario/a almacenar información digital en servidores externos que son propiedad del proveedor del servicio. Comprende tres grandes categorías de servicios: *i*) "infraestructura como servicio" ("infrastructure as service" o IaaS), *ii*) "software como

servicio" ("software as service" o SaaS) y *iii*) "plataforma como servicio" ("platform as service" o PaaS). La primera refiere a la provisión de "máquinas" (servidores) a través de Internet, la segunda a la de aplicaciones de software por la misma vía y la tercera a la provisión de una red completa (incluyendo servidores, sistemas operativos y espacio de almacenamiento).

106. **Hash criptográfico (Cryptographic hash):** es un algoritmo matemático que crea, a partir de una entrada, una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado y que sólo puede volverse a crear con esos mismos datos. De este modo se asegura que no se ha modificado el archivo, ya que cualquier cambio en la información, por pequeño que sea, altera totalmente el "hash", siendo imposible encontrar otra información que tenga como resultado el mismo valor alfanumérico.

107. **Imagen forense:** Se trata de una copia "bit por bit" ("bitstream copy") del contenido de un archivo, disco rígido o servidor, con la finalidad de permitir el análisis informático forense del mismo sin alterar el original. Esta copia o "imagen" difiere de las tradicionales, como las que se llevan a cabo cuando se transfieren archivos informáticos de una carpeta a otra o de una computadora a otra, en que duplica cada bit del original, por lo que se trata de un clon exacto de aquél. Si se realiza una imagen forense de un disco, la duplicación comprende a todos los archivos, los espacios vacíos, la "tabla maestra de archivos" ("master file table") y los metadatos en exactamente el mismo orden en que se encuentran en el original.

IV. ASPECTOS RELEVANTES VINCULADOS A LA INVESTIGACIÓN, INCAUTACIÓN Y DECOMISO DE ACTIVOS VIRTUALES

A. Lavado de activos y financiación del terrorismo mediante activos virtuales

108. El recurso al uso de activos virtuales para el lavado de activos (criptolavado) es, de inicio, una derivación natural del surgimiento de los mercados online de bienes y servicios ilegales (drogas, armas, virus informáticos, servicios de hackeo, etc.) en la denominada "Red oscura" ("Dark web" o "Darknet"). Esto es: el sector de la Internet al que sólo puede accederse con herramientas tecnológicas que permiten la navegación anónima, como el sistema TOR. Este fenómeno criminal, a su vez, es consecuencia de la aparición del Bitcoin en 2009, que posibilitó el funcionamiento de estos "mercados oscuros" al ofrecer un medio de pago, en principio, también anónimo.

109. La aparición del primero de estos mercados (Silk Road) a comienzos del 2011 marcó el comienzo de una nueva etapa en el comercio de bienes y servicios ilícitos. A pesar de haber sido cerrado con bastante rapidez por las autoridades, fue inmediatamente reemplazado por otros mercados similares. A partir de allí, los "mercados oscuros" han proliferado en la Red, y hoy son fuente de un alto porcentaje de los fondos ilícitos que se reciclan mediante los AV y los servicios

asociados a estos. Al respecto, un estudio que analizó las transacciones con Bitcoin entre 2013 y 2016[31] concluyó que la casi totalidad de los bitcoins de origen ilícito lavados a través de plataformas de intercambio de criptomonedas provenían de los mercados de la Red oscura.

110. No obstante ello, también se recurre a los AV para legitimar fondos provenientes tanto de ciberdelitos propiamente dichos (Ramsonware, fraudes informáticos, estafas como la reciente estafa piramidal "Plus Token" en China[32], etc.) como de ilícitos cometidos en el mundo físico, como por ejemplo el cobro de sobornos. La mayoría de los esquemas criminales que involucran AV no son necesariamente novedosos, sino variantes de los esquemas tradicionales realizados sacando provecho de los avances tecnológicos[33].

111. El proceso de "criptolavado" admite las mismas tres etapas que el lavado de activos tradicional (colocación, estratificación e integración). Sin embargo, las maniobras asociadas a cada una de esas fases tienen características propias, producto de la naturaleza de los AV involucrados. Así, por ejemplo, la propia necesidad de que exista, o no, una etapa de colocación depende de si los fondos ilícitos son obtenidos en moneda fiduciaria o directamente en criptomonedas. Ello así, desde que en el primer supuesto es necesario efectuar una conversión de una moneda a otra, mientras que en el segundo no lo es.

112. En caso de que se requiera cumplir la etapa de colocación, se suele ser recurrir a un PSAV -por lo general una plataforma de intercambio de criptomonedas- para convertir la moneda fiduciaria en bitcoins u otro AV semejante. Dicha circunstancia puede ser explotada por las autoridades encargadas de la ALA/CFT o por las agencias de investigación del Estado para obtener información sobre las personas que intentan llevar adelante una maniobra de LA/FT con AV. De allí que, en especial a partir de la actualización de las 40 Recomendaciones del GAFI en 2019, muchos países han ajustado su normativa interna a lo establecido en la nueva Recomendación 15 del citado organismo, y ahora exigen a los PSAV que lleven a cabo tareas de DDC respecto de sus clientes y reporten operaciones sospechosas.

113. Para sortear este obstáculo, es posible que los lavadores recurran a los métodos empleados para lograr los mismos fines con respecto a las entidades financieras tradicionales, como por ejemplo la estructuración de los fondos o el uso de testaferros. Otra vía consiste en concretar la colocación a través de un PSAV localizado en una jurisdicción en la que no esté sometido a deberes de ALA/CFT, o que incumpla con las obligaciones vigentes. Aprovechando el carácter trasnacional de la Internet, algunos PSAV han buscado el modo de prestar servicios a clientes/as en ciertas

[31] Ver: FANUSIE, Yaya J. / ROBINSON, Tom: "Bitcoin laundering: An analysis of illicit flows into digital currency services", Elliptic Center on Sanctions & Illicit Finance, enero 2018.
[32] Este fraude arrojó ganancias ilícitas de más de 3.000 millones de dólares, que en su mayoría fueron reciclados exitosamente a través de servicios de conversión de criptomonedas. Se estima que la transformación posterior de esos fondos en moneda fiduciaria fue lo que ocasionó el brusco descenso del valor del Bitcoin en agosto de 2019 (ver: DUPUIS, Daniel / GLEASON, Kimberley: "Money laundering with cryptocurrency: Open doors and the regulatory dialectic", Journal of Financial Crime, agosto 2020).
[33] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 12 § 22.

jurisdicciones sin registrarse en las mismas, a fin de evitar el cumplimiento de obligaciones de ALA/CFT, como se ilustra en el siguiente caso[34]:

Caso § 1: BitMex. Plataforma de intercambio de AV en infracción a la normativa de ALA/CFT:
En octubre de 2020, el Departamento de Estado de los EE.UU. procesó a cuatro ejecutivos de la plataforma de intercambio de AV BitMex por infracciones a la normativa antilavado de ese país.
A pesar de prestar servicios a al menos 85.000 clientes en los EE.UU. y manejar la mayor parte de su infraestructura financiera desde ese país, BitMex nunca se registró ante las autoridades estadounidenses.
La principal controlante de BitMex era la firma HDR Global Trading Ltd., incorporada en un refugio fiscal (las Islas Seychelles), donde nunca tuvo operaciones ni empleados. La plataforma era propiedad de una serie de compañías pantalla (HDR Global Trading Ltd., 100x Holdings, ABS Global Trading, Shine Effort y HDR Services) controladas por las mismas personas. El propio CEO declaraba domicilio legal las Islas Seychelles, pero era propietario de parte de las acciones de BitMex a través de una LLC registrada en Delaware, que era titular de cuentas bancarias en instituciones financieras en los EE.UU.
Se acusó a BitMex de ser una entidad financiera no registrada, brindando servicios a clientes en los EE.UU. a pesar de declarar que su sistema está diseñado para excluirlos, como así también de infracciones a la normativa de ALA/CFT, incluyendo el borrado de información crítica sobre sus clientes.

114. De todas maneras, la conversión de grandes volúmenes de fondos ilícitos en AV puede resultar problemática. El mercado de criptomonedas todavía es relativamente pequeño, de modo tal que una compra masiva puede despertar sospechas. Tal como quedó de manifiesto en el caso de las ganancias ilícitas de la estafa Plus Token, una venta o compra masiva de criptomonedas tiende a generar alteraciones bruscas en el precio de dichos valores, susceptibles de llamar la atención de las autoridades. En cualquier caso, y debido a la preponderancia de esa criptomoneda, es probable que un volumen de alto de operaciones pase más desapercibido en la Blockchain de Bitcoin, mientras que transferencias por montos altos seguramente resultarán conspicuas en las de monedas menos utilizadas.

115. Una vez cumplida la fase de colocación, existen múltiples formas de llevar a cabo la estratificación de los fondos. Por un lado, puede concretarse mediante una serie de transacciones entre monederos de AV controlados por distintas personas o incluso por una sola, ya que las criptomonedas admiten que los/las usuarios/as mantengan un número indefinido de direcciones. Esta circunstancia, sumada a la simplicidad de creación de nuevas direcciones, la disociación entre estas y las identidades en el mundo real, la velocidad con que se concretan las transferencias (mayor que la de las llevadas a cabo en la red de corresponsalía bancaria) y la facilidad con la que cruzan fronteras nacionales y regulatorias, posibilita la creación de patrones de estratificación extremadamente complejos.

[34] Fuente: CipherTrace: “Cryptocurrency crime and anti-money laundering report”, febrero 2021.

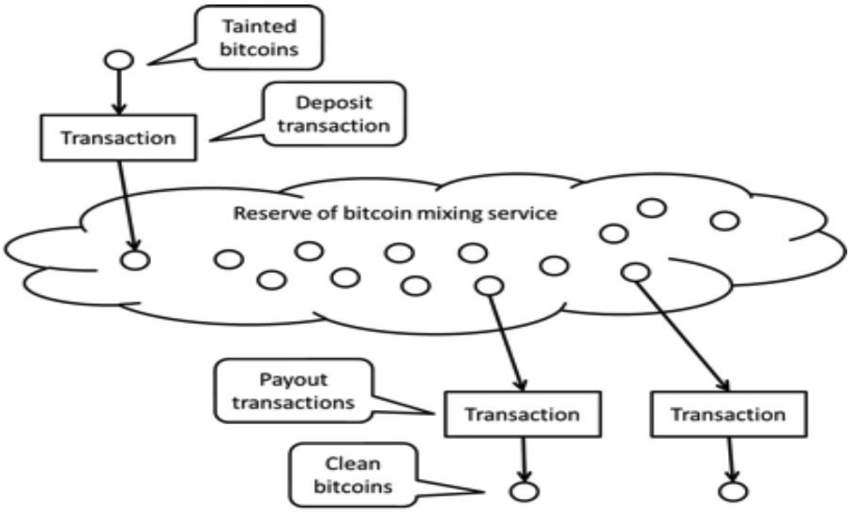
116. Estas características de los AV no sólo resultan útiles para el criptolavado de activos, sino que también pueden ser explotadas para el financiamiento del terrorismo. Así, la facilidad con que puede convertirse la moneda fiduciaria en criptomonedas para luego transferirlas a través de las fronteras con rapidez y con un nivel relativamente alto de anonimato, ha derivado en que algunas organizaciones terroristas recurran a estos métodos para obtener fondos recibiendo "donaciones" anónimas en AV. Asimismo, esta clase de activos también puede ser utilizado para adquirir armas u otros elementos en los mercados virtuales de la Dark web.

117. Los PSAV cumplen una función esencial en los esquemas de criptolavado, ya sea en la fase de colocación (para la conversión de moneda fiduciaria en AV), durante la fase de estratificación (por ejemplo, permitiendo el cambio de una criptomoneda por otra o brindando servicios de "mezclado") o en la etapa final, donde los/las beneficiarios/as de la maniobra convierten los fondos nuevamente a moneda fiduciaria[35]. Ello ha derivado en la aparición de plataformas de intercambio de AV específicamente creadas y estructuradas para facilitar el criptolavado[36]. En tal contexto, un informe reciente concluye que un tercio del volumen de tráfico transfronterizo de bitcoins se vuelca a PSAV con políticas deficientes de ALA/CFT[37].

118. Entre los principales servicios que pueden ofrecer los PSAV para asistir a los/las lavadores/as de fondos ilícitos están los de "mezclado" ("mixing") de criptomonedas. Los denominados "mezcladores" o "conmutadores" ("mixers" o "tumblers") funcionan como servicios independientes de lavado de activos, que combinan los ingresos y egresos de fondos de distintos/as usuarios/as para tornarlos indistinguibles entre sí. En tal contexto, el paso por un "mezclador" sustituye la transferencia de AV entre dos direcciones (por ejemplo, de Bitcoin), de modo tal que los fondos de origen ilícito que una persona pretende transferir a otra se entremezclan con los provenientes de muchas otras direcciones de AV antes de ser finalmente enviadas a la del/la destinatario/a, dificultando la identificación de la dirección de origen y de las cuentas asociadas con los fondos de origen ilícito[38]. Ello, como se ilustra en el siguiente gráfico[39]:

[35] Ver: GAFI: "Guidance for a risk-based approach: Virtual currencies", junio 2015.
[36] Ver: GAFI: "Professional money laundering", julio 2018, págs. 45/46.
[37] Ver: CipherTrace: "Cryptocurrency crime and anti-money laundering report", febrero 2021, pág. 6. Si bien, en el mismo informe, se reporta una baja pronunciada del porcentaje global de bitcoins canalizados a PSAV de alto riesgo, ello se debe fundamentalmente al rápido incremento del interés en dicha moneda como instrumento de inversión, que ha determinado una merma de la proporción estimada de bitcoins de origen ilícito del 57% entre 2019 y 2020. Ello se debe en gran medida al enorme aumento del valor de los bitcoins, que al momento de ser lanzados estaban valuados en menos de un centavo de dólar cada uno, mientras que en febrero de 2021 alcanzaron un valor global de 200.000 millones de dólares (ver: FANUSIE, Yaya J. / ROBINSON, Tom: "Bitcoin laundering: An analysis of illicit flows into digital currency services", Elliptic Center on Sanctions & Illicit Finance, enero 2018, pág. 1).
[38] Ver: GAFI: "Guidance on financial investigations involving virtual assets", Junio 2019, pág. 34, § 109.
[39] Fuente: VON WEGBERG, Rolf / OERLEMANS, Jan-Jaap / VAN DEVENTER, Oscar: "Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using Bitcoin", Journal of Financial Crime, Vol. 25, N° 2, 2018, págs. 419/432.

Gráfico 1: funcionamiento de un mezclador:



119. El concepto básico de los mezcladores se asemeja al de los fondos de inversión, en los múltiples individuos acumulan sus fondos para obtener un beneficio colectivo. La diferencia es que, en el caso de los mezcladores, el fondo común es utilizado para concretar múltiples transacciones con criptomonedas, y el beneficio es lograr un mayor grado de anonimato impidiendo la vinculación de las transferencias con direcciones de AV específicas.

120. Los mezcladores dedicados al LA/FT por lo general cobran una comisión por sus servicios, no mantienen registros de sus usuarios/as y pueden opacar su infraestructura operando como "servicios ocultos" del sistema TOR. Desde el punto de vista de las AOP, el uso de servicios de mezclado por parte de las personas objeto de investigación dificulta considerablemente la reconstrucción de la cadena de transacciones (salvo que dicha persona concentre una cantidad significativa de los fondos procesados a través del mezclador o no se utilicen métodos aleatorios o semi aleatorios para combinar los AV de los/las usuarios/as)[40].

121. Los mezcladores ocupan un lugar importante en el mercado de AV de origen ilícito, a punto tal que algunos mercados ocultos de la Red oscura tienen integrado un mezclador para facilitar el lavado de los fondos provenientes de la compraventa de bienes y servicios ilegales. De allí que, pesar de representar solo un pequeño porcentaje del tráfico de bitcoins desde y hacia PSAV, los

[40] Ver: GAFI: "Guidance on financial investigations involving virtual assets", Junio 2019, pág. 35, § 110.

mezcladores son mucho más propensos a ser utilizados para el criptolavado[41]. Algunos de los mezcladores más utilizados publicitaban en forma manifiesta la posibilidad de recurrir a esos servicios para "limpiar" "monedas sucias", tal como se ilustra a continuación[42]:

Gráfico 2: Explicación del funcionamiento del mezclador "Helix":

122. El recurso a los PSAV también facilita la concreción de otras metodologías de estratificación mediante AV, como el "Chainhopping" (literalmente, "salto de cadenas"), que consiste en intercambiar distintas criptomonedas entre sí, a fin de cortar la cadena de transacciones en las respectivas blockchains, maniobra que -según algunos estudios- se ha convertido en uno de los métodos preferidos para el criptolavado[43].

B. Importancia de la imposición de deberes de ALA/CFT a los PSAV para la prevención e investigación de maniobras de LA/FT con AV

123. En atención a lo expuesto, la imposición de deberes de información y reporte a los PSAV resulta un elemento central de cualquier estrategia de ALA/CFT referida a AV que pretenda ser efectiva. A su vez, constituye una herramienta fundamental para el desarrollo de las investigaciones patrimoniales sobre conductas de LA/FT con criptomonedas, en la medida en que saca provecho del rol esencial que juegan los PSAV en su carácter de intermediarios entre el mundo físico y el virtual, es decir entre los AV y la moneda fiduciaria.

124. En esa dirección, la nueva Recomendación 15 del GAFI establece que los países miembros deben adecuar su regulación interna de modo tal de extender las reglas de ALA/CFT, registro y reporte que pesan sobre los prestadores de servicios financieros o no financieros a los PSAV,

[41] Así, por ejemplo, entre 2013 y 2015, más del 20 % de las transacciones concretadas por "mezcladores" provino directamente de fuentes ilícitas (ver: FANUSIE, Yaya J. / ROBINSON, Tom: "Bitcoin laundering: An analysis of illicit flows into digital currency services", Elliptic Center on Sanctions & Illicit Finance, enero 2018, pág. 7).
[42] Fuente: Página web del ya desaparecido Mixer "Helix", cuyo administrador, Larry Dean Harmon, fue arrestado en febrero de 2020 por lavado de activos.
[43] Ver: GAFI: "FATF report to G20 Finance Ministers and Central Bank Governors", julio 2018, § 35 y LEE, Seunghyeon / YOON, Changhoon / KANG, Heedo / KIM, Yeonkeun / KIM, Yongdae / HAN, Dongsu / SON, Sooel / SHIN, Seungwon: "Cybercriminal minds: An investigative study of cryptocurrency abuses in the Dark Web", Network and Distributed Systems Security (NDSS) Symposium, 2019.

entendidos como las personas naturales o legales que llevan a cabo comercialmente una o más de las siguientes operaciones en beneficio de otra persona legal o natural: *i)* intercambio entre AV y monedas fiduciarias; *ii)* intercambio entre una o más clases de AV; *iii)* transferencia de AV (entendida como el desplazamiento de dichos activos de una dirección virtual o cuenta a otra); *iv)* custodia y/o administración de AV o de instrumentos que permitan el control de los mismos; y *v)* participación en o provisión de servicios financieros vinculados a la oferta y/o venta de AV por parte de los usuarios.

125. Por consiguiente, quedan comprendidos dentro de la definición los principales actores del ecosistema de AV, como las plataformas de intercambio de criptomonedas y los servicios de transferencia de AV; algunos proveedores de monederos de AV (como los que alojan monederas o mantienen custodia o control sobre los AV de otra persona natural o legal, sus monederos y/o sus claves privadas); y los proveedores de servicios financieros vinculados a la emisión, oferta o venta de AV; entre otros posibles modelos de negocios[44].

126. La importancia de estos actores reside en que fungen como el principal punto de entrada al sistema financiero global para los criminales que buscan convertir los fondos obtenidos o mantenidos en forma de AV en moneda fiduciaria. Al respecto, es importante tener presente que, si bien es cierto que algunos negocios en muchos países admiten el pago con criptomonedas para la adquisición de bienes y servicios, la mayoría de los bienes siguen pagándose con moneda fiduciaria. Por consiguiente, lo más probable es que las ganancias obtenidas o recicladas en el ciberespacio (mediante AV) eventualmente sean transferidas al mundo real y convertidas en moneda fiduciaria, para que su titular pueda gozar de las mismas o reinvertirlas en su negocio ilegal (por ejemplo, adquiriendo elementos que sólo pueden ser pagados con divisas físicas).

127. En este escenario, los nexos entre el mundo físico y el virtual constituyen el principal punto focal de las investigaciones patrimoniales referidas a la operatoria con AV, ya que es allí donde las transacciones perpetradas en el ciberespacio -en un contexto de (pseudo) anonimato- pueden llegar a conectarse con una o varias personas de existencia real. Lo mismo ocurre en sentido opuesto, si los/las criminales pretenden recurrir al uso de criptomonedas para la colocación o estratificación de fondos obtenidos en moneda fiduciaria, en cuyo caso los PSAV serán el punto de entrada al ecosistema de los AV.

128. Es evidente que si los PSAV están obligados a requerir el espectro completo de información dirigida a identificar a sus clientes y establecer el origen de los fondos con los que operan, el recurso a los AV perderá parte de su atractivo en comparación con la moneda fiduciaria. A su vez,

[44] Ver: GAFI: "Virtual assets and virtual assets service providers. Guidance for a risk-based approach", junio 2019, pág. 14, § 35.

la regulación de ALA/CFT les brinda a los organismos de supervisión y a las AOP un punto de partida importante para la identificación y persecución de lavadores de activos y otros criminales[45].

129. El punto de ingreso o salida más importante hacia y desde el ecosistema de los AV son las plataformas de intercambio de criptomonedas ("exchanges"), que presentan distintas formas y modelos de negocios. Su función principal consiste en permitir a sus clientes comprar o vender AV a cambio de moneda fiduciaria, otros AV, u otros bienes o valores negociables; a cambio de una tasa, comisión u otra forma de remuneración. Por lo general, aceptan una amplia variedad de modos de pago, incluyendo efectivo, transferencias bancarias, pagos con tarjetas de crédito o débito, o incluso otros AV[46].

130. Existen dos grandes tipos de plataforma de intercambio de criptomonedas: centralizadas o descentralizadas. En el primer supuesto, los AV son transferidos "a través" de la plataforma, que actúa como intermediaria. Es decir, forma parte de la transacción, comprándole los AV al vendedor y vendiéndoselos al comprador. En algunas de estas plataformas centralizadas, los usuarios primero depositan moneda fiduciaria o criptomonedas en cuentas en custodia, que luego se utilizan para fondear las transacciones. Las plataformas descentralizadas, en cambio, solo ofrecen un ámbito para que los compradores y vendedores se encuentren para llevar a cabo los intercambios, que se concretan exclusivamente bajo un formato P2P[47]. Aunque la mayoría de las plataformas son centralizadas, ello las hace vulnerables al hackeo, motivo por el cual existe una tendencia en la comunidad de AV en favor de sustituirlas por la variante descentralizada[48].

131. A diferencia de las plataformas centralizadas, que están comprendidas en la definición de PSAV del GAFI (lo cual indica que deben estar sometidas a las obligaciones de DDC y reporte establecidas en la normativa de ALA/CFT, conforme la nueva Recomendación 15 del citado organismo), las plataformas P2P, en principio, no lo están[49]. Ello, toda vez que se entiende que, por el momento, el uso de este último tipo de plataformas no se ha generalizado a punto tal de constituir un riesgo relevante de LA/FT.

[45] Ver: MBIYANGA, Stefan "Cryptolaundering: Anti-money laundering regulation of virtual currency exchanges", Journal of Anti-Corruption Law, Vol. 3, N° 1, 2019, pág. 1.
[46] Ver: GAFI: "Virtual assets and virtual assets service providers. Guidance for a risk-based approach", junio 2019, págs. 14/15, § 37.
[47] Ver: MBIYANGA, Stefan "Cryptolaundering: Anti-money laundering regulation of virtual currency exchanges", Journal of Anti-Corruption Law, Vol. 3, N° 1, 2019, pág. 4.
[48] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 67, §§ 238/239.
[49] Ver: GAFI: "12-month review of the revised FATF standards on virtual assets and virtual asset service providers", junio 2020, pág. 7, § 20. Sin embargo, el Instituto para la Estabilidad Financiera (FSI, por sus siglas en inglés) destaca que el uso de plataformas P2P constituye una fuente potencial de riesgos, precisamente debido a que no involucra a ninguna entidad que se encuentre alcanzada por obligaciones de ALA/CFT. Este riesgo podría incrementarse si las criptomonedas son adoptadas masivamente, y el volumen transado sin ningún control a través de estas plataformas se incrementa en forma proporcional (ver: Financial Stability Institute: "Supervising cryptoassets for anti-money laundering", FSI insights on policy implementation, N° 31, abril 2021, pág. 18. Se citan datos de la empresa CipherTrace indicando que el 40% de los pagos con Bitcoin en 2020 fueron a parar a monederos privados).

132. Otra vía para el intercambio entre AV y moneda fiduciaria está dada por el recurso a los denominados "cajeros" o "quioscos" de AV ("VA ATM"). Se trata de máquinas similares a los cajeros automáticos, ubicadas en muchas ciudades en todo el mundo, que ofrecen un punto físico en el que las personas pueden comprar o vender criptomonedas. En ausencia de una regulación y supervisión efectiva, los cajeros de AV pueden convertirse en una vulnerabilidad del sistema de ALA/CFT; y, de hecho, ya existen reportes que indican que los operadores de esta clase de cajeros tienden a cumplir en menor medida que otros PSAV con las obligaciones de DDC y reporte establecidas en la normativa. A su vez, los cajeros de AV han sido relacionados con actividades ilícitas, habiendo sido utilizados por narcotraficantes, redes de fraude con tarjetas de crédito o de prostitución y plataformas de intercambio P2P no registradas[50]. Esta fue la vía utilizada en el caso que se detalla a continuación[51]:

Caso § 2. Operación Glutons. Uso de Cajeros Bitcoin para LA.
La Guardia Civil de España reportó a través de Europol el uso frecuente de cajeros Bitcoin operados por una compañía objeto de investigación, por parte de una organización criminal con antecedentes por narcotráfico, para convertir las ganancias ilícitas en AV. A fin de eludir los controles de ALA/CFT, las personas encargadas de hacer los depósitos aplicaban técnicas de "pitufeo" (estructuración), dividiendo los fondos en partidas de menos de 1.000 EUR. En un mismo día, llevaban a cabo múltiples depósitos en distintos cajeros de AV en diferentes locaciones, por montos totales de aproximadamente 200.000 EUR mensuales.
La sospecha de las autoridades españolas era que existía complicidad con la operatoria ilegal por parte de la compañía administradora de los cajeros de AV, ya que no se efectuaron tareas de DDC ni se presentaron ROS referidos a las maniobras antes mencionadas.

C. Diagnóstico sobre la situación regional en orden a la regulación de los AV y PSAV

133. Como se viene señalando, para el desarrollo de una estrategia de ALA/CFT efectiva respecto del posible uso ilegal de AV, resulta esencial que exista una regulación coherente, a nivel global, tanto en lo que respecta a dichos valores como a los PSAV. En sentido opuesto, la ausencia de una regulación coherente constituye uno de los principales motivos por los que los AV son vulnerables a la explotación con fines ilícitos. Por tal motivo, el GAFI ha señalado que la eficacia de los estándares revisados en 2019 para prevenir el LA/FT con AV depende de su efectiva implementación por parte de todas las jurisdicciones, como así también del cumplimiento de las obligaciones que dichos estándares imponen a las entidades del sector privado[52].

[50] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 40, § 131.
[51] Fuente: GAFI: "Guidance on financial investigations involving virtual assets", Junio 2019, pág. 40, § 132
[52] Ver: GAFI: "12-month review of the revised FATF standards on virtual assets and virtual asset service providers", junio 2020, pág. 2, § 3.

134. En tal contexto, el referido organismo llevó a cabo, con posterioridad a la actualización de las 40 Recomendaciones, una revisión anual global acerca de la implementación de los estándares revisados por parte de las distintas jurisdicciones y del sector privado. Como resultado de la misma, el GAFI concluyó que, en general, tanto el sector público como el privado han hecho progresos en la implementación de los estándares revisados. Destacó, en tal sentido, que 35 de las 54 jurisdicciones evaluadas reportaron haber implementado dichos estándares, con 32 de ellas regulando la actividad de los PSAV y los 3 restantes, prohibiéndola[53].

135. En cuanto atañe específicamente a Latinoamérica, con anterioridad a la actualización de las 40 recomendaciones del GAFI y la evaluación posterior de dicho organismo, el Grupo de Expertos para el Control del Lavado de Activos de la OEA llevó a cabo, entre los años 2017 y 2018, un relevamiento de la situación en orden a los AV a nivel regional[54]. En tal contexto, se pudo establecer que la situación en ese momento presentaba las siguientes características:

- Carencia de regulación en orden al funcionamiento de los AV.
- Inexistencia de condenas por hechos ilícitos perpetrados con/involucrando AV.
- Estrategias de estudios incipientes, solamente a nivel de UIF.
- Identificación de portales de oferta de monedas virtuales en casi todos los países consultados, con la mayoría de ellos señalando la circulación de más de una criptomoneda.
- Existencia de un considerable sector de la economía que aceptaba como medio de pago monedas virtuales (en especial, Bitcoin).
- Ausencia de normas mínimas de usuarios/as y de regulación de ALA/CFT referidas a los AV y los PSAV.

136. Con respecto al rubro condenas o investigaciones, la OEA señaló que se había verificado una única investigación patrimonial referida al uso ilícito de AV en la región (el caso “Liberty Reserve”, en Costa Rica). Por otro lado, en lo tocante a la incautación o decomiso de esa clase de activos, el relevamiento no encontró experiencias en la materia, como así tampoco ningún tipo de regulación para la incautación, decomiso o administración de AV[55].

137. Por otro lado, es importante remarcar que en lo que respecta a la evaluación de la Recomendación 15 con base en las modificaciones del GAFI, a la fecha del presente informe, ningún país del GAFILAT ha sido evaluado en ese sentido, por lo que se podrán apreciar los resultados ya sea a los países faltantes en la 4ª Ronda de Evaluaciones Mutuas, o en futuros informes de seguimiento y otras rondas de evaluación.

[53] Ver: GAFI: “12-month review of the revised FATF standards on virtual assets and virtual asset service providers”, junio 2020, pág. 2, § 2.
[54] Ver: Organización de los Estados Americanos (OEA): “Estudio sobre nuevas tipologías en el lavado de dinero, específicamente en el uso de moneda virtual”, conclusiones de la XLV Reunión del Grupo de Expertos para el Control del Lavado de Activos – Subgrupo de Trabajo de UIF/OIC 2016-2018, OEA/Ser.L/XV. 4.45 DDOT/LAVEX/doc. 16/18, octubre de 2018.
[55] Ver: Organización de los Estados Americanos (OEA): “Estudio sobre nuevas tipologías en el lavado de dinero, específicamente en el uso de moneda virtual”, conclusiones de la XLV Reunión del Grupo de Expertos para el Control del Lavado de Activos – Subgrupo de Trabajo de UIF/OIC 2016-2018, OEA/Ser.L/XV. 4.45 DDOT/LAVEX/doc. 16/18, octubre de 2018.

138. Por otra parte, a los efectos de la elaboración de esta guía se dirigió un cuestionario a los puntos de enlace de la RRAG requiriendo información -entre otras cuestiones- sobre si se reconocían a nivel local los riesgos asociados de LA/FT asociados a los AV, si existía legislación local regulando su uso y sobre si se habían introducido normas de ALA/CFT referidas a los PSAV, en cumplimiento de la nueva Recomendación 15 del GAFI.

139. En tal contexto, 15 de los 17 países de la región (el 88 %) consideraron al uso de AV como fuente potencial de riesgo de LA/FT.

140. Sin embargo, la identificación del posible uso ilícito de AV como vulnerabilidad en orden al LA/FT no ha derivado, hasta el momento, en que se generalice la sanción de normas locales regulando el mercado de AV. Ello, toda vez que de las respuestas al cuestionario se desprende que sólo 4 de los 17 países del GAFILAT han legislado sobre dicha cuestión (24%).

141. Finalmente, en orden a la introducción de normativa dirigida a regular la actuación de los PSAV -en línea con lo establecido en la nueva Recomendación 15 del GAFI-, se advierte que, de los 11 países que respondieron a esta pregunta, 6 han ido abordando a los PSAV, (55%), mientras que los restantes 5 todavía no lo han hecho.

142. En esa dirección, se aprecia un avance en orden al reconocimiento del uso de AV como una fuente potencial de riesgos de LA/FT, el cual -si bien no conllevó una regulación genérica del mercado de criptomonedas en la mayoría de los países- si derivó en que la mayoría de ellos actualizaron su normativa local sobre ALA/CFT para incluir a los PSAV.

143. Dada la importancia de una adecuada regulación de la actuación de los PSAV -tanto a los efectos de prevenir el ALA/CFT, como de servir como fuente de información para las agencias de cumplimiento de la ley, en el marco de investigaciones patrimoniales sobre maniobras de LA/FT con AV- resulta esencial que el proceso de implementación de los nuevos estándares del GAFI siga avanzando en Latinoamérica, en procura de lograr un marco regulatorio homogéneo en toda la región.

D. Desafíos inherentes a la investigación del LA/FT con AV

144. La aparición de los AV como elemento para desarrollar novedosas tipologías de LA/FT supone el traslado de una porción importante de las investigaciones referida a dichas maniobras -así como las medidas tendientes a concretar la incautación y decomiso de los fondos- al ciberespacio, un escenario completamente diferente a aquél en que tradicionalmente venían desarrollándose. Ello obliga a las autoridades nacionales encargadas de la persecución del LA/FT en general, y de la investigación, identificación, incautación y decomiso de AV en particular, a enfrentar nuevos obstáculos y desafíos y, a su vez, a recurrir a nuevas estrategias y metodologías para seguir siendo eficaces.

145. En cuanto atañe a los obstáculos y desafíos, sobresalen el carácter "extraterritorial" atribuido al ciberespacio por muchos expertos; la libertad y velocidad del intercambio de datos informáticos (incluyendo los que pueden ser relevantes como evidencia o para identificar AV susceptibles de incautación o decomiso) a través de la Internet; el fenómeno de la "pérdida de conocimiento de la localización" de esos datos[56] y la consecuente dificultad para establecer la ley procesal que debe regir su recolección. A ello viene a sumarse la aparición de novedosas tecnologías que impiden -o cuanto menos dificultan en gran medida- el ejercicio, por parte de las agencias policíacas, de las facultades de vigilancia que las leyes locales les confieren, entre las que cabe mencionar -además de las relacionadas al funcionamiento de los AV- a los nuevos métodos de comunicación que sustituyen a la Red Telefónica Pública Conmutada" (RTPC)[57], los sistemas de navegación anónima en la Internet y la encriptación de comunicaciones y contenidos almacenadas, entre otros.

146. La problemática relacionada con la determinación de la normativa aplicable a la implementación de medidas de investigación restrictivas de derechos o tendientes a la incautación de AV en atención al carácter trasnacional de dichos valores es especialmente aguda en lo tocante a los AV descentralizados. Ello, toda vez que en lo que respecta a los centralizados (por ejemplo, las monedas virtuales emitidas en el ámbito de los "Videojuegos de rol multijugador masivos en línea" o MMORPGs, por sus siglas en inglés), al existir una autoridad administrativa central que controla el manejo de los activos, salvo disposición expresa en contrario, rige la normativa aplicable en la jurisdicción en la que tiene su base dicha autoridad.

147. Cuando se trata de activos descentralizados como las criptomonedas, en cambio, no existe -por diseño- una autoridad central que controle el flujo de los AV. Las monedas en sí no son otra cosa más que información digital (puntualmente, el registro de transferencias entre usuarios/as de la criptomoneda que se trate). Su localización a los efectos de la jurisdicción aplicable para una eventual incautación o decomiso es la que corresponda al lugar donde se encuentra el monedero en la que dicha información esta almacenada. Ahora bien: esta localización puede ser fija (si se trata de un monedero fijo) o puede no serlo, como ocurre cuando se trata de un monedero online, en especial si se encuentra "en la nube", en cuyo caso la información suele estar almacenada en servidores ubicados en data centers ubicados en puntos estratégicos del globo. Además, los datos electrónicos pueden estar en un solo lugar o distribuidos (en secciones) en varios servidores (incluso en diferentes países), y reacomodarse automáticamente dependiendo de la disponibilidad y demanda de espacio de almacenamiento en la nube en un momento determinado. También

[56] El cual reside en la imposibilidad de establecer a ciencia cierta la ubicación geográfica de datos digitales como resultado del uso de servicios de "computación en nube" para su almacenamiento y de factores tecnológicos asociados a dichos servicios, como la fragmentación de datos, el desplazamiento automático de los mismos (por cuestiones de espacio de almacenamiento) o la generación de múltiples copias de seguridad.
[57] Traducción de lo que se conoce, en idioma inglés, como Public Telephone Switched Network (PTSN). Esto es: aquél en el cual todas las llamadas telefónicas son establecidas a través de un conmutador central que es el que dirige la llamada saliente hacia su destino buscado (el teléfono del receptor de la llamada, identificado por su número de línea).

pueden estar almacenados en forma redundante, en múltiples copias, para que puedan ser recuperadas incluso si falla un servidor (o Data center).

148. Por consiguiente, en algunos casos puede ocurrir que ni la propia compañía que brinda el servicio de almacenamiento en la nube -y, por ende, tampoco las autoridades nacionales que pretendan incautar o decomisar AV- puedan establecer con precisión donde se encuentra un conjunto específico de datos digitales -por ejemplo, un monedero Bitcoin- en un momento determinado. Lo que supone, como lógica consecuencia, que tampoco puede establecerse qué país tiene jurisdicción para disponer o concretar la incautación o decomiso de las criptomonedas.

149. A esta problemática alude el concepto de "pérdida de conocimiento de la locación" acuñado en un documento del Consejo de Europa[58], que a su vez se da en el marco de un fenómeno más general, que es la deslocalización como rasgo esencial de la Internet o, más concretamente, del ciberespacio. Ello, en la medida en que se trata de un ámbito que no está situado en un sitio en concreto, sino que, en sentido funcional, está en todos a la vez, pero en sentido físico, en ninguno. Estas características chocan con el sostenimiento del principio de territorialidad como punto focal del ejercicio de la soberanía por los países a través de la aplicación de la normativa procesal en el ámbito de su jurisdicción territorial, en la medida en que ponen en crisis la posibilidad de establecer en dónde se encuentran los objetos a los que se refieren las normas. Ello, toda vez que la velocidad e imprevisibilidad de los flujos de información electrónica dificultan (o imposibilitan) la localización de los datos en un momento dado[59].

150. La evolución tecnológica conlleva, asimismo, otra serie de consecuencias derivadas de la aparición de desarrollos tecnológicos que pueden ser explotados por los/las cibercriminales (ya sea que se trate, a los efectos de la presente guía, de LA o FT) para eludir la acción de las autoridades o entorpecer su actuación. A su vez, el surgimiento, en paralelo, de sofisticadas herramientas de vigilancia o forenses ha convertido a la persecución del cibercrimen en una verdadera carrera armamentista entre los delincuentes y las agencias de investigación, con unos y otros buscando el modo de aprovechar los adelantos tecnológicos para prevalecer.

151. En este contexto, uno de los principales focos de conflicto se da en torno a las tecnologías de "anonimato por diseño" ("Anonymity by design"), que constituyen uno de los rasgos más importantes de las monedas virtuales descentralizadas como el Bitcoin, que han sido creadas con el fin específico de garantizarle a sus usuarios/as al menos cierto grado de anonimato. En esa dirección, el primer rasgo tendiente a lograr ese objetivo es, precisamente, la estructura descentralizada, carente de una autoridad central que pueda ser sometida a la supervisión estatal y conozca las verdaderas identidades de los/las usuarios/as. A tal efecto, las criptomonedas están

[58] Ver: SPOENLE, Jan: "Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal", Council of Europe Discussion Paper N° 31, 2010.
[59] Ver: DASKAL, Jennifer; "The un-territoriality of data", The Yale Law Journal, Vol. 125, N° 2, 2015, pág. 329.

organizadas como sistemas de intercambio P2P, en los que las interacciones se llevan a cabo en forma directa entre dos usuarios/as, sin intermediarios.

152. Sin perjuicio de ello, las distintas criptomonedas también implementan una serie de desarrollos tecnológicos adicionales dirigidos a incrementar el anonimato de los/las usuarios. Así, de acuerdo al modo en que están estructuradas, estos AV pueden ofrecer cuatro niveles distintos de anonimato, a saber: 1) pseudo anonimato: derivado del uso de pseudónimos (direcciones alfanuméricas) para oscurecer la identidad del/la usuario/a; 2) anonimato parcial ("Set anonymity"), en el que la identidad del/la verdadero/a usuario/a puede ser una entre varias posibles, lo que se consigue mediante el uso de "firmas en círculo"; 3) anonimato total del/la usuario/a, la cual se obtiene cuando el/la verdadero/a puede ser cualquiera de los nodos del sistema; y 4) transacciones confidenciales, en las que se garantiza que los montos transferidos también permanecen ocultos.

153. Tanto el Bitcoin como la mayoría de las Altcoins se mueven en el primer nivel, en el que las direcciones involucradas en las transacciones (y los montos transferidos) son públicos, pero la identidad de los/las usuarios/as que participan está protegida por el uso de pseudónimos (las claves alfanuméricas que identifican a las direcciones). Por consiguiente, si bien no es difícil seguir los flujos de valores dentro del sistema, entender como ello refleja las transferencias de valores reales entre personas resulta más complicado. Sin embargo, la aparición de herramientas tecnológicas que facilitan esto último, debilitando el anonimato ofrecido por el Bitcoin y otras criptomonedas tradicionales, ha derivado en la creación de monedas alternativas -denominadas "monedas privadas" ("privacy coins")- que incluyen rasgos tendientes a asegurar un nivel mayor de anonimato a los/las usuarios/as. Las principales de estas monedas son Dash, Zcash y Monero.

154. La característica más importante de las monedas privadas es que, aunque -al igual que Bitcoin- operan a partir de una Blockchain pública de fuente abierta, no visibilizan los mismos datos. A saber:

- Dash (DASH), lanzada en 2014, utiliza un tipo de mezclador "Coinjoin" conocido como "PrivateSend" para reducir la trazabilidad de las monedas en su Blockchain.
- Zcash (ZEC), creada en 2016, se basa en el uso de una novedosa variedad de criptografía conocida como "prueba con cero-conocimiento" ("zero-knowledge proof"), que permite a los/las usuarios/as alcanzar un consenso sobre la validez de la información (necesario para evitar el surgimiento de transacciones apócrifas) pero manteniendo, a la vez, los datos encriptados. De este modo se garantiza la legitimidad de las transferencias de la red Zcash y se resguarda, al mismo tiempo, la verdadera identidad de los/las participantes.
- Monero (XBR) lanzada también en 2014, no publica información sobre el emisor, receptor ni el valor de las transacciones en su Blockchain. En cambio, utiliza "direcciones opacas" ("stealth addresses"), creadas específicamente para ser usadas por única vez para garantizar que sólo los/las usuarios/s que intervienen en la transacción tengan acceso a los datos de la misma. También emplea una forma de criptografía conocida como "firma en círculo", que permite confirmar transacciones en el seno de un grupo de usuarios/as de modo tal que un

observador no sea capaz de identificar a la persona específica que confirmó una determinada transferencia[60].

155. Una de las principales diferencias entre Monero, Dash y Zcash es que, en estas últimas, las aplicaciones tendientes a incrementar el anonimato son optativas, mientras que en la primera se encuentra habilitada por defecto. Por consiguiente, el uso de la variante de anonimato avanzado de Dash o Zcash es minoritario[61]. Además, por ser derivaciones de la Blockchain de Bitcoin, tanto Zcash como Dash mantienen algunas vulnerabilidades (en términos de protección del anonimato) similares a las de aquella.

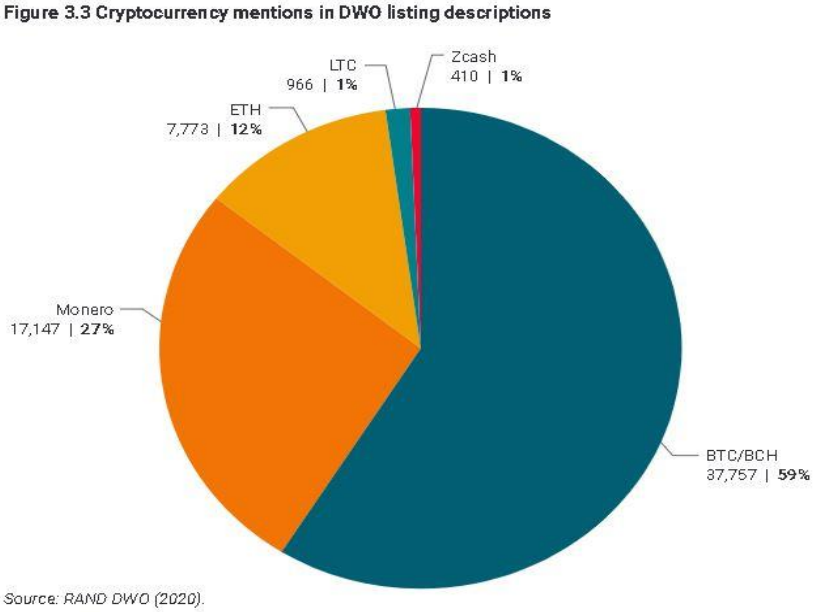
156. En comparación, las criptomonedas que utilizan el protocolo Cryptonote (como Monero) ofrecen un nivel superior de privacidad. Mediante el recurso a dicho protocolo, la trazabilidad de las transacciones se ofusca evitando identificar el verdadero saldo resultante de una transferencia (conocido como "unspent transaction output" o TXO), sustituyéndolo por un conjunto de posibles TXOs que incluye al verdadero junto con otros "de relleno", denominados "mixins".

157. En parte debido a ello, Monero se ha ido posicionando, desde su lanzamiento en 2014, como la principal alternativa al Bitcoin desde el punto de vista de la (in)trazabilidad de las transacciones. En ese aspecto, recibió un gran impulso cuando fue aceptada como moneda de pago por el (ya desaparecido) mercado de la Red oscura AlphaBay, en agosto de 2016, fecha en la que la cantidad de transacciones registradas en la Blockchain de Monero se incrementó en un 80%[62]. En la actualidad, uno de los mercados ocultos más importantes de la Red Oscura (White House Market) sólo acepta esta moneda para abonar los productos y servicios comercializados allí.

158. En la actualidad, no obstante, la presencia de "monedas privadas" en investigaciones patrimoniales sobre LA/FT es mínima, aunque su creciente aceptación por los principales PSAV y en mercados de la Red oscura parecieran indicar que su uso está llamado a incrementarse en el futuro[63]. De todas maneras, Bitcoin sigue siendo la moneda más aceptada en la mayoría de los mercados virtuales, tal como lo refleja la información proveniente del Observatorio de la Dark Web (DWO), sobre el uso de criptomonedas en los principales mercados virtuales de dicha red[64].

[60] European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses", Policy Department for Citizen's Rights and Constitutional Affairs, mayo 2018, pág. 32.
[61] Conforme datos actualizados al mes de enero, solo el 15.5 % de las transacciones con Zcash se habían realizado con la variante anónima (ver: SILFVERSTEN, Erik / FAVARO, Marina / SLAPAKOVA, Linda / ISHIKAWA, Sascha / LIU, James / SALAS, Adrian: "Exploring the use of Zcash cryptocurrency for illicit criminal purposes", RAND Europe, 2020, pág. 12).
[62] Ver: Möser, Malte / Soska, Kile / Heilman, Ethan / Lee, Kevin / Heffan, Henry / Srivastava, Shashvat / Hogan, Kile / Hennesey, Jason / Miller, Andrew / Narayanan, Arvind / Christin, Nicolas: "An empirical analysis of traceability in the Monero Blockchain", Proceedigs on Privacy Enhancing Technologies, Vol. 3, 2018, pág. 153.
[63] Ver: GAFI: "Guidance on financial investigations involving virtual assets", Junio 2019, pág. 35, § 113.
[64] Según surge del relevamiento efectuado por el DWO, las criptomonedas más usadas son Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (ETH), Litecoin (LTC), Monero (XBR o BitMonero) y Zcash (ZEC). Ver: Silfversten, Erik / Favaro, Marina / Slapakova, Linda / Ishikawa, Sascha / Liu, James / Salas, Adrian: "Exploring the use of Zcash cryptocurrency for illicit criminal purposes", RAND Europe, 2020, pág. 17.

Gráfico 3: Incidencia de las criptomonedas en los mercados de la Red oscura:



159. Conforme los datos colectados por el DWO, Bitcoin, Monero y Ethereum monopolizan los intercambios en los mercados de la Dark web (98%). Si bien Monero tiene una presencia significativa (del 27%), desplazando a Ethereum (12%), se mantiene claramente el predominio de Bitcoin en las transacciones (59%). En cambio, el uso de otras "monedas privadas" es mínimo, con Zcash registrando apenas un 1%.

160. La persistencia del Bitcoin como criptomoneda dominante en este ámbito pareciera contradecir la idea de que la actividad delictiva se volcaría masivamente hacia las "monedas privadas", a fin de explotar sus ventajas en términos de ofuscación de la información vinculada a las transacciones. Ello podría deberse a la circunstancia de que Bitcoin ha alcanzado una "masa crítica" en los mercados lícitos e ilícitos de criptomonedas, lo cual aumenta las posibilidades de que las operaciones concretadas mediante dicha moneda pasen desapercibidas dentro del volumen general de transacciones.

161. Otro factor en favor del mantenimiento del predominio del Bitcoin esta dado por la mayor facilidad para acceder a los mismos en las plataformas de intercambio de criptomonedas (incluyendo aquellas localizadas en jurisdicciones con escasos controles de ALA/CFT). En contraste, las monedas privadas siguen siendo relativamente difíciles de conseguir y

cuentan con menor liquidez, lo que puede obligar a buscarla en plataformas con mayor volumen de transacciones, en las que -a su vez- es más probable que se hayan implementado medidas de ALA/CFT. Por ende, al menos por el momento, las monedas privadas no parecen ser aptas para el lavado de fondos ilícitos a gran escala, sino que están reservadas para el uso de porción minoritaria del elemento delictivo, como moneda de intercambio para el tráfico de drogas en pequeña escala u otros delitos[65]. Aunque si puede considerárselas aptas para el financiamiento del terrorismo involucrando volúmenes reducidos de fondos.

162. Por otra parte, el anonimato que no se obtiene mediante el uso de monedas privadas puede conseguirse a través de otros métodos o herramientas, como el uso de mezcladores, plataformas o aplicaciones de intercambio descentralizadas, cambios de criptomoneda mediante el "salto de cadena" ("Chain-hopping") o los "intercambios atómicos" ("Atomic swaps"), o mediante el "dusting" (que consiste en la transferencia rastros o trazos de criptomonedas a múltiples direcciones al azar, a fin de dificultar la trazabilidad de la cadena de transacciones)[66].

163. Los mezcladores operan con las principales criptomonedas (Bitcoin, Ethereum, Litecoin) y se puede acceder a ellos tanto en la Red superficial como en la Dark web, mediante el sistema TOR. Si bien no existen límites para los montos de las transacciones con criptomonedas, si los hay al momento de transformar esos AV en moneda fiduciaria, aspecto que puede reducir la eficacia de los mezcladores para el reciclaje de volúmenes importantes de fondos de origen ilícito. Para sortear estos límites y evitar llamar la atención, los/las lavadores/as pueden optar por espaciar los pagos de salida en el tiempo y efectuarlos por montos dispares.

164. Las plataformas de intercambio descentralizadas (DEXs, por sus siglas en inglés) habilitan los intercambios directos P2P entre usuarios/as de criptomonedas. Se trata de aplicaciones que explotan innovaciones tecnológicas como las cuentas de fondos en custodia ("escrow accounts") multi-firma para permitir que los/las usuarias intercambien AV sin la necesidad de un tercero que custodie los fondos. Entre estas se encuentran IDEX, Bitsquare, OpenLedger, CryptoBridge y Bitshares.

165. Los usos posibles para los desarrollos tecnológicos basados en la encriptación, para ofrecer un grado mayor de anonimato, no se agotan en el diseño de las criptomonedas o en la implementación de mecanismos para añadir dificultades a la trazabilidad de las operaciones realizadas con las mismas. Por el contrario, la encriptación es, en la actualidad, el principal elemento para la protección de datos digitales en todo el ecosistema informático global, tanto respecto de los datos que se encuentran "en tránsito" a través de la Internet como los que se encuentran

[65] Ver: MBIYANGA, Stefan "Cryptolaundering: Anti-money laundering regulation of virtual currency exchanges", Journal of Anti-Corruption Law, Vol. 3, N° 1, 2019, pág. 7.
[66] Ver: GAFI: "12-month review of the revised FATF standards on virtual assets and virtual asset service providers", junio 2020, pág. 7.

almacenados, pasando por aquellos datos que son generados por las comunicaciones o necesarios para que aquellas se concreten.

166. En este contexto, el propio ámbito de la "Red oscura" (Dark web), en el que funcionan los mercados online en los que se desarrolla gran parte de la actividad ilícita con criptomonedas, es producto de la aparición de estas herramientas de anonimato basadas en la encriptación. En especial, del sistema TOR ("The Onion Router"). Se trata de una red distribuida de computadoras en Internet, en la que sirven como nodos todas las máquinas que operan con el software TOR (el cual puede descargarse gratuitamente), lo que le permite a todos los/las usuarios/as del sistema navegar anónimamente enmascarando su verdadera dirección IP (y, por ende, su identidad) mediante el recurso de enrutar las comunicaciones a través de circuitos al azar entre los nodos de todo el mundo. Además, el sistema cubre los paquetes de datos informáticos que constituyen la comunicación (incluyendo los que indican origen y destino) con múltiples capas de encriptación, lo cual impide su trazabilidad. Otros métodos, como las redes privadas virtuales (virtual private networks o VPNs) o la red I2P, operan con una mecánica similar.

167. El sistema TOR permite alojar páginas web en la "Red oscura" cuya verdadera dirección IP no puede ser identificada -denominadas "Servicios ocultos" ("Hidden services")-, lo cual dificulta determinar desde qué jurisdicción geográfica están operando. A los mismos fines, otras plataformas de intercambio de criptomonedas que operan en la Red superficial optan por recurrir a intermediarios para registrar sus dominios de Internet o utilizar registros DNS que suprimen u ocultan la identidad de los verdaderos titulares del dominio[67]. La mayoría de los AV de origen ilícito son reciclados a través de plataformas de intercambio o mezcladores localizados en jurisdicciones desconocidas[68].

168. Por añadidura, en los últimos diez años se ha consolidado el uso de encriptación "fuerte" (esto es: con claves criptográficas de 128 bits o superiores) para resguardar el contenido de las comunicaciones concretadas a través de Internet. La adopción masiva del recurso a estas tecnologías, a partir de su implementación por parte de las principales empresas tecnológicas globales, ha generado nuevas oportunidades para los criminales online, y -como contrapartida- nuevos desafíos para las agencias policíacas o de investigación.

169. Así, los/las administradores/as y vendedores/as en los primeros mercados ilícitos online protegían sus comunicaciones con el software de encriptación "Pretty Good Privacy" (PGP), el que luego fue adoptado también por los delincuentes u organizaciones criminales de mayor sofisticación técnica. También el sistema TOR permite encriptar los correos electrónicos. A su vez, los/las criminales también comenzaron a utilizar medios de comunicación que dificultan la

[67] Ver: GAFI: "12-month review of the revised FATF standards on virtual assets and virtual asset service providers", junio 2020, pág. 7.
[68] Ver: FANUSIE, Yaya J. / ROBINSON, Tom: "Bitcoin laundering: An analysis of illicit flows into digital currency services", Elliptic Center on Sanctions & Illicit Finance, enero 2018, pág. 8.

interceptación, como los sistemas de "Voz sobre Protocolo de Internet" (VoIP) como Skype. Posteriormente, algunas compañías han desarrollado sistemas de comunicación mediante teléfonos encriptados específicamente diseñados para evitar el monitoreo estatal, que fueron rápidamente adoptadas por las organizaciones criminales en todo el mundo. En 2020 y 2021, dos de estos sistemas (EncroChat y Sky ECC) fueron objeto de operaciones encubiertas altamente sofisticadas de las agencias policíacas de Europa. Lo mismo ocurrió, en 2021, con otro sistema similar (An0M), en este caso por parte del FBI en los EE.UU.

170. En muchas de sus variantes, la encriptación es utilizada de tal modo que el acceso al contenido de las comunicaciones no sólo se encuentra fuera del alcance técnico de las autoridades (con independencia de si cuentan, o no, con autorización judicial para obtenerlas) sino de las propias compañías que implementaron la tecnología. Tal es el caso de los sistemas de mensajería de mayor difusión a escala global (Whatsapp, Facebook Messenger, Telegram, Signal), en los que las comunicaciones en tránsito están protegidas por un sistema de encriptación "punto a punto" que genera automáticamente y por defecto una única clave al azar para cada comunicación, que solo poseen el remitente y el receptor. Ello impide que cualquier tercero ajeno a la comunicación (incluyendo a la propia compañía que desarrolló la aplicación) sea capaz de desencriptarla para acceder a su contenido.

171. Por añadidura, también han surgido aplicaciones que usan la encriptación para resguardar la información digital almacenada en equipos informáticos (ya sea que se trate de computadoras de escritorio, laptops, servidores externos o unidades de almacenamiento como pendrives o discos rígidos extraíbles). Estas aplicaciones permiten encriptar tanto archivos específicos como el disco completo con protocolos de "encriptación fuerte" prácticamente invulnerables. Teniendo en cuenta la tendencia cada vez más pronunciada a sustituir los documentos en papel por documentos digitales (incluyendo, naturalmente, a los que pueden ser útiles como evidencia en procesos por LA/FT), la aparición de tecnologías que tornan imposible el acceso a estos documentos por parte de las autoridades legalmente autorizadas para obtenerlos supone un desafío considerable.

172. La disponibilidad de herramientas de encriptación fuerte baratas o incluso gratuitas (como TrueKrypt, BitLocker o PGP) les ofrece a los delincuentes con mínimos conocimientos de informática la posibilidad de resguardar su información confidencial detrás de una barrera infranqueable. El problema que esto genera a las agencias de investigación se ha venido agravando desde 2014 en adelante, a partir de la implementación, por parte de dos de las principales compañías tecnológicas (Apple y Google) de la encriptación de disco completo de los equipos que contienen los sistemas operativos desarrollados por esas firmas, mediante claves privadas generadas a partir de la contraseña generada por cada usuario/a del dispositivo (lo cual implica que

la compañía no cuenta con dicha clave y, por consiguiente, no puede desencriptar el contenido del disco)[69].

E. Desarrollos tecnológicos que favorecen la investigación de maniobras de LA/FT con activos virtuales

173. Los delitos que, como ocurre con el LA/FT con AV, se cometen en gran medida en el ciberespacio (esto es, los denominados cibercrímenes), presentan por tal motivo características especiales que los distinguen de los delitos cometidos en el mundo físico. De ello, a su vez, se deriva que la investigación de esas conductas ilícitas requiera del empleo de estrategias, métodos, técnicas y herramientas que se adecuen al ámbito en que se desarrolla la pesquisa (el ciberespacio) y a la clase de evidencia que es preciso obtener para probar la comisión del delito y la responsabilidad de los/las acusados/as (evidencia electrónica o digital).

174. Al respecto, se ha señalado que la existencia de instrumentos procesales que amparen el uso de técnicas y herramientas de investigación aptas para la investigación de los delitos cometidos en el ciberespacio es un requisito esencial para que las AOP puedan ser efectivas en la lucha contra el cibercrimen. Por consiguiente, los países que no cuentan con legislación adecuada corren el riesgo de que sus autoridades no sean capaces de dar respuestas a los ciudadanos damnificados por los delitos informáticos[70]. En esa dirección, organismos como Interpol y Europol destacan que la adopción de nuevas tecnologías en el ámbito de las investigaciones referidas a AV resulta crucial para asistir en la efectividad de dichas pesquisas e incrementar el decomiso de fondos de origen ilícito. Por consiguiente, recomiendan la investigación y desarrollo de herramientas tecnológicas que faciliten la prevención e investigación de conductas de LA/FT con AV[71]. En el ámbito de América Latina, la OEA ha exhortado a los Estados que aún no lo han hecho a que, en el menor plazo posible, adopten o actualicen la legislación y las medidas procesales necesarias para asegurar la obtención y mantenimiento en custodia de todas las formas de evidencia electrónica y su admisibilidad en los procesos y juicios penales[72].

175. En este escenario, desde los albores del nuevo milenio han comenzado a aparecer instrumentos internacionales dedicados a la problemática del cibercrimen, empezando por el Convenio del Consejo de Europa sobre Cibercriminalidad (Convención de Budapest), que, desde su entrada en vigor, en el año 2001, se ha convertido en el instrumento multilateral sobre la materia más relevante a nivel global. Con posterioridad, a nivel regional aparecieron otros documentos

[69] Ver: International Association of Chiefs of Police (IACP): "Data, privacy and public safety. A law enforcement perspective on the challenges of gathering electronic evidence", IACP Summit Report, 2015, pág. 15.
[70] Textos Legislativos Modelo de la Comunidad del Caribe (ITU/CARICOM/CTU Model Legislative Texts), pág. 8.
[71] Ver: INTERPOL / Basel Institute on Governance / EUROPOL: "Recommendations. 4th Global Conference on Criminal Finances and Cryptocurrencies", noviembre 2020, pág. 3.
[72] Ver: Organización de los Estados Americanos (OEA): "Recomendaciones de la 9ª reunión del Grupo de Trabajo en Delito Cibernético", Reuniones de Ministros de Justicia u Otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), 12 y 13 de diciembre de 2016.

referidos a esta cuestión, entre los cuales cabe destacar a los Textos Legislativos Modelo de la Comunidad del Caribe (ITU/CARICOM/CTU Model Legislative Texts), el Proyecto de Convención de la Unión Africana (Draft African Union Convention), la Ley Modelo del Commonwealth (Commonwealth Model Law), el Proyecto de Directiva de la Comunidad Económica de los Países de África Occidental (ECOWAS Draft Directive) y la Convención de la Liga de Estados Árabes (League of Arab States Convention).

176. Aunque con matices entre sí, todos esos instrumentos multilaterales coinciden en señalar que, a los efectos de combatir más efectivamente el cibercrimen, no sólo se requiere que los países criminalicen los principales ciberdelitos, sino que también es necesario incorporar a la normativa procesal de los países signatarios disposiciones que legitimen el uso de técnicas y métodos de investigación y obtención de evidencia adecuados a la problemática del cibercrimen. Entre estas, cabe destacar a las siguientes:

- **Órdenes de presentación**: son las impartidas por un juez o autoridad competente con el fin de requerir a los proveedores de servicios de Internet u otras compañías vinculadas a las TIC la entrega de evidencia informática relevante, que obre en su poder o a la que tengan acceso conforme a la ley vigente.

- **Órdenes de preservación**: son las impartidas por una autoridad competente, a los efectos de requerir a los proveedores de servicios de Internet u otras compañías vinculadas a las TIC la preservación, por un plazo determinado de tiempo, de información o evidencia digital que corra riesgo de ser alterada o destruida, a fin de permitir que se cumplan los pasos legales necesarios para su recolección.

- **Cooperación obligatoria de proveedores de servicios de Internet u otras compañías vinculadas a las TIC**: referida a casos en los que sea necesario brindar asistencia técnica a las autoridades estatales competentes para la recolección de evidencia informática. Esta cooperación puede incluir la obligación de mantener en secreto las medidas cumplidas en tal contexto.

- **Registro de sistemas o equipos informáticos**: consistente en la posibilidad de que un magistrado disponga el registro de un sistema o dispositivo que pueda contener evidencia o información digital importante, a fin de extraerla o copiarla.

- **Acceso extendido**: consistente en la posibilidad de concretar el registro remoto de la evidencia o información electrónica contenida en otro sistema o equipo informático accesible desde el sistema informático objeto de un registro '*in situ*' y a través de este último, a fin de extraerla o copiarla. Por lo general, se requiere para considerar legítimo el acceso extendido que la autoridad estatal sepa (o tenga motivos para creer) que el segundo sistema o equipo se encuentra dentro del mismo país en que se lleva a cabo el primer registro.

- **Obtención de datos de tráfico de comunicaciones electrónicas**: consistente en la posibilidad de que un juez o autoridad competente pueda ordenar el monitoreo de las

comunicaciones electrónicas por parte de las agencias policíacas (ya sea con la cooperación de las empresas de telecomunicaciones o por medios técnicos propios), a fin de obtener datos "de envoltorio" (esto es, los que no incluyen el contenido de las comunicaciones).

- **Interceptación de datos de contenido de comunicaciones electrónicas**: consistente en la posibilidad de que un juez pueda disponer la interceptación de las comunicaciones electrónicas, ya sea con la cooperación de las empresas de telecomunicaciones o por medios técnicos propios.

- **Cooperación internacional**: se menciona la necesidad de establecer disposiciones que permitan a los países colaborar entre sí para la obtención de evidencia digital a través de órdenes de presentación o preservación. Se pone de resalto, asimismo, la importancia de implementar mecanismos para agilizar el intercambio de información, adecuándolo a las características de la evidencia digital.

177. En este escenario, es importante tener presente que la evolución tecnológica no sólo favorece a los/las criminales que pretenden explotar sus desarrollos para facilitar la comisión de ilícitos o entorpecer su investigación, sino que también puede ofrecer ventajas y herramientas novedosas a las AOP, a las que les brinda la posibilidad de recurrir a técnicas de investigación vinculadas a las nuevas tecnologías para perseguir (por ejemplo) posibles maniobras de LA/FT con AV.

178. Así, en cuanto atañe a la materia objeto de estudio en esta guía, se ha señalado que el uso de criptomonedas no sólo facilita el intercambio ilícito en la Internet, sino también su detección, debido al carácter público de las respectivas blockchains. En efecto, aunque el Bitcoin y otras monedas similares son utilizadas habitualmente para perpetrar delitos, algunos autores entienden que -de hecho- su empleo favorece la investigación de los flujos de fondos ilícitos[73].

179. En realidad, tanto Bitcoin como la mayoría de las Altcoins no ofrecen verdadero anonimato, sino un "pseudo anonimato". Ello así, desde que, si bien la identidad de los/las usuarios/as esta resguardada bajo un pseudónimo en la forma de la secuencia alfanumérica que constituye su dirección, los datos referidos a las transacciones que realizan (fechas, montos, saldo y direcciones de las contrapartes) se consignan en un registro público (la correspondiente Blockchain). Ello es inherente a la tecnología de "libro mayor distribuido" ("Distributed ledger technology" o DLT), en la que se apoya el funcionamiento de las criptomonedas[74], en virtud de la cual la legitimidad de las transacciones -en ausencia de una autoridad central que las convalide- está dada por el registro criptográfico de las mismas en bloques que conforman una cadena (la "Blockchain"). Esta, a su vez, conforma un registro secuencial inalterable de todas las operaciones realizadas con la criptomoneda que se trate.

[73] Ver, en tal sentido, Foley, Sean / Karlsen, Jonathan R. / Putnins, Talis J. "Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?", The Review of Financial Studies, Vol. 32, N° 5, 2019, págs. 1798/1853.
[74] Para una explicación detallada sobre esta tecnología, ver: European Union Agency for Cibersecurity (ENISA): "Crypto assets. An introduction to digital currencies and distributed ledger technologies", febrero 2021.

180. En este escenario, el carácter público de la Blockchain permite que la información contenida en la misma sea minada durante años en busca de indicios que permitan determinar la identidad de los/las usuarios/as. Ello ha dado origen al denominado "Chain analysis" (análisis de la cadena, en referencia a la Blockchain), término que engloba a una serie de técnicas basadas en el uso de herramientas informáticas para revertir el anonimato de los/las usuarios de criptomonedas. El origen de estas técnicas -desarrolladas por empresas privadas dedicadas a asistir a agencias de investigación y otros entes privados en la identificación de actores en la Blockchain- se remonta a estudios académicos realizados a partir de 2011, que demostraron los límites del pseudo anonimato ofrecido por Bitcoin y otras criptomonedas[75].

181. Uno de los principales métodos de desanonimización consiste en determinar la identidad de los/las titulares de ciertas direcciones mediante el uso de herramientas estadísticas que, a partir del análisis de información contenida en la Blockchain, los/las vincula con direcciones conocidas (por ejemplo, de plataformas de intercambio de criptomonedas, de mercados online o de personas ya identificadas) o con pseudónimos publicados online. Esto es: se explotan los datos generados por las redes de intercambio entre los/las usuarios/as con vínculos comprobados con actividades ilícitas para reconstruir la cadena completa de transferencias entre estos y sus clientes o contactos. A fin de identificar direcciones de AV relevantes dentro del ecosistema de criptomonedas, los/las investigadores/as también pueden efectuar pagos con AV propios a distintos servicios (plataformas de intercambio, páginas de apuestas, monederos online, etc.), o llevar a cabo búsquedas en la Internet en procura de direcciones de AV publicadas.

182. Las herramientas de Chain analysis también sacan provecho de las vulnerabilidades intrínsecas en la red Blockchain (como el filtrado de direcciones IP y de estampillas temporales asociadas con cada transacción publicada) para desanonimizar a los/las usuarios/as. Y ello, con independencia de la aplicación Blockchain específica que estén empleando, e incluso cuando recurren a herramientas de anonimato como TOR. En esta dirección, trabajos académicos señalan que se puede sacar provecho de una contramedida incorporada en el sistema Bitcoin para repeler

[75] Ver: ALSALAMI, Nasser / ZHANG, Bingsheng: "SoK: A systematic study of anonymity in cryptocurrencies", IEEE Conference on Dependable and Secure Computing (DSC), noviembre 2019; BIRYUKOV, Alex / KHOVRATOVICH, Dimitry / PUSTOGAROV, Ivan: "Deanonymisation of clients in Bitcoin P2P network", AAVV, *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Scottdale, 2014, págs. 15/29; Biryukov, Alex / Feher, Daniel: "Deanonimization of hidden transactions in Zcash", University of Luxembourg, 2018; HERRERA-JOANCOMARTÍ, Jordi: "Research and challenges on Bitcoin anonymity", *Data privacy management, autonomous spontaneous security, and security assurance*, Revised Selected Papers from 9th International Workshop, DPM 2014, 7th International Workshop, SETOP 2014, and 3rd International Workshop, QASA 2014, Wroclaw, 2014, págs. 3/16; KAPPOS, George / HAAROON YOUSAF, Mary Maller / MEIKLEJOHN, Sarah: "An empirical analysis of anonymity in Zcash", Proceedings of the 27th USENIX Security Symposium, Baltimore, 2018; KOSHY, Phillip / KOSHY, Diana / MCDANIEL, Patrick: "An analysis of anonymity in Bitcoin using P2P network traffic", 18th International Conference on Financial Cryptography and Data Security, 2014; MAURER, Felix Konstantin: "A survey on approaches to anonymity in Bitcoin and other cryptocurrencies", *Informatik 2016. Lecture notes in informatics*. Bonn, 2016, págs. 2145/2150; Meiklejohn, Sarah / Pomarole, Marjori / Jordan, Grant / Levchenko, Kirill / McCoy, Damon / Voelker, Geoffrey M. / Savage, Stefan, "A fistful of bitcoins: Characterizing payments among men with no names", *Proceedings of the 2013 Conference on Internet Measurement Conference (IMC '13)*, ACM, New York, 2013, ps. 127/140; y MÖSER, Malte / SOSKA, Kile / HEILMAN, Ethan / LEE, Kevin / HEFFAN, Henry / SRIVASTAVA, Shashvat / HOGAN, Kile / HENNESEY, Jason / MILLER, Andrew / NARAYANAN, Arvind / CHRISTIN, Nicolas: "An empirical analysis of traceability in the Monero Blockchain", Proceedigs on Privacy Enhancing Technologies, Vol. 3, 2018, págs. 143-163.

ataques DDoS, de modo tal de evitar que los usuarios se oculten mediante el uso del TOR[76]. También puede recurrirse al método conocido como "dusting attack", que consiste en enviar rastros o trazas de criptomonedas (conocidos como "dust") a miles (o cientos de miles) de monederos para luego analizar sus movimientos posteriores en busca de indicios sobre la identidad de sus titulares.

183. Cuando se concretan grandes transacciones con AV, el rastreo de los movimientos de los involucrados por medio de métodos de Chain analysis se facilita, lo cual importa que el ecosistema de Bitcoin y las principales criptomonedas no ofrece un alto grado de anonimato para operaciones importantes de lavado de activos. La rastreabilidad de las transacciones es aún mayor si se cuenta con acceso a un servicio central, como un PSAV.

184. La creciente trasparencia de la Blockchain de Bitcoin y las principales Altcoins ha derivado en el surgimiento de las denominadas "monedas privadas", como Monero o Zcash. Sin embargo, estudios académicos han demostrado que también los/las usuarios/as de monedas privadas pueden ser desanonimizados/as con un grado de precisión mayor al esperado[77], explotando características específicas del funcionamiento de dichos AV.

185. En el caso de Monero, se saca provecho del modo en que se crean las "monedas de relleno" (denominadas "Mixins") que se utilizan para ofuscar la identificación de las que realmente se intercambian. En lo tocante a Zcash, un análisis sobre el funcionamiento de esta criptomoneda determinó que sólo el 3,5% de las operaciones concretadas con la misma involucran la variante de anonimato incrementado que ofrece el sistema, y de esas, hasta un 31,5% de los movimientos pueden ser reconstruidos mediante herramientas analíticas avanzadas. Lo que significa que, en la práctica, el 98% de las transacciones con Zcash están sujetas a trazabilidad[78].

186. La disponibilidad de herramientas informáticas diseñadas para explotar las características de las criptomonedas para permitir la desanonimización de sus usuarios/as no es, sin embargo, el único producto de la evolución tecnológica de las últimas dos décadas que favorece la vigilancia estatal. Por el contrario, también puede explotarse a tal fin el vuelco de las sociedades modernas hacia el uso masivo, generalizado y constante de TICs informáticas para la concreción de prácticamente todas las actividades humanas (ya sean institucionales, comerciales, informativas, educativas, académicas, recreativas, y, por supuesto, también las delictivas), cuya principal consecuencia es la generación de una ingente cantidad de datos vinculados a esas actividades, que pueden ser "minados" por las AOP con fines investigativos. El aprovechamiento de este cúmulo de

[76] Ver: BIRYUKOV, Alex / KHOVRATOVICH, Dimitry / PUSTOGAROV, Ivan, "Deanonymisation of clients in Bitcoin P2P network" en AA.VV., CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottdale, 2014, ps. 15/29.
[77] Ver: European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses", Policy Department for Citizen's Rights and Constitutional Affairs, mayo 2018, págs 34/35.
[78] Ver: DUPUIS, Daniel / GLEASON, Kimberley: "Money laundering with cryptocurrency: Open doors and the regulatory dialectic", Journal of Financial Crime, Agosto 2020.

datos se ve favorecido por el hecho de que los mismos, por ser digitales, son generados, almacenados, entrecruzados y almacenados mucho más fácilmente. Sobre todo, a partir del surgimiento de las herramientas que configuran el fenómeno conocido como "Big data", específicamente diseñadas para permitir el análisis de enormes volúmenes de información.

187. Otro rasgo fundamental de la nueva realidad tecnológica que puede ser aprovechado a los efectos de la "vigilancia informática" estatal es que el modelo de negocios imperante en las principales compañías tecnológicas -sobre todo en derredor de la Internet- se funda en la explotación de los datos generados por los/las usuarios/as. Por consiguiente, en la práctica las propias compañías han generado, por motivos comerciales, una verdadera "superestructura de vigilancia" de proporciones nunca vistas, a cuyos resultados pueden acceder las agencias estatales requiriendo la cooperación de los privados, conforme recomiendan los instrumentos internacionales reseñados precedentemente.

188. En tal contexto, las AOP están en condiciones de acceder a tres grandes categorías de información sobre los/las ciudadanos/as. A saber:

a. Información sobre comunicaciones y movimientos recolectada por las empresas de telecomunicaciones (que incluyen tanto los generados constantemente, como producto de la comunicación entre los smartphones y las torres de telefonía celular, como la generada por los dispositivos GPS insertos en la mayoría de esos dispositivos y recolectada por aplicaciones a las que se habilita a "conocer la localización" de los/las usuarios/as);

b. Datos almacenados y procesados por las compañías de Internet (comprendiendo a la que se deriva de los historiales de búsqueda en los buscadores de Internet, los datos y metadatos generados por la interacción en redes sociales, los datos sobre compras o navegación en los mercados online y la información sobre navegación en la Red colectada por las "cookies" en las páginas web); y

c. La información generada por los dispositivos comprendidos en la denominada "Internet de las cosas" (IoT, por sus siglas en inglés).

189. Por añadidura, el avenimiento de la era digital ha redundado en un notorio incremento de la capacidad de las técnicas tradicionales de vigilancia estatal, como resultado de la disponibilidad de herramientas tecnológicas como las cámaras digitales (incluyendo las instaladas en sistemas de circuito cerrado en la vía pública, las infrarrojas o las colocadas en aeronaves no tripuladas -"drones"-, los dispositivos GPS, los micrófonos espías digitales, los equipos simuladores de celdas de telefonía celular, y las tecnologías para interceptación y análisis de tráfico de Internet, entre otras).

190. La principal consecuencia de estos avances tecnológicos es que la eficacia de la vigilancia realizada por el Estado ya no se vea limitada por su magnitud o duración, ya que la disminución de los costos de tecnología y de almacenamiento de datos ha eliminado muchos de los inconvenientes

financieros o prácticos que tradicionalmente entrañaba su realización. Por consiguiente, los estados cuentan, como nunca, con la capacidad potencial de llevar adelante actividades de vigilancia simultáneas, invasivas, con objetivos precisos y a gran escala[79].

191. Por último, han surgido otras dos herramientas especialmente concebidas para responder a las defensas anti-forenses empleadas por los modernos delincuentes cibernéticos (incluyendo a los que se dedican al criptolavado) sacando provecho, a tal efecto, de los mismos rasgos de la Internet y de los sistemas informáticos que aquellos explotan para desarrollar su actividad ilícita. Así, la posibilidad de navegar anónimamente en la Red permite la actuación de los "agentes encubiertos digitales"; mientras que la existencia de vulnerabilidades en los programas informáticos abre la puerta al hackeo estatal.

192. El uso de agentes encubiertos digitales consiste, básicamente, en sacar ventaja de las herramientas de anonimato como el TOR y del empleo generalizado de pseudónimos en la Internet (y sobre todo en la Red oscura) para que personal de las agencias de investigación (designado y autorizado conforme la legislación de cada Estado) pueda interactuar online con potenciales delincuentes, infiltrarse en organizaciones y obtener evidencia que pueda ser utilizada para lograr una condena.

193. El hackeo estatal supone adaptar los programas "troyanos" o espías ("spyware") que emplean los cibercriminales de modo tal que puedan ser utilizados para obtener información o evidencia informática en forma remota (esto es: sin tomar contacto físico con el dispositivo que almacena o genera los datos). Ello conlleva dos grandes ventajas para los investigadores: a) que, a diferencia del registro físico, la recolección remota de evidencia puede realizarse en forma subrepticia, sin anoticiar a la persona objeto de investigación sobre la existencia de dicha investigación; y b) que puede concretarse incluso si se desconoce dónde se encuentra la persona investigada y/o la localización del dispositivo en el que se introduce el programa espía.

194. Además, el recurso a un spyware estatal admite múltiples usos. No sólo se lo puede emplear para acceder remotamente a datos almacenados, sino también para obtener claves de acceso a documentos encriptados o que se encuentran en servidores externos, para monitorear comunicaciones realizadas a través de la Internet, para realizar vigilancias acústicas o audiovisuales, para localizar e individualizar a las personas que se contactan con determinadas páginas (o individuos) a través de la red, o para rastrear en tiempo real a sujetos sometidos a investigación.

[79] Ver: Organización de las Naciones Unidas (ONU): "El derecho a la privacidad en la era digital", Declaración A/HRC/27/37, informe de la Oficina del Alto Comisionado por los Derechos Humanos de las Naciones Unidas, junio 2014, pág. 3, § 2.

195. Los primeros antecedentes de uso de spyware por agencias de investigación estatales datan de hace más de dos décadas[80]. Esta herramienta comenzó a utilizarse en los EE.UU. y fue luego adoptada también en otros países, como Italia, Francia, Alemania, el Reino Unido, Australia e Israel[81]. En algunos países (España, Francia, Inglaterra, Países Bajos, Polonia), el recurso estatal a software espía se encuentra expresamente regulado en la normativa procesal local, mientras que en otros (EE.UU., Australia, Alemania, Italia) su utilización se rige por la aplicación analógica de normas procesales referidas a las medidas de investigación tradicionales[82].

196. A su vez, dos de los instrumentos internacionales sobre cibercrimen mencionados precedentemente aluden directa o indirectamente a la posibilidad de recurrir al uso de spyware para concretar la obtención de datos de contenido de comunicaciones. Así, la Ley Modelo del Commonwealth (art. 18.b) menciona la posibilidad de que las agencias policíacas obtengan los datos de contenido mediante "la aplicación de medios técnicos"; mientras que los Textos Legislativos Modelo de la Comunidad del Caribe (art. 27.1.) hacen referencia al posible uso de "software forense" con fines investigativos.

197. A partir de la difusión del uso estatal de spyware, la circunstancia de que pueda ser utilizado de un modo más invasivo que las medidas tradicionales -en la medida en que es posible obtener, por ese medio, la totalidad de la información contenida en un smartphone (más allá de que, conforme la legislación vigente en cada país, sea en general la autoridad judicial aplicable la que decida el alcance con el que va a ser empleada esta herramienta)- ha derivado en que organismos internacionales como la Organización de las Naciones Unidas expresaran su preocupación por el posible impacto para el derecho a la privacidad derivado de las prácticas que aprovechan la vulnerabilidad de las tecnologías digitales de la comunicación para la vigilancia electrónica[83].

198. No obstante ello, la propia ONU ha reconocido también que puesto que las tecnologías de comunicación digital pueden ser, y han sido, utilizadas por particulares con fines delictivos (como el reclutamiento para la comisión de atentados terroristas y el financiamiento de los mismos), la vigilancia legal y específica de las comunicaciones digitales puede constituir una medida necesaria y eficaz para las agencias de aplicación de la ley cuando se la lleva a cabo en cumplimiento de la

[80] Ver: CARRELL, Nathan E.: "Spying on the mob: United States v. Scarfo – A constitutional analysis", Journal of Law, Technology & Policy", Vol. 2002, N° 1, 2002, págs. 193/214.
[81] Ver: United against crime: Improving criminal justice in European Union cyberspace, Instituti Affari Internazionali, 2016 y European Parliament: "Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices", Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, 2017.
[82] Ver: European Parliament: "Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices", Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, 2017.
[83] Ver: Organización de las Naciones Unidas (ONU): "El derecho a la privacidad en la era digital", Declaración A/HRC/27/37, informe de la Oficina del Alto Comisionado por los Derechos Humanos de las Naciones Unidas, junio 2014, pág. 3, § 3. La ONU emitió declaraciones vinculadas al "derecho a la privacidad en la era digital" en 2013, 2014 y 2016. Ver: ONU: "El derecho a la privacidad en la era digital", Declaración 68/167, 18 de diciembre de 2013; "El derecho a la privacidad en la era digital", Declaración 69/166, 18 de diciembre de 2014; y "El derecho a la privacidad en la era digital", Declaración A/C.3/71/L.39/Rev.1, 19 de diciembre de 2016.

legislación internacional y nacional[84]. En igual sentido se expidieron, en el ámbito europeo, ENISA y Europol[85].

199. En tal contexto, se considera por lo general preferible que el recurso a nuevas formas de vigilancia electrónica como el spyware estatal estén expresamente reguladas, en tanto se entiende que la aplicación analógica de normas ya existentes puede no ser apta para compensar el carácter invasivo de dicha herramienta de investigación[86]. Sin perjuicio de ello, en ausencia de regulación normativa expresa, allí donde la legislación vigente autorice la aplicación analógica, es posible reducir los riesgos con respecto al derecho a la privacidad y garantizar la proporcionalidad entre la restricción a ese derecho y los fines estatales adoptando, al momento de ordenar una medida de este tipo, los requisitos previos y posteriores establecidos en las normas de los países que si han legislado sobre la materia.

200. Dichos requisitos comprenden la exigencia de autorización judicial, la restricción del uso del hackeo estatal a la investigación de delitos graves, el establecimiento de límites en el modo de uso, la exigencia de autorizaciones separadas para cada función del spyware estatal, el control sobre el funcionamiento de las herramientas informáticas utilizadas y la destrucción de la información irrelevante. A su vez, resulta recomendable establecer la obligación de remover el software después de su uso, la notificación a los interesados y la implementación de mecanismos de supervisión del empleo de spyware, entre otros.

F. Situación regional en orden a la incorporación de nuevos métodos de investigación tecnológica

201. La relación entre las nuevas tecnologías y la investigación del cibercrimen fue objeto de un relevamiento efectuado a nivel global por la UNODC en 2013[87], en el cual quedaron en evidencia los problemas y desafíos generados por el surgimiento de herramientas tecnológicas con capacidad antiforense. Estas mismas cuestiones fueron señaladas posteriormente por otros organismos vinculados a las agencias policíacas, como la Asociación Internacional de Jefes de Policía (IACP, por sus siglas en inglés)[88]. En sentido opuesto, el Parlamento Europeo llevó a cabo otro relevamiento, en este caso referido al uso estatal de spyware como recurso para contrarrestar los

[84] Ver: Organización de las Naciones Unidas (ONU): "El derecho a la privacidad en la era digital", Declaración A/HRC/27/37, informe de la Oficina del Alto Comisionado por los Derechos Humanos de las Naciones Unidas, junio 2014, pág. 9, § 24.
[85] Ver: European Union Agency for Cibersecurity (ENISA) y Europol: "On lawful criminal investigation that respects 21st century data protection. Europol and ENISA joint statement", declaración del 20 de mayo de 2016.
[86] Ver: European Parliament: "Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices", Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, 2017, págs. 12/13. En igual sentido: ONU: "El derecho a la privacidad en la era digital", Declaración A/HRC/27/37, informe de la Oficina del Alto Comisionado por los Derechos Humanos de las Naciones Unidas, junio 2014, págs. 10/11, § 28; y ENISA/EUROPOL: "On lawful criminal investigation that respects 21st century data protection. Europol and ENISA joint statement", declaración del 20 de mayo de 2016, pág. 1.
[87] Ver: United Nations Office on Drugs and Crime (UNODC), *Comprehensive study on cybercrime*, 2013.
[88] Ver: International Association of Chiefs of Police (IACP): "Data, privacy and public safety. A law enforcement perspective on the challenges of gathering electronic evidence", IACP Summit Report, 2015.

problemas antes apuntados[89], del que se desprendió la creciente adopción de dicha herramienta por EE.UU., varios países de Europa, Israel y Australia.

202. En el cuestionario enviado a los efectos de la elaboración de la presente guía, se consultó a los puntos de enlace de la RRAG obre si la legislación procesal en sus respectivos países contenía normas referidas tanto al uso de herramientas informáticas (software) para el acceso remoto a sistemas informáticos y/o el monitoreo de comunicaciones como a la investigación mediante técnicas de inteligencia de fuentes abiertas (OSINT). También si, en caso negativo, la normativa procesal existente puede ser utilizada analógicamente a fin de amparar el uso de técnicas de investigación no reguladas expresamente.

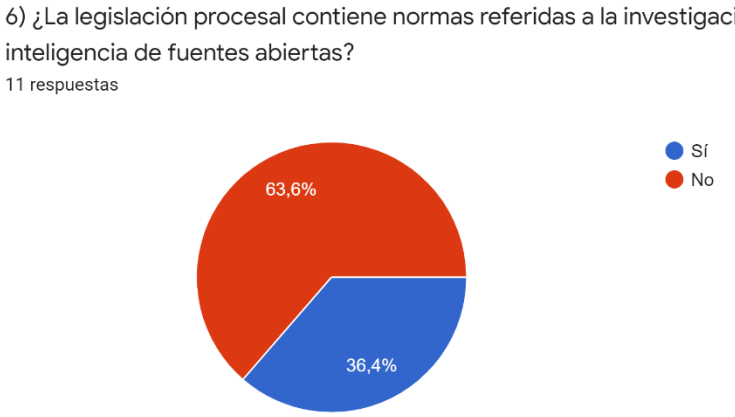
203. Con respecto a si la legislación procesal ampara el uso de spyware, una amplia mayoría de los países que respondieron (7 de 11, 63,6 %), lo hizo afirmativamente. Se aprecia, no obstante ello, que de las respuestas no surge que las normas citadas aludan en forma expresa a la utilización de herramientas informáticas (como ocurre, por ejemplo, con la legislación de España, Francia, Inglaterra o los Países Bajos), sino que se interpreta que dicha utilización se encuentra comprendida en el alcance de las normas que rigen, en forma genérica, la interceptación de comunicaciones electrónicas y otras medidas en las que puede emplearse el spyware, sea estableciendo que dicha medida puede cumplirse mediante "cualquier medio técnico" o sin decir nada al respecto. Es decir, dejando en manos de la autoridad encargada de llevar a cabo la medida la elección de los recursos técnicos que corresponde emplear a tal efecto.

Gráfico 4: Regulación del uso de spyware como herramienta de investigación:

204. La situación es distinta en lo referido a las técnicas de OSINT, dado que en este supuesto la mayoría de los países que respondieron (7 de 11, 63,6 %) contestó que no se encuentra regulado el uso de dichas técnicas.

[89] Ver: European Parliament: "Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices", Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, 2017.

Gráfico 5: Regulación del uso de técnicas de OSINT:



205. De cualquier modo, la circunstancia de que la información que se obtiene a través de las técnicas de OSINT sea -como su propio nombre indica- de "fuente abierta", determina que la falta de regulación expresa no constituye un obstáculo para el uso de ese método investigativo.

206. Por otra parte, de las respuestas al cuestionario se desprende que una amplia mayoría de los países que contestaron (7 de 11, 63,6 %) señalaron que el ordenamiento procesal local permite aplicar analógicamente ambas técnicas de investigación (spyware y OSINT). De los 4 restantes, uno no descartó que dicho uso analógico sea factible, sino que consignó que no podía aportar una definición al respecto por entender que ello queda librado a la interpretación judicial. Mientras que, en dos de los otros 3 casos, la respuesta negativa obedeció a que la aplicación analógica no resultaba necesaria ante la existencia de normativa procesal que, a juicio de la autoridad informante, ampara la utilización de las medidas de investigación en trato.

207. Evaluadas en su conjunto, las respuestas al cuestionario permiten inferir que existe en la región un escenario favorable, en principio, para la implementación de nuevas técnicas de investigación informáticas en el marco de investigaciones patrimoniales referidas a ciberdelitos en general, y a maniobras de LA/FT con AV en particular.

G. Tratamiento de la evidencia digital

208. Un elemento común a la investigación de maniobras de LA/FT con AV y a las herramientas tecnológicas que pueden utilizarse para llevar adelante esa clase de investigaciones (e incluso para procurar el decomiso de dichos activos), es que en ambos supuestos se está tratando con información digital, generada por las TICs.

209. Las TICs son, de hecho, el elemento central que posibilita el uso de AV, ya con estos se opera en el ámbito virtual y todas las operaciones vinculadas a los mismos involucran, en un

momento u otro, el recurso a sistemas y datos informáticos. Los únicos rastros "de papel", si es que existen, podrían encontrarse en los registros generados por los PSAV cuando los AV son intercambiados por moneda fiduciaria o viceversa. Por ende, la mayor parte de la evidencia que eventualmente vaya a incorporarse a los procesos judiciales para probar la operatoria ilícita con AV -y de seguro la más importante- va a encontrarse casi exclusivamente en formato electrónico o digital[90].

210. En esa dirección, la UNODC señala una serie de rasgos relevantes de la evidencia electrónica o digital, que deben tenerse en cuenta a los efectos de su búsqueda, obtención, mantenimiento y análisis y que revisten enorme importancia en el contexto de las investigaciones sobre LA/FT mediante AV[91]. A saber:

- **Difícil trazabilidad**: derivada de la circunstancia de que se la encuentra en sitios en las que sólo pueden ser detectadas por especialistas, y por medio del uso de herramientas específicas, que permiten no sólo identificar la información verdaderamente relevante -distinguiéndola de la que no lo es- sino inferirla a partir del entrecruzamiento de datos aparentemente inocuos.

- **Necesidad de la intervención de especialistas**, toda vez que, sin su participación, la información localizada en los sistemas informáticos no puede ser extraída de forma tal que se garantice que la misma es confiable y no ha sido manipulada o alterada en modo alguno. La intervención de especialistas también es necesaria para identificar y procesar información vinculada, que pueda resultar relevante para la investigación. Si ésta tiene relación, además, con maniobras de LA/FT, la especialización de los expertos que participen deberá incluir también conocimientos sobre finanzas, metodologías de lavado de activos y otras cuestiones de ese tenor.

- **Alta volatilidad**, desde que los sistemas informáticos que crean procesan y almacenan la evidencia digital destruyen, como parte de su funcionamiento de rutina, algunos de los datos existentes cada vez que ocurren determinados eventos, como por ejemplo actualizaciones automatizadas que sobrescriben información antigua a fin de liberar especio para nueva información.

- **Susceptibilidad a la alteración**. Los sistemas o equipos informáticos constantemente modifican el estado de sus memorias, ya sea a pedido del/la usuario/a (cuando guarda, copia o actualiza operaciones) o en forma automática (adjudicación de espacio en la memoria, almacenamiento temporal, actualizaciones preprogramadas, etc.). Este rasgo es

[90] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, pág. 60.
[91] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, págs. 61/62.

relevante para entender las limitaciones temporales inherentes a la evidencia informática y estar en condiciones de manipular dicha evidencia en forma apropiada desde el momento mismo en que se la identifica como relevante para una investigación.

- **Capacidad para copiarse ilimitadamente**. La información digital puede ser copiada indefinidamente sin que se pierda fiabilidad. Esto es: de modo tal que cada copia sea idéntica al original. Si bien esto puede resultar problemático para la diferenciación entre el original y la copia, una vez que se establece que las copias son, de hecho, idénticas al original se convierte en una ventaja, en la medida en que permite la distribución de copias exactas de la evidencia relevante para ser analizadas simultáneamente por distintos expertos.

211. De todo ello se sigue que el tratamiento de evidencia digital requiere de mayores recursos (en términos de tecnología y de recursos humanos especializados) que la evidencia física, toda vez que la intervención de agentes no capacitados en operativos en los que pueda encontrarse esta clase de prueba no sólo puede redundar en que se pase por alto evidencia relevante, sino también que ésta pueda ser accidentalmente alterada o destruida. Asimismo, para que resulte realmente eficaz en un proceso judicial, es preciso que sea obtenida, resguardada y analizada de forma tal que se garantice su autenticidad, su completitud, su confiabilidad y su verosimilitud.

212. La capacidad para garantizar que dichos estándares se cumplan es un requisito esencial en relación con las herramientas informáticas que se utilicen para obtener la evidencia electrónica, como por ejemplo un software espía estatal. Ello así, desde que -en atención al carácter novedoso de estos métodos- la cuestión de la confiabilidad de la información recuperada deviene crucial para que los operadores del sistema judicial se convenzan de que constituyen un medio legítimo para incorporar evidencia a un proceso penal. Por consiguiente, las herramientas tecnológicas que se empleen deben asegurar que sea posible captar la evidencia buscada cumpliendo con las pautas antes mencionadas.

213. Por otra parte, el rol preponderante que pasa a adquirir la evidencia electrónica -y, potencialmente, también el empleo de herramientas tecnológicas novedosas- en las investigaciones sobre ciberdelitos en general y maniobras de LA/FT con criptomonedas en particular exige la adquisición de conocimientos nuevos a todos los intervinientes. Esto incluye tanto a los/las integrantes de las agencias policíacas o dependencias del Ministerio Público Fiscal que encabecen las pesquisas, como a los magistrados que deban autorizar la adopción de medidas o el uso de técnicas que involucren TICs (incluyendo desde el análisis de la Blockchain al recurso a spyware, pasando por la utilización de técnicas modernas de vigilancia) o sopesar la evidencia resultante. La realidad marca, sin embargo, que existe un déficit importante en cuanto a la capacitación de los actores relevantes en todo lo concerniente al vínculo entre las TICs y las investigaciones penales, lo cual supone un riesgo concreto para la eficacia en la persecución de maniobras de LA/FT con criptomonedas y la incautación y decomiso de AV.

214. En atención a ello, y a efectos de brindarle a las autoridades competentes en general y las agencias policíacas en particular instrumentos útiles para cumplir eficazmente con sus funciones en lo tocante a la recolección, custodia, tratamiento y análisis de la evidencia electrónica, en el mundo han ido surgiendo una serie de protocolos conteniendo estándares o buenas prácticas sobre la materia, elaborados por organismos o agencias especializadas en el cumplimiento de la ley o en el uso de nuevas tecnologías.

215. Entre estos, cabe incluir los siguientes: "First Responders Guide Template" de la IOCE; RFC 3227 de la Internet Engineering Task Force – Internet Society (IETF-ISOC); "Electronic Crime Scene Investigation, a Guide for First Responders" del Technical Working Group on Digital Evidencie (TWGDE); "Electronic Crime Scene Investigation, a Guide for First Responders", "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" e "Investigation Involving the Internet and Computer Networks", todos del National Institute of Justice (NIJ) del Departamento de Justicia de los EE.UU. (DOJ); "APCO Good Practice Guide for Digital Evidence" del Association of Chief Police Officers (APCO); "Identification and Handling of Electronic Evidence" de European Union Agency for Cibersecurity (ENISA); e ISO/IEC 27037:2012 "Information Technology -Security Techniques- Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence".

216. En tal contexto, en el cuestionario dirigido a los puntos de enlace de la RRAG a los efectos de la elaboración de la presente guía, se consultó a los países, en primer lugar, sobre la aplicación de protocolos que regulen el tratamiento de la evidencia informática. De los países que respondieron al cuestionario, una amplia mayoría (13 de 16, 81 %) respondieron que cuentan con protocolos propios que regulan la actuación de las fuerzas de seguridad en la recolección de evidencia informática y/o el secuestro de dispositivos informáticos.

217. Cabe mencionar, no obstante ello, que de los tres países que respondieron negativamente, uno (Colombia) refirió que a pesar de no contar con protocolos que regulasen la actividad de las fuerzas de seguridad en la recolección de evidencia digital, la normativa local si contiene protocolos sobre la materia, aunque dirigidos a la Fiscalía General de la Nación.

218. De lo expuesto se desprende que existe, en general, un grado alto de conciencia en la región sobre la necesidad de contar con protocolos que regulen la recolección de evidencia. Siendo que, incluso en los casos en los que no se han elaborado guías de buenas prácticas a nivel interno sobre la materia, pueden tomarse como referencia, en lo pertinente, los reseñados precedentemente.

219. Por otro lado, en lo tocante a la existencia de unidades especializadas en investigación de ciberdelitos o en ciberseguridad existe también una mayoría sustancial de respuestas positivas, si bien no tan amplia como la referida a los protocolos (11 de 16, 69%).
220. Asimismo, de los 7 países que respondieron afirmativamente, 4 señalaron contar con unidades del Ministerio Público Fiscal especializadas, con un quinto consignando que se encuentra en proyecto la creación de una unidad fiscal de esa clase.

H. Problemática de la incautación de AV

221. Debido a las particulares características de los AV, su incautación o decomiso puede ser considerablemente más difícil que la de bienes tangibles como la moneda fiduciaria. Sin embargo, la experiencia recogida desde la aparición del Bitcoin hasta la fecha demuestra que puede lograrse. Esto quedó demostrado a partir del cierre de Silk Road, el primer mercado ilícito online en operar con AV como medio de pago, oportunidad en la que una extensa investigación patrimonial del FBI culminó con el arresto del creador de dicho mercado y el decomiso de bitcoins valuados (en esas fechas) en entre 3.5 y 4 millones de dólares.

222. En los años siguientes, se produjeron otros decomisos de criptomonedas (sobre todo bitcoins, aunque no exclusivamente) valuadas en millones de dólares en Europa, Australia, Japón y China. Las más recientes fueron la incautación de AV sustraídos por un hacker de las cuentas de Silk Road y el decomiso de criptomonedas provenientes de la estafa piramidal "PlusToken" por las autoridades chinas, por un valor total de aproximadamente 4.000 millones de dólares. También se produjeron incautaciones vinculadas al financiamiento del terrorismo, como la captura de alrededor de 2 millones de AV pertenecientes a grupos terroristas (incluyendo Al-Qaeda, ISIS y Hamas) en agosto de 2020[92]. Incluso se lograron decomisar "monedas privadas". En un caso, se incautaron aproximadamente 3,691 Zcash que estaban en manos del administrador del ya desaparecido mercado ilícito online AlphaBay (uno de los sucesores de Silk Road), que había sido arrestado en 2017[93].

223. Asimismo, de las respuestas recibidas al cuestionario enviado durante la elaboración de la presente guía se desprende que los países europeos que forman parte de la RRAG en carácter de observadores reportaron casos en los que se consiguió "bloquear" los AV de un sospechoso en una plataforma de intercambio de criptomonedas (España), secuestrar monederos de AV (Andorra) y transferir AV pertenecientes a sospechosos a monederos controlados por las autoridades estatales (Francia).

224. De igual manera, a nivel regional se advierte un escenario favorable, desde el punto de vista normativo, para la implementación de medidas de incautación y decomiso. En esa dirección, cabe

[92] Ver: CipherTrace: "Cryptocurrency crime and anti-money laundering report", febrero 2021.
[93] Ver: SILFVERSTEN, Erik / FAVARO, Marina / SLAPAKOVA, Linda / ISHIKAWA, Sascha / LIU, James / SALAS, Adrian: "Exploring the use of Zcash cryptocurrency for illicit criminal purposes", RAND Europe, 2020.

señalar que a partir de los resultados de la 4ª Ronda de Evaluaciones Mutuas sobre cumplimiento con los estándares del GAFI, 12 de los 17 países del GAFILAT que han sido evaluados, cuentan con un grado de cumplimiento entre mayormente cumplido y cumplido con las Recomendación 4 y 38. En virtud de estas Recomendaciones, se establece que los países deben establecer mecanismos que permitan a sus autoridades competentes administrar de manera eficaz y, cuando sea necesario, disponer de los bienes congelados, incautados o confiscados. Estos mecanismos deben ser aplicables tanto en el contexto de los procedimientos internos como de conformidad con las solicitudes de países extranjeros[94]. Ello, conforme se ilustra a continuación[95]:

Tabla 1: Cumplimiento con la Recomendación 4 y 38 del GAFI:

Rec	Cuba	Costa Rica	Honduras	Guatemala	Nicaragua	México	Panamá	Perú	Colombia	República Dominicana	Uruguay	Chile
R4	MC	MC	C	MC	MC	MC	C	C	C	C	MC	MC
R38	MC	MC	MC	MC	MC	PC	MC	C	C	MC	MC	C

225. Cabe destacar, sin embargo, que ninguna de las normas reseñadas en las respuestas recibidas refiere expresamente a la incautación y/o decomiso de AV. Sin perjuicio de ello, a partir de la reforma operada en orden a la Recomendación 15 del GAFI (a fin de incorporar a los mencionados activos en los sistemas de ALA/CFT), estas Recomendaciones, particularmente lo referente a la cooperación internacional (R.38), también debe aplicarse a los AV[96].

226. Aun así, el propio GAFI reconoce que muchas AOP o fiscalías carecen de los conocimientos y/o los recursos requeridos para investigar conductas ilícitas vinculadas a AV. Destaca que la mayoría de los/las investigadores/as no se han topado aun con esa clase de activos en sus pesquisas, y deben enfrentar una curva de aprendizaje bastante empinada cuando ello ocurre[97].

227. En tal contexto, los países de la región están comenzando a dar los primeros pasos en dicha dirección. En efecto, de las respuestas recibidas se desprende que 8 de los 16 (50 %) países consultados reportaron haber registrado investigaciones sobre LA/FT con AV.

228. En cuanto a la incautación o decomiso de AV, tres países (Argentina, Brasil y Chile) reportaron la adopción de medidas tendientes a lograr ese cometido, mientras que otro, que también tuvo casos, no aportó información sobre si se adoptaron, o no, medidas sobre los AV involucrados. Así, en lo tocante a Argentina, se informó un caso en el cual, tras identificarse un monedero virtual radicado en una plataforma local de intercambio de AV a nombre de una

[94] Es importante destacar que en esta 4ta Ronda a los países que ya fueron evaluados no se les consideró a los AV o los PSAV dado los recientes cambios en los Estándares del GAFI. Se hace una mención especial a estas Recomendaciones dadas las obligaciones de las autoridades competentes para el congelamiento y decomiso de los bienes u activos.
[95] Fuente: GAFILAT: "Plan estratégico GAFILAT 2020-2025", págs. 26/27. Las calificaciones de las recomendaciones (R) se encuentran ajustadas de acuerdo con los informes de Recalificación presentados por el GTEM y aprobados por el Pleno de Representantes.
[96] Ver: GAFI: "Virtual assets and virtual assets service providers. Guidance for a risk-based approach", junio 2019, pág. 33, § 137.
[97] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 36, § 119.

sociedad implicada en el lavado de activos provenientes del narcotráfico, se procedió al embargo preventivo con fines de decomiso de los fondos. A tal efecto, los AV contenidos en el monedero (aprox. U$S 295.000) fueron transferidos a un monedero controlado por el juzgado interviniente. En otros casos en trámite, la fiscalía especializada en LA/FT sugirió la adopción de medidas similares con relación a fondos en custodia de plataformas de intercambio, sin que hasta el momento se haya podido concretar la incautación de los AV.

229. Brasil reportó cuatro casos en los que las autoridades adoptaron medidas cautelares referidas a esa clase de activos. Se trata de las operaciones "Faroeste", "Rekt", "Faraó" y "Egipto". En el primer caso mencionado, se investigó el uso de criptomonedas (en especial Bitcoin) como uno de los medios de pago en un presunto plan de venta de sentencias en un tribunal local. En las tres restantes, se consiguió bloquear una cantidad considerable de AV mediante órdenes judiciales dirigidas contra monederos "en custodia" en manos de PSAV. Así, en el marco de la "Operación Rekt", la medida cautelar tuvo por objeto AV valuados en 110 millones de reales, presuntamente originados en venta de drogas. En la "Operación Faraó", se congelaron bitcoins por valor de 6.4 millones de reales, vinculados a una estafa piramidal. Mientras que la "Operación Egipto" involucró el bloqueo de U$S 24 millones en criptoactivos que estaban bajo la custodia de una plataforma de intercambio de criptomonedas registrada en los EE.UU., también con relación a una investigación por una presunta estafa piramidal.

230. Por último, Chile reportó que en un caso en el que se investigan delitos de tráfico de drogas y LA, se logró incautar una suma importante de criptomonedas en un monedero virtual perteneciente a uno de los sospechosos, las que fueron traspasadas a una cuenta controlada por el Ministerio Público Fiscal para su custodia.

V. RECOMENDACIONES, PASOS QUE DEBEN ADOPTARSE Y CONCLUSIONES

A. Introducción

231. El objetivo principal de una investigación de carácter patrimonial es identificar y documentar los movimientos de fondos originados en -o vinculados con- la actividad delictiva. A tal efecto, los nexos entre *i)* el origen de los fondos; *ii)* sus beneficiarios; y *iii)* los momentos en los que los fondos son recibidos y los sitios en los que son almacenados, depositados o transferidos constituyen fuentes de información valiosa para las investigaciones referidas a la actividad delictiva subyacente[98].

232. En cuanto respecta a la operatoria criminal de LA/FT con AV, es importante tener presente que más allá de las especiales características de estos valores, que los hacen más vulnerables a la

[98] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 7, § 1.

explotación con fines delictivos y representan una dificulta adicional para los/las investigadores/as, lo cierto es que la manera en que se detectan e investigan dichas operatorias delictivas no es disímil a la que se utiliza en los casos tradicionales de LA/FT o de conductas ilícitas de tipo patrimonial.

233. La investigación patrimonial referida al uso de criptomonedas puede ir en dos direcciones. Por un lado, puede partir de la constatación de la existencia de actividad delictiva e intentar seguir el rastro de AV hasta sus beneficiarios/as (como ocurrió en el caso "Welcome to video" reseñado debajo, Caso § 4). En tal contexto, las conductas de LA con AV suelen identificarse como resultado de una investigación concerniente a actividades criminales que involucran el uso intensivo de efectivo, se desarrollan online o son aptas para generar montos significativos de ganancias ilícitas[99]. Entre las actividades criminales que pueden derivar en el uso de criptomonedas pueden encontrarse tanto conductas delictivas tradicionales trasladadas al mundo online (como el narcotráfico en los mercados de la Dark Web); o de ciberdelitos propiamente dichos como el ramsonware, la extorsión a partir de robo de información confidencial, o diversas modalidades de fraude informático.

234. Por otro lado, la investigación puede encontrar como punto de partida a ciertas transacciones con AV consideradas sospechosas, sea porque fueron realizadas o están conectadas con personas que se sabe están involucradas en actividades ilícitas, o porque han sido identificadas como sospechosas por una Unidad de Información Financiera (UIF) u otro organismo similar (por ejemplo, por asemejarse a las que llevan a cabo las "mulas de dinero" o por concretarse por medio de PSAV que se sabe están involucrados en la prestación de servicios de LA/FT, como los "mezcladores").

235. A fin de procurar una mayor eficacia en las investigaciones patrimoniales, es preciso que las autoridades encargadas de llevarlas a cabo tengan a su disposición el rango más amplio posible de información, ya sea a partir de fuentes propias, del intercambio con otras autoridades nacionales o de la cooperación con terceros (por ejemplo, en el ámbito privado). El GAFI destaca entre distintas categorías de información relevante para las investigaciones patrimoniales[100]. A saber:

- **Registros criminales e información de inteligencia**: se trata de la información almacenada por las AOP respecto de personas objeto de investigación con nexos potenciales con la actividad criminal. En el contexto de las AV, puede incluir datos sobre presunta actividad ilícita de esas personas en la Dark Web; identificación de su pseudónimos o alias; direcciones de criptomonedas o cómplices conocidos (y sus pseudónimos o alias); arrestos o condenas previas; direcciones físicas o electrónicas, números de teléfono o direcciones

[99] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, págs. 12/13 § 24.
[100] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 16/16, §§ 42/49 (remitiendo, a su vez, a GAFI: "Operational issues – Financial investigations guidance", junio 2012).

de correo electrónico que hayan podido utilizar en conexión con actividad delictiva. Esta información puede provenir de bases de datos propias u obtenerse mediante consultas a las bases que mantienen organizaciones policíacas como Interpol o Europol.

- **Información proveniente de controles de ALA/CFT**: Los reportes de operación sospechosa (ROS) originados en las UIF por lo general contienen abundante información respecto del perfil patrimonial y las actividades de las personas objeto de investigación. En pesquisas vinculadas al uso de AV, revisten especial importancia los ROS que provengan de PSAV capaces de relacionar a sus clientes/as con las transacciones realizadas.

- **Información patrimonial**: La cual comprende toda aquella que puede obtenerse a partir del cumplimiento de los deberes de DDC de los sujetos obligados por la regulación de ALA/CFT. Esto es: cuentas bancarias, registros financieros o comerciales, etc. En lo tocante al uso de AV, puede incluir registros de transacciones realizadas mediante PSAV, o de PSAV con entidades financieras tradicionales, o cualquier otra actividad patrimonial que pueda generar sospechas del posible uso de AV para reciclar fondos de origen ilícito.

- **Información de entes regulatorios**: Esto es, toda aquella que se encuentre en manos de organismos de supervisión como los bancos centrales, autoridades tributarias, reguladores de actividad bursátil o de seguros, etc.

- **Información de fuente abierta**: Incluye a toda la que puede obtenerse a través de fuentes abiertas de uso irrestricto, como Internet, las redes sociales, la prensa o electrónica o registros de acceso público. En el contexto de la investigación de LA/FT con AV, puede comprender datos como la cotización de las distintas criptomonedas, información de contacto o datos sobre PSAV, o nexos entre las personas objeto de investigación y potencial información identificatoria (direcciones de criptomonedas, monederos, vinculaciones con actividad criminal o con criminales, etc.). A nivel regional, la RRAG ha publicado un listado de fuentes abiertas de los países miembros[101].

236. Asimismo, teniendo en cuenta la estrecha relación que en muchos casos presenta la operatoria de LA con AV con los ciberdelitos, también puede encontrarse información valiosa en poder de las unidades nacionales especializadas en ciber seguridad, en aquellos países en los que las mismas existan. Esta puede incluir: a) reportes sobre incidentes que involucren al sector financiero; b) información sobre malware dirigido al robo de identidad o a la obtención no autorizada de información confidencial y/o financiera (incluyendo datos o programas utilizados para el manejo de AV); y c) información de inteligencia sobre la comunidad hacker o sobre amenazas a la ciberseguridad[102].

[101] Ver: GAFILAT /RRAG: "Listado de fuentes abiertas de los países miembros de la RRAG", junio 2021.
[102] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, págs. 87/88.

B. Importancia de los nexos entre los AV y la moneda fiduciaria

237. Dado que gran parte de la operatoria con AV tiene lugar en el ciberespacio, un punto focal esencial de las investigaciones patrimoniales referidas a conductas ilícitas que involucren esa clase de activos reside en la identificación de los nexos entre el mundo físico y el virtual, en los que se produce el intercambio entre los AV y la moneda fiduciaria. Estos nexos funcionan tanto como "puerta de entrada" -cuando los criminales pretenden llevar a cabo maniobras de criptolavado para la colocación y/o estratificación de fondos ilícitos obtenidos en moneda fiduciaria (convirtiéndolos en criptomonedas)- como de "rampa de salida", en los supuestos en los que el/la beneficiario/a de un delito intenta retirar la ganancia ilícita y convertirla en dinero tradicional, ya sea para gastarlo o reinvertirlo más fácilmente.

238. Esta "rampa de salida" o "puerta de entrada", desde o hacia el ecosistema de los AV, es, en la práctica, el punto vulnerable de cualquier esquema de LA/FT que involucre esos valores, en especial cuando se manejan montos importantes, dado que el carácter (relativamente) reducido de los mercados de criptomonedas los tornan más sensibles al ingreso o egreso masivo de fondos, que por lo general provocan alzas o bajas pronunciadas en el valor de los AV, que a su vez invitan al escrutinio de las operaciones que las causaron.

239. Es importante tener en cuenta, además, que las redes de intercambio de AV están pobladas de intermediarios centralizados, como las plataformas de intercambio y los servicios de monederos en custodia. Ello, toda vez que a pesar de que las criptomonedas fueron creadas para funcionar con una estructura descentralizada, y el intercambio entre usuarios dentro de la red es bastante simple, la conversión de moneda fiduciaria en AV o viceversa puede resultar difícil sin asistencia de un tercero, en especial si se opera con criptomonedas por primera vez. Las plataformas de intercambio surgieron para cumplir con ese rol, y han adquirido tal preponderancia que, en la actualidad concentran hasta el 99% de las transacciones con criptomonedas[103]. Gran parte de ese volumen es manejado por grandes plataformas internacionales como Binance, Bitstamp, Bitfinex, Coinbase y Kraken[104].

240. También existen numerosas plataformas dedicadas al intercambio de AV en América Latina, de las cuales la mayoría presta servicios en más de un país de la región: ArgenBTC, Bitex, Ripio, Satoshi Tango, Buda.com, Crypto MTK, Coinmama, BitCambio, Flowbtc, Bitcointoyou, Coinmama, CEX.io, Orionx, Obsidiam, Panda.exchange, Coinfield, Bitso, Volabit, Isbit, Bitrus, Cryptobuyer y CritoWay, entre otras.

[103] Ver: SILFVERSTEN, Erik / FAVARO, Marina / SLAPAKOVA, Linda / ISHIKAWA, Sascha / LIU, James / SALAS, Adrian: "Exploring the use of Zcash cryptocurrency for illicit criminal purposes", RAND Europe, 2020 (citando datos contenidos en: MOISENKO, Anton / IZENMAN, Karla: "From intention to action: Next steps in preventing criminal abuse of cryptocurrency", Royal United Services Institute (RUSI) Occasional Paper, Londres, 2019).
[104] Ver: European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses", Policy Department for Citizen's Rights and Constitutional Affairs, mayo 2018, pág. 40.

241. Esto implica que, en la práctica, la casi totalidad de las cadenas de transacciones con AV están llamadas a pasar, en un momento u otro, a través de uno de estos intermediarios. Así, la inserción de este elemento centralizado en un ecosistema naturalmente descentralizado genera cuellos de botella que pueden ser explotados para una mayor eficacia, tanto en la supervisión como en la investigación de conductas delictivas involucrando AV. De allí que, a partir de la nueva Recomendación 15 del GAFI, se requiera que la normativa a nivel local le imponga a los PSAV la obligación de recolectar, mantener y compartir con las autoridades competentes información obtenida por medio de la DDC, que puede resultar de enorme utilidad para las agencias de investigación a efectos de identificar a las personas que operan con AV, además de constituir una fuente potencialmente útil de evidencia sobre maniobras de LA/FT.

242. Habida cuenta que los PSAV constituyen la primera línea de alerta en lo tocante al LA/FT con AV -en la medida en que se encuentran en un lugar de privilegio para detectar posibles operaciones sospechosas y reportarlas a las respectivas UIF- los ROS derivados de transacciones consideradas sospechosas por aquellos constituye una de las principales fuentes de información para las investigaciones patrimoniales concernientes a maniobras ilícitas con AV descentralizadas (en especial, las criptomonedas)[105].

243. En esa dirección, la lista elaborada por el GAFI sobre las principales "señales de alerta" de actividad sospechosa con AV en su reporte de junio de 2020 debe ser considerada como la principal referencia sobre la cuestión[106]. A su vez, en un informe anterior, el citado organismo destacó, como las señales de alerta más relevantes, a las siguientes[107]:

- Estructuración de transacciones con AV para eludir límites de registro o reporte (similar a la estructuración de operaciones con dinero en efectivo);
- Transferencia de AV que operan en una Blockchain pública y transparente (como Bitcoin) a una plataforma de intercambio centralizada, para convertirlos inmediatamente en "monedas privadas" (como Monero, Zcash o Dash);
- Depósito de AV en una plataforma de intercambio y posterior retiro (a menudo inmediato), sin actividad de intercambio adicional, que constituye un paso innecesario que genera el pago de tasas de transferencia;
- Operaciones con direcciones de AV vinculadas a esquemas fraudulentos conocidos o con mercados en la Red oscura;

[105] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, pág. 150.
[106] Ver: GAFI: "Virtual assets: Red flag indicators of money laundering and terrorist financing", septiembre 2020.
[107] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 53, § 181.

- Creación de cuentas separadas bajo diferentes nombres para eludir restricciones a los límites operativos o de retiro de fondo impuestos por PSAV;
- Uso de servicios de transferencia de dinero publicitados en páginas de plataformas P2P;
- Efectuar un depósito inicial importante para abrir una nueva relación con un PSAV;
- Transferencia de AV desde/hacia monederos cuya actividad previa indique el uso de servicios de mezclado;
- Transacciones con AV originadas o dirigidas a servicios de apuestas online;
- Uso de múltiples tarjetas de crédito o débito asociadas a un monedero de AV para retirar montos importantes de moneda fiduciaria ("criptomonedas a plástico"); y
- Uso de monederos de almacenamiento "en frío" para transportar AV a través de las fronteras.

244. La información generada por las UIF a partir de los datos obtenidos por los PSAV (o por entidades financieras tradicionales, que operan con los PSAV) en cumplimiento de sus obligaciones de ALA/CFT reviste gran valor potencial para las investigaciones patrimoniales. En ese orden de ideas, se aprecia que los ROS presentados por estas entidades a partir de la detección de alguna de las "señales de alerta" antes mencionadas contienen tanto información sobre transacciones (cliente emisor, beneficiario, direcciones de los monederos del cliente, saldo en los monederos, fecha y hora de las transacciones, tipo de AV transferido, localización de la transferencia, transacciones canceladas, cuentas bancarias registradas o verificadas y tipo de dispositivos utilizados); como información sobre los/las clientes (nombre, identificación como usuario/a, dirección/nes IP, domicilio -físico- de facturación, dirección de correo electrónico, fecha de nacimiento, nacionalidad, ciudadanía, perfil económico y actividad comercial)[108].

245. El rol asignado a los PSAV como primera línea de alerta en la prevención del LA/FT con criptomonedas y su efectividad de la estructura global de ALA/CFT, dependen de que su actividad sea regulada en forma homogénea a nivel mundial. En tal contexto, y dada la facilidad con la que pueden transferirse AV y ofrecerse servicios vinculados a esos valores a través de las fronteras mediante Internet, la existencia de jurisdicciones con controles débiles o inexistentes respecto de los PSAV supone una vulnerabilidad para el sistema completo.

246. Aunque muchas plataformas o procesadoras de pagos con AV buscan operar en el marco de la legalidad, también existen otras que no. Estas últimas se ven favorecidas por la propia naturaleza de las criptomonedas, que facilita la existencia de PSAV que operan por fuera de la

[108] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 19, § 55.

regulación estatal, aprovechándose de las herramientas de anonimato en Internet que les permiten ocultar su verdadera localización y ofrecer sus servicios a clientes de todo el mundo. Como ya se señaló previamente, estos PSAV procesan un porcentaje importante de los AV de origen ilícito.

247. En tal contexto, las agencias de investigación deben poner especial énfasis en las actividades de los "mezcladores" o "conmutadores" y en los sitios de apuestas online, que concentran un alto volumen de fondos provenientes de delitos. Las investigaciones referidas al uso de AV deben tener, como objetivo, no sólo identificar y perseguir a las personas que exploten el recurso a las criptomonedas para desarrollar conductas delictivas, sino también perseguir y eventualmente hacer cesar la actividad de los PSAV u otros proveedores de servicios cuando la misma esté dirigida a favorecer o facilitar la operatoria criminal[109].

248. Un aspecto favorable a la actuación de las autoridades contra los PSAV que actúan ilegalmente es que, por lo general, suele existir cierta concentración en orden a los actores que prestan servicios a los criminales. Así, un estudio reciente sobre la actividad de los mezcladores y los sitios de apuestas online que reciben fondos de origen ilícito determinó que tres de estos servicios acaparaban el 97% de los bitcoins provenientes de actividad delictiva reconocida[110].

249. Por consiguiente, la identificación de los responsables de estos servicios debe ser prioritaria para las AOP. Aunque no publiciten su localización o la identidad de sus titulares, existen herramientas informáticas para el análisis de los dominios de Internet que pueden utilizarse para determinar quiénes son los probables responsables o administradores/as de las páginas en que se alojan dichas plataformas. Si estos PSAV están basados en la Red oscura, es posible explotar, a efectos de identificar a los/las titulares, el hecho de que su éxito se basa en la reputación, lo cual redunda en que exista abundante información potencialmente valiosa sobre los mismos en foros y páginas especializadas.

250. Sin perjuicio de lo señalado, también es preciso tener presente que los estándares establecidos por el GAFI sobre la materia no exigen que el intercambio de AV se canalice a través de PSAV. Las transacciones "par-a-par", sin intermediarios, entre titulares de monederos que no estén en custodia no está alcanzada por las regulaciones de ALA/CFT recomendadas por dicho organismo.

251. En Internet pueden encontrarse varias plataformas P2P como LocalBitcoins, LocalCryptos, Local.Bitcoin.com y Ccoins.io, entre otras, cuyo servicio se limita a conectar a compradores y vendedores entre sí para el intercambio de criptomonedas -ya sea entre sí o con moneda fiduciaria-, sin establecer mecanismos de pago dentro de la página o almacenar dinero fiduciario de sus

[109] Ver: GAFI: "Guidance on financial investigations involving virtual assets", unio 2019, pág. 44, § 147.
[110] Ver: FANUSIE, Yaya J. / ROBINSON, Tom: "Bitcoin laundering: An analysis of illicit flows into digital currency services", Elliptic Center on Sanctions & Illicit Finance, enero 2018, pág. 8.

usuarios. En algunas de estas plataformas sólo se permite el intercambio entre AV, pero no su conversión a dinero fiduciario, como por ejemplo Binance, Poloniex, Bittrex, Cripto Intercambio, KuCoin, Changelly, ShapeShift y PrimeXBT, entre otras. Algunas de estas ofrecen la posibilidad de llevar a cabo maniobras de CoinJoin o "Salto de cadenas".

252. Si bien el recurso a estas páginas podría servir para efectuar transacciones con AV evitando los controles de ALA/CFT (allí donde hayan sido implementados), su uso todavía no se ha vuelto masivo. En la actualidad, los PSAV siguen ofreciendo un servicio más fácil y seguro a las personas que desean operar con criptomonedas, con independencia de su origen (lícito o ilícito). La relativa dificultad en la concreción de transacciones P2P funciona, por el momento, como un limitante a su volumen. Sin embargo, si llevar a cabo esta clase de operación sin intermediarios se volviese más simple y seguro, ello podría derivar en un incremento del número y valor de las transacciones no sometidas a controles de ALA/CFT y representar una vulnerabilidad que deba ser atendida[111].

253. Otro punto de intercambio entre AV y moneda fiduciaria son los quioscos de criptomonedas o "Cajeros Bitcoin" que han empezado a aparecer en las ciudades de buena parte del mundo, incluida Latinoamérica. En estos cajeros, es posible intercambiar, comprar o vender criptomonedas (en especial, pero no exclusivamente, bitcoins), aunque por una comisión por lo general más elevada que en las plataformas de intercambio online. Si bien las compañías que operan estos cajeros están comprendidas en la definición de PSAV del GAFI, lo cierto es que, incluso en los países donde su actividad está regulada, la mayoría de estos cajeros requiere a sus clientes/as solo una cantidad limitada de información identificatoria para llevar adelante las transacciones, y en muchos casos los operadores no pueden garantizar que la documentación que reciben sea auténtica o que el/la usuario/a no esté actuando en favor de un tercero[112].

254. No obstante ello, el uso habitual de cajeros de AV por parte de personas objeto de investigación puede ofrecer ventajas para la pesquisa, en la medida en que constituye un punto de partida para eventuales tareas de vigilancia o seguimientos. En esa dirección, si se conoce que esas personas se mueven en determinados lugares y recurren a cajeros AV para desarrollar su actividad ilícita, es posible identificar los cajeros localizados en el área a través de páginas como CoinATMradar[113] y establecer puntos de vigilancia en los mismos a fin de determinar las fechas y horarios en los que son usados por los/las sospechosos/as. A partir de ello puede, por un lado, requerirse u obtenerse la información correspondiente a las transacciones concretadas en esa fecha y horario (direcciones utilizadas, tipo de AV involucrado, montos de las operaciones, etc.), o efectuar un seguimiento de los movimientos posteriores de aquellos a fin de identificar a sus potenciales socios o cómplices.

[111] Ver: GAFI: "FATF report to the G20 Ministers and Central Bank governors on the so-called stablecoins", junio 2020, pág. 8 § 32.
[112] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 40, § 133.
[113] https://coinatmradar.com/.

C. Técnicas investigativas basadas en el análisis de la Blockchain

281. Además de la información que pueda obtenerse de los PSAV, también es posible extraer datos de gran relevancia para las investigaciones patrimoniales de la propia estructura subyacente al funcionamiento de las AV. Como ya se explicó, tanto las transacciones de Bitcoin como de la mayoría de las criptomonedas se basa en la existencia de un registro público -denominado Blockchain o "cadena de bloques"- en las que aquellas se confirman y registran (en orden cronológico) a fin de garantizar la integridad del sistema.

282. El funcionamiento del proceso de transferencia y registro es similar con respecto a la mayoría de los AV conocidos, con excepción de algunas "monedas privadas". Las transacciones se inician cuando el/la vendedor/a transfiere una determinada cantidad de criptomonedas desde su monedero a la dirección de AV del/la comprador/a, que representa el monedero de éste/esta ultimo/a. Al validarse la operación mediante la introducción de la clave privada del/la vendedor/a, la red reconoce el envío de información y los "mineros" de dicha red procesan la transacción y agregan el valor de la misma al final de una cadena de datos informáticos que representa las transacciones anteriores. Los "mineros" luego incorporan un bloque conteniendo las últimas transacciones transmitidas a la red a continuación del último bloque completado, a un ritmo de aproximadamente un bloque cada diez minutos[114]. La sucesión de bloques resultante conforma la "cadena de bloques" (Blockchain).

283. En la Blockchain quedan registradas todas las transacciones que realizó el/la titular de un determinado monedero de AV, en orden cronológico. Respecto de cada operación, se consigna la ID de la transacción (valor hash), la fecha y hora en que se llevó a cabo, la dirección de origen y destino (puede haber una o más direcciones de origen y una o más direcciones de destino para cada transacción), el monto transferido, el costo de la transacción (esto es, la comisión cobrada por los mineros que la procesaron) y el saldo restante (esto es, cuantos bitcoins le quedan al emisor y cuantos al receptor al cabo de la operación).

284. En la siguiente imagen[115] se ilustra el modo en que se ve reflejada una operación en la Blockchain de Bitcoin. Allí figuran el "hash" (la ID de la transacción), la fecha y hora de la operación, la dirección del remitente, la cantidad de bitcoins transferidos, la dirección del receptor y el saldo resultante. El apartado "fee" representa la comisión que se asigna a los "mineros" para procesar la transacción, que -como puede apreciarse- todavía no fue confirmada.

[114] Ver: BRYANS, Danton: "Bitcoin and money laundering: Mining for an effective solution", Indiana Law Journal, Vol. 89, 2014, pág. 446.
[115] Fuente: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 13.

285. Toda esa información es pública, y puede ser consultada en muchas páginas web diferentes, como por ejemplo (respecto de Bitcoin) https://explorer.bitcoin.com/btc. En la Blockchain también se puede consultar el balance de cada dirección de AV, en el cual se consigna el historial completo de operaciones, el total enviado y recibido y el saldo resultante.

286. A partir de los datos consignados en la Blockchain, las agencias de investigación pueden conocer el historial completo de transacciones de una determinada dirección de AV, incluyendo las direcciones de todos los usuarios/as con las que efectuó transacciones y la fecha, hora y monto exacto transferidos (lo cual puede resultar útil como criterio de búsqueda, cuando se analizan en simultaneo muchas operaciones); como así también la cadena completa de transacciones efectuada por cada AV desde su creación y las direcciones IP asociadas a cada dirección de AV (a menos que el/la usuario/a se conecte con la red a través de una herramienta de anonimato como un VPN o el sistema TOR). El análisis de este conjunto de datos, y su entrecruzamiento con la información que se obtenga de otras fuentes (en especial si se lleva a cabo por medio de herramientas informáticas de "Big data") puede resultar fundamental para detectar la actividad delictiva con AV, identificar a sus responsables y conseguir evidencia incriminatoria.

287. Debido a ello, el análisis y rastreo de transacciones con AV tendiente a relacionar a las personas objeto de sospecha con direcciones de AV o monederos específicos debe convertirse en una tarea de rutina en el marco de las investigaciones sobre maniobras de LA/FT con AV[116]. A tal efecto, el análisis de la Blockchain constituye una herramienta investigativa esencial, tanto para obtener evidencia que sirva para conectar a las personas objeto de investigación con actividades delictivas o ganancias ilícitas[117], como para procurar la incautación y decomiso de dichas ganancias. Un caso reciente ilustra la importancia de la referida herramienta[118]:

Caso 3: Decomiso de Bitcoins robados de Silk Road a partir de análisis de la Blockchain:
En noviembre de 2020, el gobierno de EE.UU. presentó una moción para concretar el decomiso de aproximadamente 69.370 Bitcoins (BTC), Bitcoin Gold (BTG), Bitcoin SV (BSV) y Bitcoin Cash (BCH) valuados en U$S 1000 millones.
Estos AV habían sido previamente incautados en el marco de una investigación en la que se rastreó el destino de bitcoins otrora pertenecientes al desaparecido mercado virtual Silk Road que habían sido apropiados por un individuo que logró hackear la página del mencionado mercado, obtener las contraseñas y transferir la criptomoneda a una cuenta propia cuya dirección era 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbh (en adelante, 1HQ3). En 2020, con la asistencia de una empresa especializada en el análisis de la Blockchain se individualizaron 54 transferencias realizadas a comienzos de 2013 desde las cuentas de Silk Road a dos direcciones Bitcoin: 1BADznNF3W1gi47R65MQs754KB7zTaGuYZ y 1BBqjKsYuLEUE9Y5WzdbzCtYzCiQgHqtPN por un total de 70,411.46 BTC (valuados en aproximadamente $354,000 al momento de la transferencia). Los valores habían sido transferidos en montos redondos y en un corto espacio de tiempo. Así, 10 de las transacciones habían tenido lugar a las 3:59, todas por exactamente 2.500 BTC, un patrón que no es usual en los usuarios de Bitcoin. Estas operaciones no habían sido registradas en la base de datos de Silk Road como extracciones de vendedores o empleados, por lo que se infirió que se trataba de valores robados de la página.
El 9 de abril de 2013, desde las dos direcciones que habían recibido un total de 70.411,46 BTC se transfirieron poco más de 69.471 BTC (valuados en ese momento en U$S 14 millones) a la dirección 1HQ3. Luego, el 23 de abril, desde esta última dirección se giraron 101 BTC (aproximadamente U$S 23.000) a BTC-e, una plataforma de intercambio de AV no registrada. Entre abril de 2015 y noviembre de 2020, los poco más de 69.370 BTC restantes permanecieron en 1HQ3. Durante ese lapso, una parte de los AV se convirtieron en BCH, BTG y BSV. Un análisis de las Blockchains de cada una de las variantes permitió determinar que los fondos seguían en 1HQ3.
En noviembre de 2020, las autoridades estadounidenses identificaron al individuo responsable del robo de los bitcoins de Silk Road, y éste suscribió un acuerdo mediante el cual consintió la incautación de los AV por parte del gobierno de ese país.

288. La investigación patrimonial se facilita en los supuestos en los que es posible rastrear los movimientos de AV desde y hacia un PSAV conocido, sobre todo si se trata de uno que, por encontrarse en una jurisdicción en la que su funcionamiento está regulado, se encuentra sometido a obligaciones de ALA/CFT. A tal efecto, cuando -por cualquier método- se logra identificar la/las dirección/es de AV que utiliza la persona objeto de investigación, puede recurrirse a la información consignada en la Blockchain para determinar si ha operado con algún PSAV, y luego requerir a los/las responsables de este último que aporten los datos asociados a aquella/s dirección/es obtenidos mediante las tareas de DDC. Otro caso reciente da cuenta de la utilidad de esta estrategia investigativa[119]:

Caso 4: Welcome to video. Seguimiento de operaciones con Bitcoin para identificar clientes de página dedicada al intercambio de imágenes de explotación sexual infantil:
Una operación conjunta entre las autoridades de Corea del Sur, los EE.UU. y otros once países permitió identificar y arrestar a 337 usuarios de la página "Welcome to video" (WTV), que funcionaba en la Dark Web y estaba dedicada al intercambio de imágenes de explotación sexual infantil.
Tras identificar y arrestar al administrador de la página en Corea del Sur a comienzos de 2018, los investigadores enviaron pequeñas cantidades de bitcoins a los monederos Bitcoin que la página le asignaba a los/las usuarios/as. A partir de allí, se rastrearon los movimientos de AV desde cada de esos monederos mediante el análisis de la Blockchain, lo cual permitió conectarlos con las direcciones de plataformas de intercambio de AV basadas en los EE.UU. (sujetas a obligaciones de ALA/CFT).
Con los datos aportados por los responsables de dichas plataformas en cumplimiento de órdenes judiciales, se logró identificar y detener a los/las usuarios/as que habían recurrido a esos servicios para el intercambio de los AV vinculados a la operatoria de WTV.

289. La identificación de las direcciones de AV de actores claves dentro de las redes de intercambio de esos valores es, por consiguiente, un elemento fundamental para la "desanonimización" de usuarios/as específicos/as y la reconstrucción de sus redes de contactos. En atención a ello, es importante que las direcciones de AV de las plataformas de intercambio de criptomonedas, mezcladores, casas de apuestas online, mercados ilícitos en la Red oscura, o de personas ya identificadas como probables sospechosas de dedicarse a alguna actividad ilícita generadora de fondos, o al LA/FT, entre otras, que vayan identificándose en el transcurso de investigaciones, sean registradas, ordenadas y catalogadas para permitir su uso ulterior, tanto en el marco de la misma investigación en la que se logró la identificación como en otras posteriores. Las AOP deben contar con una base lo más amplia posible de direcciones de AV con titulares identificados, ya que ello facilita el uso de la Blockchain para permitir la identificación de otros/as usuarios/as que tengan contacto con aquellos[120].

290. Los/las usuarios/as de AV involucrados en actividades ilícitas también pueden ser identificados mediante un análisis de la Blockchain centrado en los patrones que surgen de su

[119] Fuente: Departamento de Justicia (DOJ) de los EE.UU.
[120] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 52, § 180.

historial de transacciones. Ello así, desde que la actividad de estos/as por lo general difiere de la de los/las que se dedican a la actividad lícita. Así, los/las usuarios/as ilegales tienden a efectuar un número mayor de transacciones, pero por montos menores. También son más propensos/as a efectuar operaciones con los mismos interlocutores. El motivo de estas diferencias en la conducta transaccional es que los/las usuarios/as ilícitos/as de AV tienden a utilizar las criptomonedas (casi) exclusivamente para facilitar el tráfico de bienes y servicios ilegales (o para reciclar los fondos originados en dicho tráfico o en otros delitos), mientras que para los/las usuarios/as lícitos/as los AV son tratados, en general, como una inversión. Por consiguiente, los/las usuarios/as ilícitos/as suelen retener los AV por menos tiempo, lo cual es consistente con la intención de prevenir la incautación de los mismos por parte de las autoridades[121].

291. De igual manera, es más probable que un/una usuario/a de AV esté involucrado/a en actividades ilícitas si utiliza "mezcladores" en sus transacciones o lleva a cabo el tipo de operaciones (como el CoinJoin o el "salto de cadenas") tendientes a impedir la reconstrucción de la cadena de transferencias. En un plano más general, el entramado de transacciones entre usuarios/as ilícitos suele ser considerablemente más denso que los que se verifican en el ámbito de los/las usuarios/as lícitos, con los distintos actores mucho más conectados entre sí a través de operaciones cruzadas. Ello es consistente con la tendencia de esa clase de usuarios/as a utilizar los AV primordialmente para el tráfico de bienes y servicios ilícitos y otras actividades delictivas.

292. A partir de ello, en el marco del análisis de la Blockchain coexisten distintos métodos para procurar la desanonimización de los/las usuarios/as de AV, siempre a partir de los datos conocidos y de la explotación de las características inherentes al ecosistema de criptomonedas que facilitan la identificación de quienes operan en dicho ámbito. Estos incluyen:

- El rastreo de las transacciones originadas en los "monederos calientes" (online) de los principales mercados ilícitos de la Red oscura, recopilando las direcciones de todos los clientes y minando la información resultante.

- La segmentación ("Clustering") de los/las usuarios/as a partir de las diferencias -ya reseñadas- entre los/las que suelen operar con fondos de origen ilícito y los/las que recurren a los AV con fines lícitos.

- La exploración de la topología de la red de AV para identificar "comunidades" de usuarios/as con base en las transacciones entre ellos/as.

- El aprovechamiento de la información contenida en foros y otros ámbitos de la Red oscura sobre usuarios/as de AV involucrados en operatoria ilegal, incluyendo direcciones de AV,

[121] Ver: FOLEY, Sean / KARLSEN, Jonathan R. / PUTNINS, Talis J. "Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?", The Review of Financial Studies, Vol. 32, N° 5, 2019, págs. 1798/1853.

pseudónimos o apodos, referencias sobre su actividad que puedan arrojar indicios sobre su ubicación, etc.

293. El recurso al análisis de la Blockchain (o "Chain analysis") como técnica investigativa requiere del uso de las herramientas tecnológicas adecuadas, además de los conocimientos técnicos necesarios para utilizarlas. En cuanto a las herramientas, en el nivel primario se usa un explorador de Blockchain, que es una aplicación de red que opera como una suerte de motor de búsqueda en el ecosistema AV, que permite encontrar direcciones, transacciones y otros datos vinculados a aquellas. Existen versiones de fuente abierta de estas aplicaciones que pueden descargarse gratuitamente en la Internet[122].

294. Asimismo, existen recursos informáticos de mayor sofisticación, específicamente diseñados para las necesidades de las agencias de investigación, en manos de compañías privadas especializadas en el análisis de la Blockchain como Chainalysis, Elliptic, Ciphertrace o Blockchain Intelligence Group, entre otras. Los métodos utilizados por dichas empresas permiten mapear las transacciones efectuadas con bitcoins con hasta un 90% de efectividad[123]; y se han desarrollado herramientas para el análisis de las principales Altcoins, como Litecoin y Ethereum, que presentan características similares a las del Bitcoin[124]. Por añadidura, las capacidades tecnológicas en manos de estas compañías privadas pueden resultar la única forma de rastrear el destino de las criptomonedas en supuestos de "chainhopping".

295. Aunque el uso de técnicas de análisis de la Blockchain pueda parecer un recurso ajeno a la actuación de las agencias de investigación tradicionales, constituye un elemento clave de cualquier investigación vinculada a los AV[125]. A tal efecto, si se opta por no desarrollar las herramientas tecnológicas necesarias internamente, la cooperación pública privada con las compañías especializadas en Chain analysis (las que, por añadidura, cuentan con extensas bases de datos de direcciones AV con titulares ya desanonimizados) puede ser una buena alternativa, recomendada además por organismos como CARIN.

296. En este último supuesto, es preciso que las AOP o unidades del MPF intervinientes cuenten con agentes o funcionarios preparados para explicar los hallazgos de estas compañías en el marco de los procesos judiciales que tengan lugar en conexión con las conductas delictivas con AV objeto de investigación. Se recomienda, en tal sentido, mantener una buena relación de trabajo con el personal de las empresas prestadoras del servicio, en especial si estos pueden llegar a ser llamados a testificar sobre el modo en que se arribó a las conclusiones presentadas[126].

---

[122] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 25, § 77.
[123] Ver: DUPUIS, Daniel / GLEASON, Kimberley: "Money laundering with cryptocurrency: Open doors and the regulatory dialectic", Journal of Financial Crime, agosto 2020.
[124] Ver: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 31.
[125] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 37, § 123.
[126] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 37, § 124.

D. Técnicas de inteligencia de fuente abierta y vigilancia electrónica

297. La información que surge del análisis de la Blockchain puede ser complementada con datos o evidencia proveniente de otras fuentes, u obtenida mediante el empleo de técnicas de investigación tradicionales, como la vigilancia, los seguimientos, o el interrogatorio de testigos o personas de interés. Una forma efectiva de explotar la profusión de datos digitales que caracteriza a las sociedades modernas es recurriendo a las técnicas de "Inteligencia de fuentes abiertas" (OSINT, por sus siglas en inglés), denominación que alude a la recolección, procesamiento y análisis sistemático de información de acceso abierto. Esto es: la información disponible para el público en general sin restricciones[127].

298. En lo referido a las investigaciones patrimoniales sobre actividades ilícitas con AV, la OSINT puede utilizarse, por ejemplo, para obtener datos sobre los titulares de direcciones de Bitcoin u otras Altcoins ya conocidas por los/las investigadores/as. A tal efecto, puede intentarse colocar la dirección de AV en los motores de búsqueda en la Internet, ya que es bastante usual que las personas que se dedican al comercio ilícito en la Red (o las organizaciones terroristas que busquen captar fondos a través de AV) publiquen su dirección (asociándola a su perfil y pseudónimo online) en foros (como Reddit, 4Chan, 8Chan) o en las secciones de comentarios de páginas web especializadas en criptomonedas o en tecnología informática. Por añadidura, pueden consultarse páginas de Internet específicamente dedicadas a la identificación de usuarios de Bitcoin y de direcciones asociadas a aquellos, como walletexplorer.com.

299. La misma técnica puede utilizarse para obtener información en la Red oscura, en la que existen múltiples foros (Dread, Darknet Avengers, The Hub, Exploit.in) en los que, aprovechando el anonimato que confiere el ingreso mediante TOR, las personas comparten libremente información sobre los servicios ocultos, incluyendo sus direcciones, los productos y servicios que ofrecen, comentarios sobre la calidad del servicio, apodos de los comerciantes más (o menos) exitosos, etc.

300. Al respecto, es importante tener presente dos cuestiones. En primer lugar, que los pseudónimos o denominaciones utilizados online por las personas que realizan su actividad ilícita en dicho ámbito rara vez se modifican. Ello se debe, por un lado, a que el éxito de su actividad comercial en la Red por lo general se encuentra estrechamente ligado a su reputación online (esto es, a los comentarios que sobre ellos se vuelcan en los bazares virtuales o en los foros). Por el otro, a que las personas que pasan gran parte de su vida en la Internet tienden a desarrollar un gran apego por los pseudónimos que los identifican en la Red, y son reacios a dejar de usarlos, incluso

[127] Ver: MEDINA, Manuel: "Inteligencia de fuente abierta", Basel Insitute of Governance, Quick Guide Series, N° 17, junio 2020.

cuando ello sería recomendable por razones de seguridad operacional, tal como se refleja en el siguiente caso[128]:

Caso 5: Albert González. Mantenimiento de identidad online como elemento clave para ligar a un individuo con actividad ilícita:
Tras ser arrestado en el marco de una investigación por el uso de tarjetas de débito clonadas, el hacker estadounidense Albert González comenzó a trabajar en conjunto con el Servicio Secreto de los EE.UU., asesorando y capacitando a sus agentes en cuestiones vinculadas a la informática.
Sin embargo, en simultaneo y sin que las autoridades lo supiesen, González organizó un nuevo grupo de hackers con el cual llevó a cabo una serie de importantes ataques informáticos a los sistemas de varias compañías de los EE.UU., haciéndose con los datos privados de millones de usuarios de tarjetas de crédito, los cuales vendía a compradores en Rusia para ser utilizados en la elaboración de tarjetas mellizas.
La intervención de González en la referida actividad ilícita fue descubierta cuando su comprador ruso fue arrestado al intentar ingresar en los EE.UU., oportunidad en la que el análisis de su computadora personal reveló que el pseudónimo de su cómplice era "Soup Nazi", precisamente el mismo que González venía utilizando desde antes de ser aprehendido por primera vez, y el cual mantuvo incluso en sus interacciones con los agentes del Servicio Secreto.

301. En segundo lugar, debe tenerse presente que los pseudónimos online muchas veces tienen un correlato ya sea en la Internet superficial (cuando el individuo actúa sobre todo en la Red oscura) o incluso en la vida real, el cual -en caso de ser descubierto- puede permitir vincular a la actividad ilícita con su verdadera identidad. En tal contexto, las AOP pueden sacar provecho de los errores que las personas suelen cometer al momento de escindir su identidad online de su identidad (secreta) en la vida real, como no recordar utilizar herramientas de navegación anónima en alguna oportunidad, usar la misma dirección de AV para actividades ilícitas y lícitas o emplear una dirección de correo electrónico asociada a su verdadero nombre en conexión con su identidad online. Ello, conforme se ilustra en el siguiente caso[129]:

Caso 6: Ross Ulbricht. Uso de mail de identidad IRL para actividad ilícita:
En el marco de la investigación referida al mercado online Silk Road, el FBI logró descubrir la identidad de su administrador, Ross Ulbricht, mediante una búsqueda de datos en la Internet superficial (no en la Dark net). En el período inicial de su actividad delictiva, Ulbricht cometió un error cuando empezó a publicitar el mercado online en un foro de la Internet superficial dedicado a las drogas ilícitas, bajo el sobrenombre "Altoid" (luego pasaría a utilizar el sobrenombre "Dread Pirate Roberts" en su rol como administrador de Silk Road). Meses después, apareció en otro foro online con el mismo apodo -Altoid- solicitando información sobre Bitcoin y pidiendo a otros usuarios que se comunicasen a su dirección de correo electrónico, oportunidad en la que suministró su dirección personal. Fue este error el que permitió, posteriormente, vincular a Silk Road con el sobrenombre "Altoid" y luego a este último con la dirección personal de correo electrónico de Ulbricht, a través de la cual el FBI pudo averiguar su verdadera identidad.

302. Por los mismos motivos, las técnicas de OSINT también pueden resultar efectivas para obtener información sobre PSAV no registrados que presten servicios a personas involucradas en conductas ilícitas con AV, incluyendo a mezcladores o plataformas P2P de intercambio de criptomonedas, sea en la Internet superficial o en la Red oscura. Ello así, desde que estos se manejan con el mismo sistema basado en la reputación que los mercados ilegales online, dependiente de la devolución de los/las participantes del mercado en la ventana de comentarios o en foros especializados, en los que se alerta a otros/as usuarios/as sobre la calidad del servicio, si sigue en línea o está caído, si es fraudulento, etc. En tal contexto, los/las investigadores/as pueden acceder en forma anónima a esos foros o páginas (al igual que cualquier otro usuario/a de la Red) y conseguir datos útiles sobre PSAV ilegales o no registrados que operen en un determinado país (o presten servicios a personas de ese país) para, a partir de allí, intentar identificar a los que puedan estar operando con la/las persona/s objeto de investigación.

303. Por añadidura, las técnicas de OSINT pueden aplicarse para vincular a las personas sospechadas de estar involucradas en conductas ilícitas generadoras de fondos con los/las presuntos/as lavadores/as de dichos fondos. En efecto, incluso si las comunicaciones entre ambas partes se llevan a cabo exclusivamente en el ciberespacio y mediante herramientas de anonimato, es probable que existan datos aptos para servir como indicios sobre la existencia de una relación entre ambas. Ello, toda vez que resulta improbable que una persona dedicada a una actividad criminal le confié el control de sus ganancias a un/una lavador/a, en ausencia de un vínculo previo de confianza o alguna circunstancia que justifique la entrega de los fondos a un tercero.

304. Por último, la información existente en fuentes abiertas puede resultar útil para comprender mejor el estilo de vida, los activos con los que cuenta la persona sospechosa, o los lugares en los que reside o desarrolla su actividad comercial o social. Ello, teniendo en cuenta que, en ocasiones, incluso los delincuentes más capaces (o sus familiares o amigos) pueden revelar información comprometedora a través de publicaciones en redes sociales como Facebook, Instagram, Twitter, TikTok, etc.

305. Asimismo, con respecto a esta información, es importante tener presente que en cada aplicación existen al menos dos capas de datos explotables para una investigación. En primer lugar, la capa de contenido, que incluye a la información “publicada” por el usuario (mensajes, fotos, videos, etc.). En esta dirección, las imágenes posteadas pueden aportar muchos datos sobre una persona, no ya únicamente sobre su aspecto físico sino también sobre su entorno, localización, estatus, ideología, etc. En especial cuando se “etiquetan” las imágenes, asociándolas a perfiles de usuarios de la red social o incluso a personas que no han ingresado al servicio).

306. Debajo de la primera capa existe una segunda compuesta por los metadatos, que pueden aportar información sobre el equipo a través del cual se publicaron los contenidos, del propio usuario o una descripción sobre los archivos propiamente dichos. Un ejemplo típico de esta última clase de metadatos está dado por los datos EXIF ("Exchangeable image file format" o "Formato de archivo de imagen intercambiable") contenidos en los videos o imágenes, que describen el equipo y la configuración ("Settings") con los que se obtuvo ese video o imagen. Dependiendo del equipo utilizado, los metadatos de la imagen o video también pueden incluir información sobre la fecha, horario y ubicación en la que fueron creados. Estos datos pueden generar oportunidades para obtener indicios o sacar conclusiones respecto de personas u organizaciones asociadas con dichos archivos o con las cuentas de la red social en la que fueron publicadas. Incluso aspectos aparentemente inocuos como los certificados SSL ("Secure sockets layer") de las páginas web permiten obtener información sobre el titular del sitio.

307. La ventaja del recurso a la OSINT como herramienta de investigación es que -en especial comparada con el análisis de la Blockchain- no requiere conocimientos técnicos avanzados por parte de quienes la lleven a cabo, lo que redunda en que el empleo de dicho recurso no este limitado a especialistas en cibercrimen. Por el contrario, todos/as los/as investigadores/as deberían estar capacitados para efectuar búsquedas en fuentes abiertas y recopilar información de acceso público[130].

308. Además, para facilitar el proceso han surgido una variedad de herramientas tecnológicas que permiten efectuar las búsquedas en forma automática, entre las que cabe mencionar a Maltego o Spokeo, entre otras. Asimismo, en la Red existen múltiples buscadores específicos para determinados objetivos, como por ejemplo Shodan, que ayuda a localizar diversas tecnologías incluyendo webcams, impresoras, dispositivos VoIP y routers, entre otras cosas; NameCHK, que es una herramienta que permite comprobar si un nombre de usuario está disponible en multitud de servicios online; Tineye, un servicio de búsqueda inversa de imágenes (en el cual, añadiendo una imagen se muestra si la misma se encuentra en algún sitio de Internet); y Pipl, que busca coincidencias en internet sobre la base de diferentes criterios como nombres, direcciones de correo o teléfonos. También hay páginas en la Internet superficial que brindan información sobre la naturaleza y estado (online u offline) de los servicios ocultos o páginas en la Darknet y sus espejos, como Dark.fail o el TNO Dark Web Monitor. Otras herramientas, como GitHub, pueden utilizarse para llevar a cabo tareas de OSINT en la Red oscura.

309. Por añadidura, el Instituto de Basilea ha desarrollado una herramienta propia para agilizar el proceso de búsqueda denominada "Basel Open Intelligence", la cual realiza búsquedas automáticas del nombre de una persona u organización, combinado más de 200 palabras clave sobre delitos financieros, procesos judiciales, otros delitos y listas de palabras clave personalizadas.

[130] Ver: Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations", 2018, pág. 51.

También rastrea la Red oscura, seleccionando cualquier referencia en listas de sanciones y personas políticamente expuestas. La herramienta puede llevar a cabo búsquedas en varios idiomas, y ofrece a sus usuarios/as la opción de traducir automáticamente artículos a su idioma para facilitar el análisis. Los documentos encontrados en la búsqueda se enumeran junto con el texto principal extraído del sitio web, excluyendo el contenido irrelevante (como publicidad, menús o avisos de cookies) y resaltando las palabras clave están resaltadas para facilitar la lectura[131].

310. Además de los datos que recopilan las propias agencias de investigación mediante técnicas de OSINT, puede obtenerse información ya procesada sobre personas de interés recurriendo a los servicios de las denominadas "data brokers". Estas compañías se dedican a la recopilación y procesamiento de información de múltiples fuentes y a la elaboración de minuciosos perfiles personales[132], que incluyen datos tales como edad, género, educación, historial de empleo y residencias, relaciones, cantidad de hijos, compras, actividades, uso de redes sociales, opiniones políticas, raza y religión, ingresos, titularidad de vehículos y propiedades, detalles de productos bancarios y de seguros adquiridos, compras con tarjeta de crédito en los últimos 24 meses, estatus socioeconómico, estabilidad económica, etc.

311. Las técnicas de OSINT son más efectivas si se las combina con el uso de medidas de investigación tradicionales como los seguimientos o la vigilancia física, la inspección de los residuos que desechan las personas objeto de interés, los pedidos de informes, las órdenes de presentación y/o los registros personales o domiciliarios, la obtención de declaraciones testimoniales, etc. Muchas investigaciones patrimoniales exitosas se basan en combinar en forma efectiva estas prácticas tradicionales con técnicas más sofisticadas, propias de una pesquisa que se vincula, total o parcialmente, con actividades desarrolladas en el ámbito online. Los siguientes casos ejemplifican la utilidad de adoptar esta estrategia[133]:

Caso 7: Investigación con técnicas combinadas:
En 2017, tras el arresto de un traficante de drogas que operaba en la Darknet, se inició, a partir del hallazgo de un perfil de usuario y una dirección AV en un foro online de esa red, una investigación que involucró a la unidad de ciber aduana de la policía francesa. Se utilizaron diversas metodologías, incluyendo la actuación de agentes encubiertos online; el rastreo de transacciones en la Blockchain a fin de reconstruir la red de contactos entre las plataformas de intercambio de criptomonedas, mercados online y mezcladores y enumerar las transacciones realizadas entre estos; se libraron ordenes de presentación para obtener y analizar datos; se libraron pedidos de información a plataformas de intercambio de AV y proveedores de servicios de monederos sobre pseudónimos online y transacciones asociadas a los mismos; y se efectuaron compras de prueba. Aunque la investigación se centraba más que nada en bitcoins, la persona objeto de la misma también realizó operaciones con Bitcoin Cash, Ethereum, Monero, Ripple, Litecoin y Zcash. Los fondos involucrados se estimaron en aproximadamente 700.000 euros en un período de 9 meses.

[131] Ver: MEDINA, Manuel: "Inteligencia de fuente abierta", Basel Insitute of Governance, Quick Guide Series, N° 17, junio 2020.
[132] Por ejemplo: Equifax, Acxiom, Experian, Epsilon, CoreLogic, Datalogix, Intelius, PeekYou, Exactis y Recorded Future, entre otras.
[133] Fuente: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, págs. 55/56, § 190 y Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations", 2018, pág. 48.

Caso 8. "Pedro el grande". Combinación de técnicas tradicionales y online.
En febrero de 2017, la adolescente de 18 años Aisha Zughbieh-Collins fue encontrada sin vida en su departamento a causa de una sobredosis del opioide sintético U-47700 (U4). La madre de la víctima, sospechando que había adquirido la droga en Internet, les aportó a los detectives su dirección de email. Por añadidura, se encontró en la escena del crimen evidencia indicando que la droga había sido enviada por correo, oculta en una variante específica de prueba de embarazo comercializada en la cadena de farmacias Dollar Tree Store. Si bien se determinó que la dirección del remitente era falsa, se pudo establecer en qué oficina postal había sido adquirido el envoltorio.
El hallazgo más relevante fue, no obstante, el de un cuaderno en el que se había anotado un código alfanumérico, que resultó ser la clave criptográfica privada de la víctima para el software de encriptación de comunicaciones "Pretty Good Privacy" (PGP). Accediendo al email de la víctima con el código, los investigadores pudieron descubrir que había adquirido las drogas en un mercado virtual de la Dark Web a un vendedor apodado "Pedro el grande", que conforme se indicaba en la propia página, había efectuado más de 10.000 transacciones.
Los investigadores efectuaron una compra controlada de U4 a "Pedro el grande", que recibieron oculta en la misma clase de prueba de embarazo hallada en el departamento de la víctima. Se determinó que estas pruebas habían sido adquiridas a través de una compañía de venta online que sólo aceptaba pagos con Bitcoin, y que estaba ligada a dos direcciones de correo electrónico, cuyo titular fue identificado como Theodore Khleborod, domiciliado en Greenville. Los investigadores pudieron determinar que Khleborod había recibido numerosos envíos internacionales desde China (uno de los países donde se fabrica la droga U4). Asimismo, mediante el análisis de las publicaciones del nombrado en redes sociales, se estableció que estaba en una relación con una mujer llamada Ana Barrero.

312. A su vez, los avances tecnológicos de los últimos años han derivado en que medidas tradicionales como la vigilancia o los seguimientos se lleven a cabo con ayuda de dispositivos electrónicos que aumentan su eficacia, abaratan sus costos y amplían considerablemente su alcance. Además de proveer información o evidencia útil para cualquier investigación sobre criminalidad organizada -como la identificación de otros individuos asociados a los/las sospechosos/as, la reconstrucción de vínculos y actividades, el descubrimiento de la posible ubicación de activos o información patrimonial de interés, etc.- la utilización de medios electrónicos de vigilancia también puede servir para la averiguación de datos relevantes para las investigaciones sobre conductas ilícitas con AV, como por ejemplo conexiones con plataformas de intercambio de criptomonedas, mezcladores, páginas de apuestas online, redes P2P dedicadas a la transferencia de AV o servicios de almacenamiento en la nube. Asimismo, se puede establecer por esa vía qué tipo de dispositivos informáticos usan las personas objeto de investigación, si cuentan con uno o más monederos online, los métodos preferidos de comunicación o si utilizan conexiones públicas de Wi-Fi u otros medios electrónicos a los que puedan acceder las autoridades[134].

313. A tal efecto, un método eficaz es el monitoreo del tráfico de Red de las personas objeto de investigación[135]. Al respecto, cabe destacar que este monitoreo incluye mucho más que la

[134] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 20, § 60.
[135] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, pág. 113.

captación de los intercambios de correos electrónicos. Ello así desde que, de hecho, solo una pequeña parte del tráfico de internet comprende a comunicaciones "entre humanos" como los e-mails. La mayoría de las comunicaciones en Internet son entre humanos y computadoras, como las páginas en tránsito de la World Wide Web (WWW), comandos enviados a servidores remotos y transferencias de archivos. Muchas otras involucran comunicaciones entre computadoras, como el tráfico administrativo de la red que mantiene funcionando a la Internet. Estas comunicaciones también pueden aportar información relevante, la que, además, puede capturarse en muchos formatos distintos: documentos digitales voluminosos, imágenes, archivos de audio, videos e incluso comunicaciones telefónicas realizadas a través de la Red.

314. Es importante tener en cuenta, asimismo, que el monitoreo de la Internet, por su propia naturaleza, supone siempre el análisis de todo el tráfico de datos que fluye a través del punto específico de la Red en que se produce la interceptación, a efectos de identificar, entre todos ellos, a los que son de interés para la investigación (igual que un policía que pretende encontrar a un individuo sospechoso en una multitud y debe observar, para poder identificarlo, a todas las personas que se encuentran allí). En tal contexto, para concretar esta medida se requiere de herramientas informáticas especialmente diseñadas para filtrar los datos, de modo tal de capturar sólo aquellos cuya obtención está amparada por la correspondiente autorización judicial.

315. En muchos casos, el monitoreo del tráfico de Red no permitirá acceder al contenido de las comunicaciones realizadas a través de Internet, toda vez que es cada vez más usual que éstas estén encriptadas. Sin embargo, por lo general si será posible capturar los denominados "datos de envoltorio", es decir todos aquellos que no forman parte del contenido de la comunicación, sino que se refieren a los mecanismos para su concreción (direcciones IP de origen y destino, volumen de los datos, nodos de Internet involucrados en el intercambio de paquetes de datos, etc.)[136]. Ello, salvo que alguna de las partes de la comunicación haya recurrido a una herramienta de anonimato (como el sistema TOR o un VPN) para enmascarar su verdadera dirección IP.

316. Por otra parte, las modernas tecnologías también facilitan el seguimiento de las personas, desde que ya no hace falta, a tal efecto, la participación de múltiples agentes y vehículos para seguir físicamente a las personas objeto de investigación, sino que la medida puede concretarse mediante dispositivos de GPS que permiten el seguimiento simultáneo de varias personas, durante muchos días y a un costo considerablemente inferior. A su vez, la proliferación del uso de aplicaciones móviles en los "teléfonos inteligentes" (para navegación, redes sociales, compra o banca online, etc.), en muchos casos asociadas a los GPS insertos en los propios teléfonos móviles, ofrece otro medio para el seguimiento prospectivo -o incluso retrospectivo- de personas objeto de investigación[137].

[136] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, pág. 113.
[137] Ver: Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations", 2018, pág. 51.

317. En efecto, el propio diseño de las redes de comunicación por telefonía celular (3G o 4G) supone un contacto constante entre los dispositivos y las torres de telefonía celular para permitir el funcionamiento en segundo plano de las aplicaciones de Red, con independencia de si el/la usuario/a esta utilizando, o no, el teléfono móvil para comunicarse. Cada uno de esos contactos entre el celular y las torres genera un registro que es almacenado por la compañía telefónica, que incluye la fecha y hora y la celda específica con la que se estableció la conexión. Estos retazos de información, denominados "información sobre ubicación de celdas" ("Cell site location information" o CSLI), resultan de enorme utilidad, ya que no sólo permiten ubicar a la persona en un lugar específico en un momento dado, sino reconstruir el historial de sus movimientos durante días o incluso meses.

E. Evidencias o indicios relevantes en los sistemas informáticos de las personas de interés

318. Cuando -como ocurre con las conductas a las que refiere esta guía- el objeto de una investigación se refiere a actividades ilícitas desarrolladas en el ciberespacio o mediante equipos informáticos (incluyendo a los modernos smartphones, que son, en esencia, computadoras portátiles), los dispositivos que almacenan información digital se convierten en un reservorio fundamental, ya sea de evidencia o de datos relevantes para el avance de la pesquisa. Entre los elementos que pueden obtenerse, se encuentran los siguientes:

- Evidencia o indicios de uso de AV.
- Evidencia o indicios de contactos con plataformas de intercambio de criptomonedas (ya sean PSAV o plataformas P2P), mezcladores, páginas de apuestas online, etc.
- Evidencia o indicios de uso de servicios de almacenamiento en la nube.
- Evidencia o indicios del empleo de herramientas de anonimato (TOR, I2P, VPNs).
- Evidencia o indicios de la utilización de herramientas informáticas de encriptación.
- Claves o contraseñas para el acceso a información almacenada en la nube o para deshabilitar encriptación.
- Evidencia o indicios sobre comunicaciones con otras personas sospechosas (titulares de fondos de origen ilícito, organizaciones terroristas, lavadores de activos, etc.).
- Documentación patrimonial u otra evidencia relevante en formato digital (documentos de constitución de sociedades, registros contables, imágenes o datos sobre activos, agendas, etc.).

319. Esta información o evidencia digital puede encontrarse en un rango cada vez más grande de dispositivos tecnológicos, incluyendo computadoras de escritorio, laptops, tabletas, teléfonos inteligentes, lectores inteligentes (como Kindle), equipos GPS portátiles, cámaras digitales, memorias flash, tarjetas SD, pendrives, discos rígidos extraíbles, servidores externos en la "nube" (como Dropbox, Google Drive, Box.Net, Amazon Cloud Drive) y discos compactos (CDs, DVDs, Blurays); como así también en los dispositivos inteligentes comprendidos dentro de la llamada "Internet de las cosas" (IoT, por sus siglas en inglés)[138]. Por consiguiente, en la medida de lo posible se debe realizar un minucioso análisis forense de todos los dispositivos electrónicos que se secuestren en poder de las personas objeto de investigación[139].

320. Existen distintos elementos que, en caso de ser hallados en un equipo informático, indicarían que su titular usa o ha usado AV. En primer lugar, la existencia de un monedero de criptomonedas. En lo tocante a la principal de estas, Bitcoin, el monedero original es Bitcoin Core, que agrupa a la gran mayoría de los nodos Bitcoin. Una de las principales diferencias entre esta aplicación y otras similares es que Bitcoin Core descarga en el equipo del usuario la Blockchain completa, que ocupa bastante espacio (más de 300 GB)[140]. Otros monederos de AV de uso habitual en computadoras de escritorio incluyen a Exodus, mSIGNA, Electrum, Mycelium, Bitcoin Core, Green Address, MultiBit HD, Armory, Copay y Jaxx. En la actualidad, la mayoría de los monederos son de los denominados "Monederos HD" ("Hierachical deterministic wallets"), en los que todas las claves derivan de una única clave maestra, conocida como la "semilla" ("seed").

321. Los archivos que contienen los monederos suelen identificarse como wallet.dat. A su vez, están representados con íconos identificatorios, como se ilustra en la imagen siguiente, que reproduce los de algunos de los monederos virtuales más populares:

[138] Ver: International Association of Chiefs of Police (IACP): "Data, privacy and public safety. A law enforcement perspective on the challenges of gathering electronic evidence", IACP Summit Report, 2015, pág. 4.
[139] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 15, § 35.
[140] Ver: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 26.

322. Las direcciones de AV que eventualmente se descubran en los monederos en control de las personas sospechosas pueden ser objeto de un análisis de la Blockchain a fin de reconstruir su historial de transferencias, y las direcciones de otros/as usuarios/as con las que se haya vinculado.

323. La existencia de software correspondiente a Videojuegos de rol multijugador masivos en línea (MMORPGs) también puede indicar el uso de AV, desde que dichos programas ofrecen valores virtuales que pueden ser adquiridos para interactuar dentro del juego, como Second Life Linden Dollars, Project Entropia Dollars o World-of-Warcraft Gold[141].

324. Otra fuente de información potencialmente valiosa se encuentra en el historial de navegación de las computadoras o smartphones, el cual puede revelar contactos con PSAV o con plataformas de intercambio P2P de criptomonedas. La presencia de aplicaciones como los "Portfolio trackers" (que ofrecen información actualizada sobre la cotización de las distintas criptomonedas) también indican el uso de AV, así como el registro de visitas a foros de discusión o páginas con información sobre criptomonedas[142].

325. En el caso de los teléfonos móviles, puede verificarse si contienen aplicaciones para autenticación de doble factor vinculadas a monederos online, sean o no en custodia. Es importante verificar, asimismo, la posible existencia de indicios de uso de servicios de almacenamiento en la nube. Vale tener presente, en tal sentido, que los AV no necesariamente deben encontrarse en la computadora personal o el teléfono móvil de la persona investigada, toda vez los monederos -salvo el ya mencionado Bitcoin Core- por lo general ocupan poco espacio (menos de 100 bytes) y

[141] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, pág. 102.
[142] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 18. § 51.

pueden ser almacenados en cualquier dispositivo, como así también en servidores externos. También puede recurrirse a servicios de correo electrónico en la red, algunos de los cuales ofrecen rasgos de privacidad como servicio adicional[143]. El almacenamiento en la nube puede inferirse tanto de la presencia de software asociado a dichos servicios como de registros en el historial de navegación reflejando el uso de los mismos.

326. Por añadidura, en los dispositivos de las personas objeto de investigación pueden encontrarse claves o contraseñas que permitan el acceso a monederos de AV de escritorio o móviles protegidos por contraseñas; a monederos online "en custodia" alojados en páginas que ofrecen ese servicio; a servidores externos de compañías de almacenamiento de datos en la nube; o a documentos encriptados que se encuentren en los equipos informáticos de dichas personas o en cualquier dispositivo de almacenamiento de datos que admita el uso de esa clase de herramientas. Las contraseñas pueden encontrarse en:

- Archivos de texto como Word o Notepad, planillas de cálculo como Excel o incluso como imágenes.

- Aplicaciones para computadoras o teléfonos inteligentes que administran las claves de acceso de los/las usuarios/as, a las que por lo general se accede también mediante una contraseña, que puede ser biométrica (mediante la huella digital o reconocimiento facial).

- En algunos navegadores, que también ofrecen la posibilidad de almacenar contraseñas asociadas al ingreso a páginas web (como las que alojan monederos "en custodia" o brindan servicios de computación en la nube)[144].

327. Por último, el hallazgo de elementos que indiquen empleo de herramientas de anonimato, si bien no constituye, por sí solo, evidencia de actividad criminal, si puede resultar relevante si se sospecha que la persona investigada utiliza dichas herramientas para llevar a cabo maniobras de lavado de activos involucrando AV. En esa dirección, es preciso atender al posible hallazgo de distintos programas[145], a saber:

- Navegadores para la Red oscura, como el sistema TOR, que se utilizan para acceder a servicios ocultos en dicha red como los mercados ilícitos online, en los que los AV son la única moneda de pago aceptada. Estos programas no sólo pueden encontrarse en versión de escritorio (para computadoras) o móvil (para smartphones), sino también en dispositivos -como Tails- en los que el navegador está alojado en un USB que se conecta al equipo

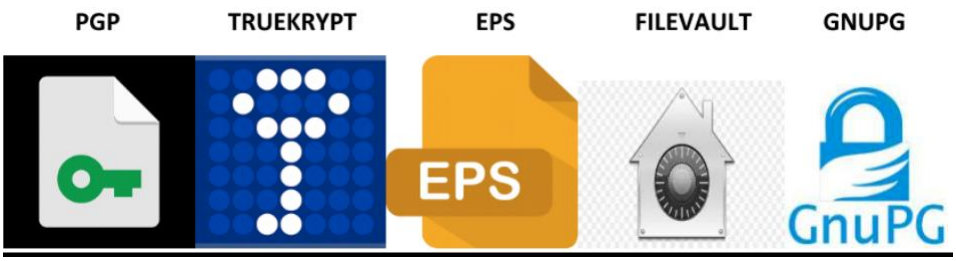
[143] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, págs. 102/103.
[144] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, págs. 103/104.
[145] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, págs. 17/18, §§ 50/51.

cuando se quiere navegar anónimamente y se retira al terminar la sesión, sin que quede ningún rastro de su utilización en la computadora. Debajo, se ilustran los iconos de los navegadores de los sistemas TOR e I2P:

- Presencia o uso de programas para navegación a través de redes privadas virtuales (VPNs, por sus siglas en inglés).

- Presencia o uso de programas de "máquina virtual" ("virtual machine") como VMware Workstation, OrAOPe VM VirtualBox, QEMU, Parallels Desktop, VMware Fusion o Microsoft Virtual PC; que permiten al/la usuario/a albergar un segundo sistema operativo (denominado "guest") dentro de su sistema operativo principal ("host"). Muchas de estas "máquinas virtuales" permiten que la totalidad del contenido se encuentre encriptado, de manera tal que no puede ser ejecutado sin introducir la contraseña. De este modo, la actividad ilícita con AV puede realizarse por entero a través de esta "máquina virtual", sin que exista ninguna evidencia de ello en el sistema operativo principal ("host"), y manteniendo encriptada la evidencia en el sistema operativo paralelo ("guest").

- Presencia o uso de tecnología de encriptación como "Pretty Good Privacy" (PGP) u otros programas similares (como EFS, FileVault, Utimaco, GnuPG, y TrueCrypt, cuyos íconos se reproducen a continuación), que suele ser utilizada por quienes llevan a cabo conductas ilícitas en la Red oscura para comunicarse entre ellos o resguardar información potencialmente incriminatoria.



- Presencia de aplicaciones para borrar los metadatos de archivos.

- Historial de navegación consignando búsquedas de información referida a la navegación en la Red oscura, o tutoriales para el uso de algunos de los programas señalados precedentemente.

F. Técnicas especiales de investigación

328. Sin perjuicio de lo expuesto hasta aquí, en casos en los que los esquemas de criptolavado mediante AV sean especialmente sofisticados, una posible alternativa para obtener información o evidencia que de otro modo no estaría disponible se encuentra en el recurso a técnicas especiales de investigación como la actuación encubierta, siempre dentro del marco de lo permitido por la legislación procesal vigente en cada país.

329. En esa dirección, el GAFI[146] destaca que los mismos programas y técnicas evasivas que utilizan los criminales para llevar adelante en forma anónima sus conductas delictivas en el ciberespacio pueden ser empleados por las AOP para infiltrar organizaciones criminales en la Internet y propiciar una mayor efectividad en el desarrollo de investigaciones patrimoniales sobre maniobras de LA/FT con AV. En efecto, la posibilidad de navegar anónimamente en la Red mediante herramientas como TOR o las VPNs, así como el uso habitual de "identidades alternativas" en el ámbito del ciberespacio, facilita la actuación de "agentes encubiertos digitales" para interactuar en Internet con las personas objeto de investigación y/o potenciales delincuentes, infiltrarse en organizaciones y obtener evidencia que pueda ser utilizada para lograr una condena.

330. La ventaja de las operaciones encubiertas en el ciberespacio, en comparación con las tradicionalmente concretadas en el mundo físico, es que requieren un esfuerzo de planificación, desarrollo y coordinación muchísimo menor, a la vez que reducen considerablemente los riesgos para los/las agentes encubiertos. No obstante ello, es importante tener en cuenta que las herramientas de análisis de la Blockchain también pueden ser utilizadas por los/las criminales, motivo por el cuál si un/a agente va a actuar en forma encubierta en Internet llevando a cabo operaciones con AV, es importante que se genere previamente un historial de transacciones que guarde relación con el "perfil" que va a representar en la Red.

331. Las herramientas de anonimato no son los únicos programas habitualmente usados por los criminales que pueden ser de utilidad también para las agencias de investigación. En los últimos años se ha ido generalizando el uso de programas espías (spyware) o "troyanos" con fines investigativos. Estos pueden utilizarse para concretar distintas medidas útiles para las investigaciones. A saber:

- Acceder remotamente a información o evidencia digital cuya localización física se desconozca o a la que resulte imposible acceder en forma efectiva (por ejemplo, porque no

[146] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, págs. 23/25, §§ 71/76.

podría lograrse el acceso antes de que los datos sean destruidos o alterados por las personas objeto de investigación). A tal efecto, se introduce el software espía en el sistema del/la sospechoso/a y se lo programa para que seleccione los datos relevantes y los envíe a una computadora controlada por la autoridad interviniente.

- Para obtener las contraseñas necesarias para poder acceder al contenido de documentos encriptados, o a información almacenada en servidores externos. Para ello, se utiliza un programa "registrador de teclas" ("keylogger"), el cual registra todo lo que teclea el/la usuario/a del dispositivo en el que se introduce el programa espía (incluyendo las contraseñas que se pretende obtener), tal como ocurrió en el siguiente caso[147]:

Caso 9: Nicodemo Scarfo. Uso de spyware para obtener la contraseña a un archivo encriptado:
En el marco de la investigación seguida en los EE.UU. respecto de dos presuntos jefes de la mafia en New Jersey, Frank Paolercio y Nicodemo Scarfo Jr., el FBI allanó la oficina de este último. Al registrar su computadora, descubrieron un archivo protegido con el programa de encriptación "Pretty Good Privacy" (PGP) a cuyo contenido no pudieron acceder.
Ante la sospecha de que el archivo pudiese contener evidencia relevante, la agencia obtuvo una nueva orden judicial autorizándola a instalar físicamente en la computadora de Scarfo un programa registrador de teclas ("keylogger") durante un mes.
Al término de ese lapso, el FBI volvió a allanar la oficina y secuestró la computadora. A partir del análisis de la información recogida por el programa keylogger, que había registrado todo lo tecleado por los/las usuarios/as del equipo, la agencia pudo obtener la contraseña para acceder al contenido del archivo encriptado, que incluía evidencia sobre la actividad ilícita de Scarfo y su socio y permitió la condena de ambos.

- Para monitorear comunicaciones realizadas a través de la Internet, mediante tecnologías de comunicación que imposibilitan la interceptación por medios tradicionales (sistemas de VoIP, o de mensajería encriptada). En estos supuestos, el programa espía captura los paquetes de datos en los que se transmite el contenido de la comunicación (en formato de texto, audio o video) no cuando están "en tránsito" en la Internet (ya que por lo general estarán encriptados) sino justo antes de que la información salga, o justo después de que ingrese al dispositivo en el que se introdujo el spyware. Así se hizo en el siguiente caso[148]:

Caso 10: Encrochat. Uso de "ataque de cadena de suministro" para infiltración masiva de usuarios de teléfonos celulares encriptados:
En el contexto de una operación de tres años de las autoridades francesas y neerlandesas con respecto a la red Encrochat, utilizada por las principales organizaciones criminales de Europa para comunicarse mediante teléfonos celulares modificados completamente encriptados, la justicia de Francia autorizó la implantación de un virus informático en los servidores de la empresa, localizados en la ciudad de Lille, que luego se descargó en la totalidad de los aparatos en manos de los usuarios (más de 60.000) instrumentalizando las actualizaciones enviadas por la propia compañía (de allí la denominación de "ataque de cadena de suministro").
Una vez instalado en los dispositivos, el spyware envió a la sede central de la agencia de investigación toda la información almacenada en los celulares (correspondiente a las dos semanas previas), así como los mensajes intercambiados de allí en adelante. De ese modo, los investigadores fueron capaces de analizar más de un millón de mensajes, lo que a su vez derivó -tan solo en los Países Bajos- en el arresto de más de 100 personas, el secuestro de 8 toneladas de cocaína, 1.200 kilogramos de metanfetamina y casi € 20 millones en efectivo y el desmantelamiento de más de 19 laboratorios de drogas sintéticas, además de evitar la comisión de homicidios y otros delitos graves.

- Para llevar a cabo vigilancia acústica o audiovisual, utilizando el programa espía para habilitar remotamente los micrófonos o cámaras de dispositivos en poder de (o en las cercanías de) las personas objeto de investigación.

- Para localizar o seguir en tiempo real a las personas objeto de investigación, ya sea programando el spyware para que encienda remotamente los GPS insertos en los dispositivos (por ejemplo, los teléfonos móviles) que dichas personas llevan consigo; o para que, al introducirse en la computadora de la persona objeto de investigación, detecte y transmita a los investigadores la verdadera dirección IP asignada al equipo que utiliza para navegar en Internet. Un ejemplo de esta última modalidad se ilustra en el siguiente caso[149]:

Caso 11: Playpen. Uso de "ataque de abrevadero" para infiltración de múltiples personas sospechosas:
En 2014 el FBI localizó en el estado de Florida los servidores de la página "Playpen", localizada en la Red oscura, dedicada a la distribución imágenes de explotación sexual infantil.
A fin de identificar a los usuarios que descargaban o subían imágenes ilícitas (cuyas direcciones IP no podían conocerse debido al uso del sistema TOR para conectarse con la página), la referida agencia obtuvo autorización judicial para asumir el control y operar Playpen durante un mes, como así también para introducir en la misma un programa espía diseñado para introducirse en la computadora de los usuarios cada vez que uno de ellos subía o descargaba archivos conteniendo imágenes de explotación sexual infantil, y enviar desde allí información incluyendo la verdadera dirección IP, las características del equipo en el que se había introducido y su localización geográfica.
A partir de dicha información, el FBI obtuvo órdenes de registro domiciliario en más de 40 distritos de ese país, en los que secuestraron las computadoras de los/las usuarios/as de la página Playpen, que almacenaban archivos conteniendo evidencia de tenencia y distribución de imágenes de explotación sexual infantil.

332. Si bien en los casos reseñados, el uso de spyware por las agencias policíacas se dio en casos referidos a ciberdelitos tradicionales como la distribución de imágenes de explotación sexual infantil o a causas vinculadas al crimen organizado, también hay ejemplos referidos al recurso a esta herramienta, combinada con otras medidas- en el marco de investigaciones referidas a maniobras de LA con AV[150]:

[149] Fuente: HENNESSEY, Susan: "The elephant in the room: Addressing child exploitation and going dark", Hoover Institution, Stanford University, Aegis Paper Series, N° 1701, 2017.
[150] Fuente: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, págs. 57/58, §§ 198/200.

Caso 12: Caso Mezclador (Países Bajos) ¿Investigación sobre VA con spyware?:
El caso se centró en la actividad de una persona que actuaba como facilitador para criminales en mercados de AV, publicitando servicios consistentes en brindar asistencia para sortear políticas de conozca a su cliente mediante el uso de mezcladores (en particular de Bitcoin, Bitcoin Cash y Litecoin). La persona objeto de investigación decía operar desde Curacao, con una facturación aproximada de 200 millones de U$S (aproximadamente 25.000 bitcoins). Sin embargo, su infraestructura operativa estaba localizada en Europa.
En el transcurso de la investigación se combinaron métodos estándar (como la requisitoria de información patrimonial o la realización de entrevistas, la interceptación de comunicaciones y el secuestro de hardware y otra infraestructura informática) con otros más avanzados, como el uso de técnicas de "intrusión digital".

333. Es probable que uso estatal de programas espía sea considerado como un recurso ajeno a la actividad de las agencias de investigación tradicionales, reservado únicamente a unidades especializadas /en cuestiones de ciberseguridad; o demasiado controversial como para ser aceptado por los tribunales. Lo cierto es, sin embargo, que en atención a la disponibilidad de herramientas tecnológicas avanzadas para actuar anónimamente en la Internet y/o técnicas anti-forenses aptas para impedir la obtención de evidencia digital, resulta imperioso que las AOP adapten sus estrategias y métodos para sostener la eficacia de las investigaciones patrimoniales[151]. Tal fue la recomendación de la Asociación Internacional de Jefes de Policía (IACP, por sus siglas en inglés)[152] en el marco de la cumbre realizada en 2015 sobre la influencia de las nuevas tecnologías en la investigación criminal[153].

334. La concreta implementación del uso estatal de programas requiere de tres etapas: primero, analizar el uso que la persona objeto de investigación hace de las redes, para determinar que plataformas o aplicaciones utiliza (y las posibles vulnerabilidades de dichas plataformas o aplicaciones, que puedan ser explotadas para introducirse en el sistema); segundo, comprometer la plataforma para introducir el "exploit" más apropiado; y tercero, monitorear la información capturada desde el objetivo.

335. La etapa inicial de reconocimiento resulta esencial, toda vez que las herramientas de intrusión informática se diseñan para funcionar con respecto a versiones específicas de una determinada aplicación o sistema operativo. Este reconocimiento se lleva a cabo mediante una variante de las técnicas de OSINT (conocida como "OS fingerprinting") dirigida a recolectar y analizar la información pública que exponen los sistemas al conectarse a un servidor controlado (sistema operativo, versión, navegador, plugins instalados, fuentes instaladas, resolución de

[151] Ver, en tal sentido, lo señalado por el Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations", 2018, pág. 47.
[152] Se trata de la principal organización mundial de jefes de policía, con más de 23.000 miembros en más de 100 países.
[153] Ver: International Association of Chiefs of Police (IACP): "Data, privacy and public safety. A law enforcement perspective on the challenges of gathering electronic evidence", IACP Summit Report, 2015.

pantalla, entre otros). La técnica consiste en el agrupamiento de este conjunto de datos, generando una "huella digital" de dicho usuario, que puede ser de utilidad para identificarlo. La última fase esta etapa de reconocimiento consiste en analizar el sistema del objetivo para descubrir vulnerabilidades y establecer con qué medios defensivos cuenta (firewall, antivirus), para de ese modo elegir los medios de ingreso más aptos para penetrar el equipo en cuestión.

336. El siguiente paso es crucial, en tanto consiste en la introducción del programa informático espía en el sistema o equipo de la persona objeto de investigación, lo que en la actualidad (a diferencia del caso "Scarfo", reseñado precedentemente), se concreta por lo general en forma remota (es decir, sin que medie acceso físico al sistema/dispositivo intrusado). A tal efecto, se han desarrollado distintos métodos para enviar el programa espía y comprometer el sistema informático o dispositivo de la persona objeto de investigación, cuya elección depende de distintos factores (con qué fines se utiliza el spyware, las características de las aplicaciones o sistemas a intrusar, el propósito y naturaleza de la investigación, entre otros). Así, por ejemplo, si se pretende usar el spyware para instalar un "registrador de teclas", o concretar la vigilancia acústica o audiovisual de una persona en particular, puede optarse por un vector de entrada consistente en un mensaje de texto o correo electrónico especialmente diseñado para simular provenir de una fuente conocida, de modo tal de engañar a sus destinatarios/as y lograr que abran un archivo adjunto o hagan click en un link que franquee la entrada del programa espía al sistema (método conocido como "Spear Phishing"). Ello, conforme se ilustra en el siguiente caso[154]:

Caso 13: "Spear phishing". Envío de enlace conteniendo spyware a una persona sospechosa específica: En el marco de una investigación sobre amenazas de bomba a una escuela del estado de Washington, en los EE.UU., la identificación de la persona responsable se vio impedida por la instrumentalización de computadoras "infectadas" mediante un virus informático para el envío de las amenazas.
A fin de sortear dicho obstáculo, la agencia a cargo de la investigación solicitó autorización judicial para introducir un spyware estatal en una falsa noticia periodística elogiando la capacidad técnica de la persona responsable de las amenazas, cuyo enlace fue enviado anónimamente al perfil de la red social Myspace controlada por aquella. Cuando la persona cliqueó la conexión, el programa se introdujo en su computadora y envió información (incluyendo la verdadera dirección IP del usuario) a los investigadores, que de ese modo pudieron establecer que se trataba de un ex alumno de la escuela y arrestarlo.

337. Más recientemente, algunas compañías especializadas en el desarrollo de programas espías para uso estatal han comenzado a ofrecer herramientas más avanzadas, con el sistema denominado "cero clic", que consiste en el envío de un SMS que introduce el spyware al ser

[154] Fuente: MAYER, Jonathan, "Constitutional malware", en Social Sciences Research Network (SSRN), noviembre 2016.

recibido, que no requieren que el individuo objeto de la medida lleve a cabo ninguna acción a tal efecto y ni siquiera aparecen en pantalla, lo cual reduce considerablemente el riesgo de detección.

338. En cambio, si el objetivo de la investigación es identificar a los/las usuarios/as o clientes/as de un mezclador clandestino en la Red oscura, se puede buscar el modo de instalar subrepticiamente el spyware en la propia página, programándolo para que se introduzca automáticamente en los equipos de cualquier usuario/a que lleve a cabo una determinada acción -por ejemplo, concretar una operación de "Coinjoin" o "Chainhopping"- y reporte al servidor de control la verdadera dirección IP del/la usuario/a y otros datos relevantes sobre el equipo, que permitan la identificación de esas personas y su geolocalización. Este método, conocido como "ataque de abrevadero" ("Watering hole attack"), fue el que se utilizó en el caso "Playpen", reseñado precedentemente (caso § 11).

339. Asimismo, para permitir el monitoreo de las comunicaciones efectuadas a través de algunos de los sistemas cerrados de mensajería encriptada que han surgido durante la última década (por ejemplo, EncroChat o Sky ECC), a los que recurren muchas de las principales organizaciones criminales, las agencias policíacas europeas han recurrido a una tercera variante conocida como "ataque de cadena de suministro" ("Supply chain attack"), conforme se detalló más arriba (caso § 10). Este consiste en la introducción del programa espía en los servidores centrales de las compañías que proveen el servicio de mensajería, de modo tal que se distribuya a través de las actualizaciones del sistema a los dispositivos (teléfonos móviles) de todos los/las usuarios/as de la red.

340. A fin de concretar cualquiera de estas variantes de uso de spyware con fines de investigación criminal, es imprescindible que las AOP cuenten con las herramientas informáticas necesarias para llevarlo a cabo. A tal efecto, cada Estado puede optar ya sea por desarrollarlas a nivel interno (mediante recursos humanos especializados propios, que descubran las vulnerabilidades explotables en los principales sistemas o aplicaciones a intrusar y diseñen programas informáticos aptos para aprovecharlas) o adquirir las que ofrecen distintas compañías privadas dedicadas al desarrollo y comercialización de spyware de uso estatal.

341. Al respecto, es importante tener presente que, cuando se trata de utilizar un programa espía en el marco de una investigación estatal, es necesario cumplir con requisitos que no rigen cuando el spyware se usa con fines ilícitos. La primera diferencia reside en que, a diferencia de los ciberdelincuentes, las AOP no pueden emplear un criterio "oportunista" para seleccionar a sus objetivos (centrándose en los más vulnerables a un posible ataque), sino que la herramienta informática que utilizan debe ser capaz de vulnerar el sistema de las personas específicas que son de interés para la investigación. Por añadidura, el spyware estatal debe garantizar un nivel más alto de eficacia que los programas maliciosos comunes, tanto en punto a permitir la obtención de la información buscada sin alertar a la persona objeto de la medida de la existencia del programa,

como en lo referido a la confiabilidad de los datos que se obtengan, de modo que puedan eventualmente ser presentados como evidencia en un proceso criminal.

342. Otra cuestión para considerar en el uso estatal de programas espías es el riesgo de proliferación, entendido como la posibilidad de que las herramientas informáticas a las que recurren las AOP (que por lo general explotan vulnerabilidades desconocidas por las compañías que desarrollaron los sistemas o aplicaciones intrusadas, y contra las que no existe defensa) caigan en manos de actores ilegales, que puedan luego usarlas para perpetrar ciberdelitos[155]. Se trata de un riesgo muy concreto, ya que el uso de spyware supone siempre introducir la herramienta informática en un sistema ajeno, de modo tal que -al menos hasta que termina de cumplir su función y se autodestruye- queda en manos de la/las persona/s objeto de investigación y no de la agencia estatal que lo envió. A fin de reducir este riesgo, el Parlamento Europeo recomienda adoptar medidas tales como la implementación de medidas técnicas para prevenir el redescubrimiento de la vulnerabilidad explotada para introducir el spyware; la notificación a la autoridad que corresponda del descubrimiento (estatal) de una vulnerabilidad y el pedido de autorización para explotarla; y la regulación del uso dual de vulnerabilidades; entre otras[156].

343. A los mismos fines, se recomienda que el uso estatal de spyware se implemente con el método conocido como "lanzador/carga" ("Dropper/payload"). Conforme este método, como "lanzador" se emplea un programa "penetrador", que es el que aprovecha la vulnerabilidad elegida, habilita el acceso al sistema y, una vez logrado ello, deposita una "carga" específicamente encriptada para ese objetivo en particular, que incluye tanto al programa espía propiamente dicho (es decir, el que va a recolectar la información que se pretende obtener) como a la infraestructura de apoyo (mediante la cual se controla el funcionamiento del programa espía y el envío de la información a la base). La "carga" se encripta como medida de seguridad, para garantizar que no sea detectada y reutilizada por criminales; como así también para que sólo pueda activarse en el sistema elegido como objetivo: el "lanzador" la desencripta cuando consigue introducirse en el mismo. A tal efecto, utiliza los datos específicos del objetivo como llave para encriptar y desencriptar la "carga"[157].

344. Esta separación entre el programa "penetrador" y el que funciona como "carga" permite también que las defensas puedan controlar el modo en que se obtuvo la evidencia de cargo en un eventual proceso judicial, sin incrementar el riesgo de proliferación ni comprometer la utilidad futura de la herramienta informática (como ocurriría si se divulgase cómo funciona). En este escenario, el programa "penetrador", que es el más peligroso en términos de proliferación (porque

[155] Este fue el caso, por ejemplo, del virus Wannacry utilizado para concretar un ataque masivo de ramsonware en mayo de 2017, que fue un subproducto de una herramienta informática sustraída en un hackeo a la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) de los EE.UU.
[156] Ver: European Parliament: "Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices", Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, 2017, pág. 26.
[157] Ver: BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan: "Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet", Northwestern Journal of Technology and Intellectual Property, Vol. 12, N° 1, 2014, págs. 1/64.

es el que explota una vulnerabilidad desconocida), se mantiene siempre en reserva, dado que -por otro lado- no interviene en la fase de recolección de la evidencia. Para esto último se usa la "carga", que es el spyware propiamente dicho. Dado que el funcionamiento de este último no requiere de la explotación de una vulnerabilidad, puede ser divulgado sin comprometer su efectividad futura ni aumentar el riesgo de proliferación.

345. A fin de acreditar que la interceptación se llevó a cabo en forma legítima (esto es, conforme lo dispuesto en la orden judicial) es preciso documentar todos los pasos y acciones adoptados para introducir la "carga" dentro del equipo del sujeto investigado. Esto puede llevarse a cabo de distintas maneras: filmando el proceso completo, documentando todos los pasos adoptados en el registro ("log") de la computadora usada para llevar a cabo la intrusión o en un acta, y/o incorporando una declaración testimonial del técnico en la que se detallen las acciones realizadas en cumplimiento de la orden judicial. Además, deben hacerse constar las características del programa usado para llevar a cabo el monitoreo y los cambios que este programa debe efectuar en el sistema a fin de permitir la interceptación y evitar ser detectado. Ello, a fin de demostrar que no se ha destruido ni alterado la evidencia.

346. En los países en los que el uso de spyware no esté expresamente regulado en la normativa procesal, se puede recurrir, para conciliar los beneficios investigativos que ofrece el recurso a esta medida con los derechos individuales de privacidad e intimidad potencialmente afectados por la misma, a las pautas contenidas a tal efecto en la legislación comparada (ver, al respecto, Anexo II). Entre estos, cabe destacar, por ejemplo, a los siguientes:

- Que la autorización judicial especifique: a) los dispositivos y los datos o contenido digital objeto de la medida; b) el alcance de la misma; y c) la forma en que la información relevante va a ser accedida y recogida.

- Que el uso de este método se limite solo a la investigación de delitos graves.

- Que se establezca un proceso de certificación del software utilizado, disponiéndose la posibilidad de verificar su funcionamiento para garantizar la imparcialidad y confidencialidad.

- Que los abogados defensores tengan derecho a obtener la documentación vinculada a las medidas de investigación concretadas mediante programas informáticos y puedan verificar si los programas usados han sido certificados.

- Que se establezca la obligación de desinstalar los programas al terminar su uso.

G. Incautación y decomiso de AV (1): Cuestiones generales y preparación

347. Las particulares características de los AV determinan que su incautación o decomiso, aunque factible, sea considerablemente más difícil que la de bienes tangibles como la moneda fiduciaria. Existen múltiples diferencias entre las AV y los bienes físicos, que impactan en la forma en que debe encararse su incautación o decomiso. En primer lugar, corresponde distinguir según se trate de AV centralizados o descentralizados. En el primer supuesto, en la medida en que su funcionamiento depende de una autoridad administrativa central (la empresa o entidad que desarrolló y opera la moneda), los AV siempre están bajo el control exclusivo de dicha autoridad. Ello facilita la incautación o decomiso, toda vez que existe una autoridad que puede ser objeto de una orden judicial disponiendo la inmovilización o incautación de los fondos. En cambio, cuando se trata de monedas descentralizadas (como las criptomonedas), no existe un banco central o institución similar que pueda inmovilizar los fondos en cumplimiento de una orden judicial.

348. Las transacciones efectuadas con la mayoría de los AV, una vez concretadas, son irreversibles. Esto depende, fundamentalmente, del tipo de moneda virtual de que se trate. Si se trata de monedas centralizadas, los términos y condiciones de uso pueden prever que las transacciones sean revocables, aunque por lo general no lo son[158]. En el caso de las monedas descentralizadas, en cambio, las transacciones son siempre irreversibles una vez que han sido confirmadas en la respectiva Blockchain.

349. El carácter descentralizado de las criptomonedas determina, asimismo, que cualquier persona que tenga la clave privada puede disponer los fondos asociados con la dirección de AV correspondiente a dicha clave. Pueden existir múltiples copias de cada clave privada, almacenadas en distintos lugares y en distintos formatos, y a las cuáles pueden tener acceso diferentes personas. Esta característica impide que pueda adoptarse una medida cautelar que simplemente inmovilice los fondos sin necesidad de que las autoridades tomen posesión de los mismos, como el congelamiento o embargo, toda vez que, mientras las criptomonedas se encuentren en el monedero de la persona sospechosa, incluso si esa persona se encuentra en custodia, cualquier tercero que cuente con la clave puede transferir los AV, de modo irrevocable, a otra dirección.

350. Tampoco resulta suficiente, a los efectos de asegurar los AV, con que las autoridades estatales obtengan la clave privada que otorga control sobre la dirección asociada a los mismos, ya que -como se señaló- cualquier otra persona que tenga en su poder una copia de la misma puede transferirlos. Por la misma razón, para incautar los AV no alcanza con secuestrar la computadora o el dispositivo en el que se encuentra alojado el monedero de criptomonedas, o efectuar una imagen digital del mismo. El único modo de salvaguardar la posibilidad de las autoridades estatales de decomisar los AV es transfiriéndolos a un monedero controlado por ellas a la mayor brevedad

[158] Ver: United Nations Office on Drugs and Crime (UNODC) “Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies”, junio 2014, pág. 42.

posible, de modo tal de evitar que algún tercero sustraiga los fondos antes de que puedan pasar a manos del Estado.

351. En atención a la complejidad potencial de las incautaciones de AV, y sus particularescaracterísticas, se recomienda que las agencias que deban ejecutar esta clase de medidas establezcan de antemano políticas o protocolos internos que regulen la incautación de AV y su tratamiento posterior[159]. En tal sentido, debería preverse, como mínimo:

- La identificación de los/las funcionarios/as autorizados/as para llevar a cabo incautaciones o transacciones con AV;
- El detalle de las notificaciones internas y externas que es preciso efectuar cuando un caso involucra AV;
- Los procedimientos estándar para recolectar y preservar evidencia electrónica; y
- Los protocolos de cadena de custodia que deben regir para todos los dispositivos que puedan contener evidencia electrónica.

352. La incautación o decomiso de AV requiere de considerable preparación previa, más allá del proceso de obtención de las autorizaciones judiciales correspondientes. Consiste en tres etapas básicas: i) planificación previa de la incautación; ii) ejecución de la incautación; y iii) administración de los bienes post incautación[160].

353. En el marco de la preparación previa, se recomienda que, en la medida de lo posible, se determine antes de proceder con qué clase de criptomonedas y monederos opera la persona objeto de investigación[161]. Los monederos son el equivalente de las cuentas bancarias en el ámbito de las criptomonedas. Ofrecen una interfaz de fácil uso para que las personas puedan recibir, almacenar y transferir criptomonedas a otras personas[162]. Son, en esencia, aplicaciones que contienen las claves privadas de una o más direcciones de AV creadas por el/la usuario/a. Con respecto a estos, la primera cuestión a determinar es si los AV que se pretende incautar se encuentran alojados, o no, en un monedero en custodia (en los que el resguardo de las claves privadas requeridas para transferir los AV se encuentra a cargo de un PSAV).

354. Si la respuesta es afirmativa, es preciso averiguar si el PSAV que tiene en custodia el monedero se encuentra registrado y sometido a regulación de ALA/CFT y, en su caso, bajo la

[159] Ver: Regional Organized Crime Information Center (ROCIC): "Bitcoin and cryptocurrencies. Law enforcement investigative guide", Special Research Report, 2018, pág. 10.
[160] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 26, § 81.
[161] Ver: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 22.
[162] Ver: Regional Organized Crime Information Center (ROCIC): "Bitcoin and cryptocurrencies. Law enforcement investigative guide", Special Research Report, 2018, pág. 10.

jurisdicción de qué país. Ello, toda vez que, una vez obtenida esa información, la incautación de los AV puede lograrse mediante una orden judicial que requiera al PSAV inmovilizar los fondos y/o transferirlos a una dirección controlada por las autoridades estatales.

355. En cambio, si los AV que se pretende incautar no están alojados en monederos en custodia, el proceso se dificulta considerablemente, ya que el manejo de los fondos no está en manos de un tercero sino de la propia persona objeto de investigación (y eventualmente también sus cómplices). Por consiguiente, la única forma de concretar la incautación es averiguando la clave privada o las "palabras semillas" que otorgan el manejo sobre los AV o sobre el monedero, respectivamente, para poder transferirlos a un monedero controlado por el Estado.

356. Existen varios tipos diferentes de monederos en los que las claves no están "en custodia". Pueden ser monederos virtuales (software), tanto de escritorio como móviles, o monederos físicos (hardware), en los que las claves están almacenadas en dispositivos portátiles como pendrives, o incluso impresas en papel. Entre los monederos virtuales, los más comunes son los de escritorio, que funcionan como aplicaciones en una computadora. También existen monederos online para los smartphones de IOS o Android, como Mycelium, Greenbits, Breadwallet y Airbitz. Por otro lado, existen monederos híbridos, que son aquellos que están alojados en los servidores de un tercero, pero en los que la custodia de la clave se mantiene en poder del/la titular de los AV. Por último, existen monederos "multi firma", que requieren de la autorización de más de una persona para confirmar una transacción[163].

357. La determinación de con qué clase de AV opera la persona objeto de investigación también es fundamental a los efectos de la incautación y decomiso, toda vez que las criptomonedas sólo pueden ser transferidas a una dirección correspondiente a su propia Blockchain. Así, los bitcoins solo se pueden enviar a una dirección Bitcoin, los moneros a una dirección Monero, etc. En el transcurso de la investigación patrimonial, esta información puede obtenerse de diversas maneras. Por ejemplo, si se investiga la actividad de un vendedor en un mercado ilícito online, el tipo de AV aceptado como pago va a figurar en su perfil. Los datos también pueden obtenerse a través de técnicas de OSINT, análisis de las Blockchain, etc. En la imagen siguiente, se reproducen los íconos de las principales criptomonedas:

[163] Ver: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 14.

358. Asimismo, es importante poder reconocer los diferentes formatos de direcciones de AV de cada criptomoneda. Distintos rasgos de una dirección de AV, como los números, tipo y distribución de los caracteres indican que tipo de criptomoneda se almacena en un monedero. A su vez, si los/las investigadores/as se topan con un formado de dirección desconocido, existen herramientas en la Internet que se pueden utilizar para averiguar de qué tipo de AV se trata. En el cuadro siguiente se detallan las principales características de las criptomonedas más importantes[164].

Tabla 2: Características de las principales criptomonedas:

Nombre	Bitcoin	Ethereum	Ripple	Litecoin	Dash	Monero	Zcash
Abreviatura	BTC	ETH	XRP	LTC	DASH	XMR	ZEC
Inicio de la dirección	1, 3, bc1	0x	r	L	X	4	t1, t3, z1, z3
Extensión de la dirección	26-35	42 hex	34	34	34	95	35 o 96
Comienzo de la clave privada	5, L, K	al azar	s, p	6, T	7, X	al azar	K, L
Extensión de la clave privada	51/52	64 hex	51/52	51/52	51/52	64 hex	51/52

[164] Fuente: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 23.

359. Existen también ciertas "buenas prácticas" en anticipación a un registro que pueda derivar en la incautación de AV[165], que incluyen:

- Estar al tanto de cuando los dispositivos de la persona sospechosa se han conectado o en uso (mediante la determinación de patrones de conducta, monitoreo de red, vigilancia o actuación encubierta, según el caso).

- El monitoreo constante de la actividad de la persona objeto de investigación y del comportamiento de su/s dirección/es de AV.

- Prepararse para la posibilidad de encontrar cuentas que requieran autenticación de doble factor.

- En la medida de lo posible, asegurarse de contar con el acceso a las huellas digitales u otros datos biométricos que permitan el acceso a dispositivos protegidos por ese medio (por ejemplo, teniendo en custodia al titular de dichos dispositivos o contando con autorización para arrestarlo durante el registro y compeler la apertura de los dispositivos).

360. Dada la importancia de la celeridad en la incautación de AV, es importante obtener autorización judicial para llevarla a cabo antes de proceder a la realización de cualquier registro que pueda derivar en el hallazgo del/los monedero/s de la persona objeto de investigación.

361. Asimismo, es importante requerir, también de antemano, autorización judicial para secuestrar, en el transcurso del registro, todos los dispositivos de almacenamiento de datos que puedan encontrarse en el domicilio o las oficinas de la persona sospechosa (discos rígidos extraíbles, CDRs, DVDRs, memory sticks, pendrives, etc.). Ello, toda vez que pueden ser monederos físicos o en su defecto contener información importante en formato digital, como las "palabras semilla" que permiten reconstruir un monedero AV, las contraseñas utilizadas por el usuario para acceder a un monedero híbrido, etc. También para efectuar una imagen forense y que un especialista analice los dispositivos en busca de evidencia relevante[166].

362. En especial, es fundamental contar con autorización judicial para que, en el caso que durante el registro de un domicilio -o el arresto de un sospechoso- se constate que la computadora de aquél o su smartphone o tableta se encuentran desbloqueados y activos, se aproveche dicha circunstancia para analizar su contenido en busca de monederos de AV. Ello así, desde que la oportunidad ideal para concretar la incautación de criptomonedas es cuando el monedero que contiene la/las clave/s privada/s se encuentra abierto, o cuando durante el registro se encuentra la contraseña para abrirlo o la "frase semilla" que permite reconstruirlo. De este modo se evita, asimismo, que el acceso futuro al contenido se vea obstaculizado por la encriptación. Cabe

[165] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 47, § 158.
[166] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 26, § 82.

recordar, en tal sentido, que los smartphones y tabletas de las principales compañías de tecnología (Apple y Google) están equipadas con una medida de seguridad que encripta la totalidad del contenido cuando el equipo se bloquea, mediante una llave criptográfica ligada a la contraseña.

363. En lo referido al contenido de las autorizaciones judiciales vinculadas al procedimiento de incautación de AV, también es importante tener presente que para impedir que mientras éste se está desarrollando, algún cómplice de la persona objeto de investigación transfiera los fondos que se pretende obtener, resulta esencial aislar a esa persona y a todas las demás que se encuentren presentes durante el procedimiento a fin de impedir que se conecten a Internet o puedan tomar contacto con el exterior, hasta tanto se haya concretado la incautación. Por otra parte, la planificación del registro debe tomar en consideración la necesidad de neutralizar, tan pronto como sea posible, toda posibilidad de que la persona objeto de investigación destruya, altere u oculte información útil para acceder al monedero de AV (contraseñas o pins manuscritos, monederos físicos, etc.) antes de que las autoridades lleguen hasta el mismo, transfiera su contenido o de aviso a un tercero para que lo haga por él.

364. Un último aspecto de la planificación previa a la incautación o decomiso consiste en la generación de direcciones AV controladas por la agencia de investigación o autoridad que esté a cargo del procedimiento de conformidad con la legislación local. A tal efecto, se recomienda[167] que las claves públicas y privadas se generen con una aplicación de monedero en una computadora no conectada a Internet[168], y utilizar luego un explorador de Blockchain para verificar que no haya registro de la dirección pública en la misma. Finalmente, la clave pública (no así la privada) debe transferirse de la computadora inicial a una computadora portátil equipada con las aplicaciones necesarias para efectuar una transferencia de AV, que es la que va a llevarse al procedimiento para concretar la incautación.

365. Es necesario tener presente, en tal sentido, que cada tipo de criptomoneda opera con una Blockchain propia y sólo puede ser transferida a una dirección de AV dentro de la misma, motivo por el cual es necesario crear tantas direcciones como tipos de criptomonedas se pretendan incautar. Lo mismo con los monederos, ya que algunos admiten múltiples AV, mientras que otros son exclusivos.

H. Incautación y decomiso de AV (2): Evidencia o indicios relevantes en registros

366. En general, pero sobre todo cuando se investigan posibles maniobras de LA/FT con AV, el propósito de un registro sobre la propiedad de la persona objeto de investigación no debe limitarse a la localización de bienes físicos como dinero fiduciario, joyas, automóviles, etc.; o documentación

[167] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 27/28, § 84.
[168] A tal efecto, la guía elaborada por el Consejo de Europa sobre incautación de AV contiene instructivos detallados sobre el funcionamiento de los principales monederos. Ver: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021.

en papel (información de cuentas bancarias, cheques, documentación referida a transferencias, etc.) para su eventual secuestro o incautación. Por el contrario, los/las investigadores/as deben considerar al registro como una puerta de entrada para obtener información que conduzca al hallazgo de elementos menos evidentes, pero que pueden resultar tanto o más útiles para las investigaciones patrimoniales objeto de esta guía.

367. En efecto, en el transcurso del registro de una propiedad (sea un domicilio, una oficina o incluso automóviles, embarcaciones, etc.), los/las investigadores/as pueden encontrarse con distintos elementos que pueden ser relevantes ya sea como evidencia, como información que conduzca a evidencia o como llave para permitir la incautación o decomiso de AV de origen ilícito. Por ejemplo:

- Computadoras u otros dispositivos que contengan información en formato electrónico, como teléfonos móviles, tabletas, pendrives, discos rígidos extraíbles, etc.

- Monederos de AV, ya sea en formato virtual (como aplicaciones dentro de los equipos electrónicos antes mencionados) o en formato físico, como por ejemplo monederos hardware o de papel.

- Información que permita el acceso a los monederos o la transferencia de AV, como contraseñas o pins para acceder a monederos encriptados o a monederos online alojados en servidores externos, direcciones de AV y -en especial- las claves privadas o "palabras semilla" que son imprescindibles para que pueda concretarse la incautación de monedas virtuales descentralizadas que estén contenidas en monederos que no sean "en custodia".

368. Los monederos de AV son, en esencia, aplicaciones informáticas en las que se almacenan la/las dirección/es AV pertenecientes a una persona y las claves pública y privada asociadas a cada dirección, a la vez que facilitan la transferencia de las criptomonedas mediante una interfaz simple. Los monederos virtuales pueden ser "de escritorio" (para computadoras), "móviles" (para smartphones) u online, que son aquellos cuyo uso se ofrece como servicio y se encuentran almacenados "en la nube" (es decir, en servidores externos). Entre estos, cabe mencionar a Armory, Bitcoin Core, Bitcoin Knots, Bither, Bitpay, Electrum, Wasabi, Mycelium, entre muchos otros. Pueden buscarse en Google Apps o en el App Store de Apple. Los monederos en general están identificados con un ícono en el escritorio de la computadora o la página de inicio del teléfono móvil (ver imagen más arriba, en § 325). De lo contrario, se los puede localizar utilizando el buscador de la computadora para identificar los archivos con la palabra "wallet" o una extensión ".dat" (aunque en algunos casos, el/la usuario/a puede haberlos guardado con otro nombre o extensión).

369. También pueden encontrarse monederos almacenados en un dispositivo físico ("hardware wallets"), como un pendrive. Al igual que los monederos virtuales, el contenido de estos también

suele estar protegido por encriptación, requiriéndose de una contraseña para acceder a las direcciones y claves en formato plaintext. La diferencia fundamental entre los monederos físicos y los virtuales es que los primeros no están conectados a Internet (motivo por el cual se los conoce como "monederos fríos" o "cold wallets"), lo cual le ofrece al/la titular un grado mayor de seguridad frente a un posible hackeo. Los más comunes son KeepKey, Nano Ledger S y Trezor. La imagen siguiente[169] muestra uno de estos monederos físicos.

370. Los monederos "de papel" consisten básicamente en documentos en papel u otro material en que pueda imprimirse información (como madera o metal), en los que se consignan la dirección AV y las claves pública y privada, ya sea en formato plaintext o en forma de código QR, para poder ser "traducidas" mediante un smartphone u otro dispositivo similar. En la imagen siguiente, se muestra un monedero de papel conteniendo las claves tanto en plaintext como en QR:

371. En la siguiente imagen, muestra un monedero papel con códigos QR[170]. A la izquierda esta la dirección Bitcoin, a la derecha la clave privada:

[169] Fuente: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 75.
[170] Fuente: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 101.

372. Si se descubre un monedero de papel, es posible verificar si existen fondos escaneando el código QR y utilizando una aplicación móvil para contrastarlo con la información disponible en la Blockchain de la criptomoneda de que se trate. La misma aplicación puede utilizarse para transferir los AV a un monedero controlado por las autoridades, concretando de ese modo la incautación de los fondos. Esta operación es considerablemente más difícil si el monedero de papel es del tipo encriptado, como el que se ilustra en la siguiente imagen[171]. En tal supuesto, los AV sólo pueden ser transferidos si se cuenta con la correspondiente contraseña.

373. Lo más probable es que los monederos de AV con los que se topen los/las investigadores/as durante un registro estén protegidos por contraseñas (para lograr el acceso), por pins (para habilitar la realización de transacciones) o por ambos. Por consiguiente, resulta fundamental revisar cuidadosamente el lugar objeto de registro -y, en especial, el entorno en derredor de la ubicación de la computadora de la persona investigada- en busca de notas manuscritas, cuadernos, apuntes, agendas, notas autoadhesivas, etc., en los que puedan haberse consignado las contraseñas o pins necesarias para concretar transacciones mediante dichos monederos. En ocasiones, las contraseñas pueden ser obtenidas a través de técnicas informáticas como el análisis de la memoria[172], interrogando a testigos que tengan conocimiento de las mismas o, en su caso, mediante la instalación subrepticia de un spyware "registrador de teclas".

374. Los elementos esenciales para llevar a cabo transacciones con criptomonedas (dirección de AV, clave pública y clave privada) son combinaciones alfanuméricas relativamente extensas y, por ende, difíciles de memorizar. Así, por ejemplo, una persona que use bitcoins debe recordar una

[171] Fuente: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 101.
[172] Fuente: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 23.

"clave privada" que consiste en un código de acceso de 64 dígitos, que por lo general tiene la siguiente forma:

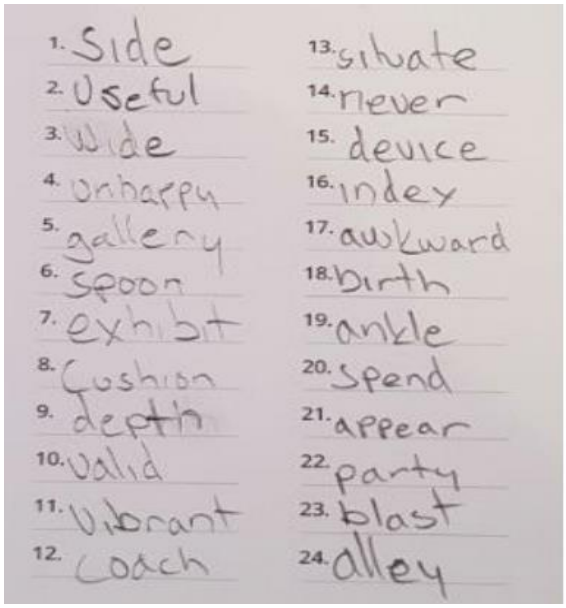
A5373D44C6D87DC0FA6A6738334369F4553213303DA61F20BD67FC233AA37485

375. Dada la complejidad de las claves con este formato, en Bitcoin se generó un algoritmo para simplificarlas (denominado "formato de importación Base 58"), convirtiéndolas en una cadena criptográfica más corta y sencilla, que es la que habitualmente se encuentra en manos de los/las usuarios/as de Bitcoin. Sin embargo, incluso así, las cadenas alfanuméricas utilizadas para operar con esa y otras criptomonedas siguen siendo extensas, tal como se ilustra en la siguiente imagen[173]:

376. Debido a ello, lo más probable es que los/las usuarios/as de AV tomen nota escrita de las claves y las pongan a resguardo en un lugar seguro, como su casa, su oficina o su teléfono móvil. Por ende, es allí donde deben buscar los/las investigadores/as.

377. Si la persona objeto de investigación utiliza un monedero más sofisticado, como monederos HD, la información relevante para el uso incluye a una lista de entre 12 a 36 palabras en distintos idiomas (inglés, japonés, coreano, español, chino, francés e italiano) que conforman un mnemónico (denominadas "palabras semilla" o "frase semilla" ("seed words"/"seed phrase"), en el que se contiene toda la información requerida para la recuperación del monedero en caso de pérdida, daño en el equipo, etc. En la siguiente imagen[174] se ilustra un listado de "palabras semilla":

[173] Allí se ve, en primer lugar, una dirección Bitcoin (Bitcoin adress), a continuación, una clave privada reducida con el algoritmo Base 58 (Private key) y finalmente una clave pública (Public key).
[174] Fuente: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 88.



378. Si durante el registro, los/las investigadores/as encuentran las "palabras semillas", las pueden utilizar para reconstruir el monedero (incluyendo su clave privada) y transferir, por ese medio, los AV a un monedero bajo control estatal, concretando la incautación. El procedimiento es muy simple: se introducen -por ejemplo, en un monedero hardware como el Ledger- las 12 o 24 palabras y al término de la última, se obtiene una copia exacta del monedero original.

379. Es importante tener presente, no obstante, que no todos los monederos siguen los mismos protocolos. Por consiguiente, dependiendo del tipo de monedero de que se trate, su reconstrucción a partir de la frase semilla puede arrojar el mismo resultado que si se accediera al original (la totalidad de los AV contenidos en aquella), o un monedero vacío[175]. Existen aplicaciones que permiten determinar qué tipo de resultado habrá de arrojar la reconstrucción de un determinado monedero mediante la frase semilla.

380. Un dato adicional, de gran utilidad para las investigaciones patrimoniales, que puede llegar a encontrarse durante un registro físico es el "Número de usuario retornante" ("Returning customer number") con el que algunos mezcladores de AV identifican a las personas que utilizan sus servicios más de una vez, a fin de evitar que las criptomonedas de origen ilícito que mantienen en reserva no se paguen dos veces al mismo cliente. A tal efecto, después de cada "mezcla" se le entrega al/la cliente/a un número que debe ser presentado si vuelven a utilizarse los servicios del mezclador, y que le sirve a la plataforma para determinar cuáles AV no usar en el nuevo proceso de mezclado[176]. El hallazgo de este número, si bien no facilita la incautación de las criptomonedas de origen ilícito,

[175] Fuente: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 116.
[176] Ver: Von Wegberg, Rolf / Oerlemans, Jan-Jaap / van Deventer, Oscar: "Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using Bitcoin", Journal of Financial Crime, Vol. 25, N° 2, 2018, págs. 423/424.

si es útil como evidencia del uso de mezcladores, como así también -potencialmente- para identificar al mezclador específico que procesó los AV de la persona objeto de investigación y permitir un eventual rastreo mediante técnicas de "Chain analysis".

I. Incautación y decomiso de AV (3): Ejecución

381. Salvo en los supuestos en los que los AV que se pretende incautar son monedas virtuales centralizadas, o criptomonedas propiamente dichas pero alojadas en un monedero en custodia (en cuyo caso, la medida puede concretarse con la asistencia de la autoridad administrativa central de la moneda centralizada o con la del PSAV que tiene los AV en custodia), en el resto de los casos la incautación de AV comienza con la obtención de las claves privadas, palabras semilla y/o monederos de la persona objeto de investigación.

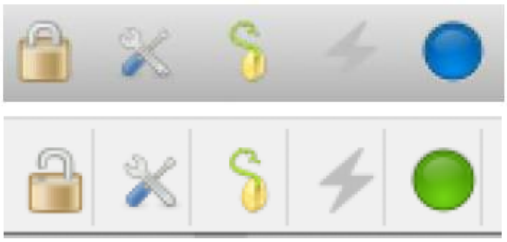
382. Debido a su mayor dificultad técnica, en comparación con la incautación de activos físicos, es preferible que la medida sea llevada a cabo por personal especializado y capacitado, siendo que -además- la celeridad puede ser esencial para garantizar el éxito de la incautación. Por consiguiente, es necesario que quienes concreten la medida estén al tanto de las distintas variedades de monederos de AV existentes y de los mecanismos de seguridad con los que estos cuentan, tales como sub monederos ocultos o la existencia de vías para recuperar el control de la cuenta después de que las autoridades hayan tomado el control de la misma[177] (por ejemplo, a través de las palabras semilla).

383. En atención a la existencia de dichas medidas de seguridad, debe tenerse presente que, en la práctica, el mejor -y en algunos casos, quizá único- modo de concretar la incautación de AV contenidos en un monedero controlado por la persona objeto de investigación es llevándola a cabo mientras el mismo se encuentra desbloqueado y en uso. Ello así, desde que, de lo contrario, el acceso al monedero probablemente requiera del ingreso de una contraseña, y su contenido se encuentre protegido mediante encriptación.

384. A tal efecto, debe procurarse, en caso de ser posible, que el procedimiento dirigido a obtener el control sobre el dispositivo que contiene el monedero se lleve a cabo de forma tal de sorprender a la persona objeto de investigación en el momento en que lo está utilizando. De ese modo se llevó a cabo el secuestro de la computadora de un sospechoso (protegida por una poderosa herramienta de encriptación) en un caso notorio, a fin de garantizar el acceso a su contenido en formato plaintext[178].

Caso § 14: Ross Ulbrich. Captura de dispositivos informáticos mientras están en funcionamiento:
El arresto del responsable del "mercado virtual" Silk Road por el FBI fue cuidadosamente planeado para garantizar el acceso a su laptop, cuyo contenido, según sabía la agencia, estaba protegido por tecnología de encriptación de disco completo cuando se encontraba en reposo.
A tal efecto, y tras averiguar que Ulbrich usaba la computadora en una biblioteca pública, el FBI envió a dos agentes de civil que generaron una distracción en la proximidad del sospechoso, oportunidad que fue aprovechada por otro agente para tomar la laptop mientras se encontraba abierta y en funcionamiento. De ese modo, mientras Ulbrich era detenido, la computadora fue entregada a un técnico especializado que pudo comenzar a analizarla en forma inmediata y acceder a la información contenida en la misma en formato plaintext.

385. A continuación, se ilustran los íconos correspondientes a un monedero bloqueado y encriptado (candado cerrado) o desbloqueado y en uso (candado abierto)[179]:



386. Si durante el registro, los/las agentes intervinientes se topan con el monedero bloqueado y no se logra encontrar la contraseña requerida para acceder, es preciso secuestrar el dispositivo que lo contiene (como se haría con cualquier otro dispositivo que contenga evidencia digital relevante), adoptando las precauciones establecidas en los protocolos sobre tratamiento de prueba electrónica. Posteriormente, y teniendo presente la necesidad de obrar con la mayor celeridad posible, deben adoptarse las medidas investigativas que resulten pertinentes para procurar obtener las contraseñas y concretar la incautación de los AV asociados al mismo.

387. Si ello no resulta posible, por no lograrse el acceso al monedero (o por encontrarlo vacío una vez abierto), una alternativa es la incautación de bienes por valor equivalente[180]. A tal efecto, el carácter público de las Blockchains supone una fuente clave de información, en tanto facilita la determinación del monto preciso de los fondos sustitutos sujetos a decomiso. Ello así, desde que en la misma quedan registradas en forma indubitable la totalidad de las transacciones que involucran AV. Por consiguiente, una vez identificadas la/las dirección/es de la persona objeto de la medida, se puede consultar en la Blockchain el monto exacto de las transacciones efectuadas por dicha persona, incluyendo a las concretadas con fondos de origen ilícito.

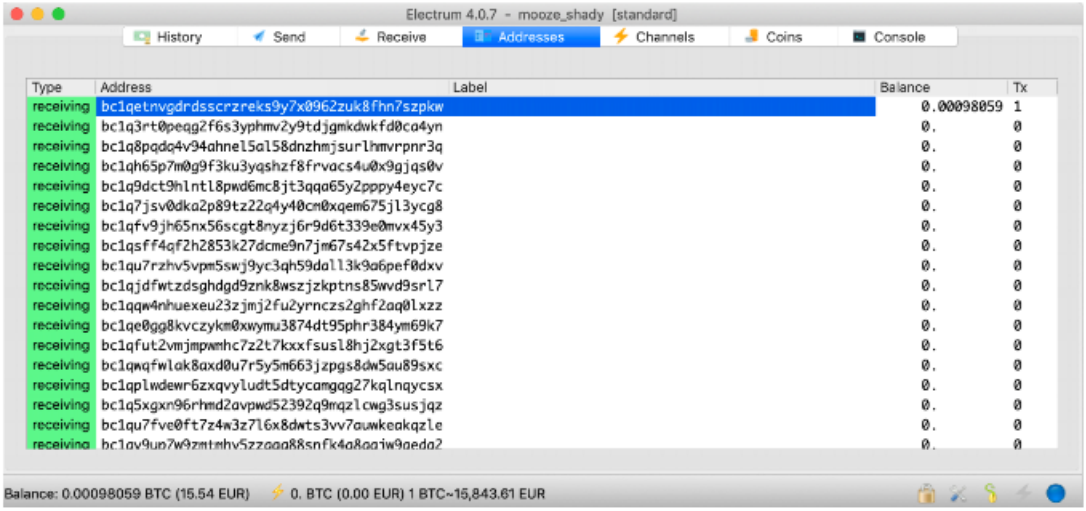
388. Si, en cambio, se encuentra el monedero desbloqueado, debe llevarse a cabo la incautación con la mayor premura posible. Asimismo, en tal supuesto -como en cualquier otro que involucre el acceso a evidencia digital contenida en dispositivos que puedan bloquearse o apagarse por sí mismos- resulta fundamental adoptar los recaudos necesarios

[179] Fuente: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 35.
[180] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, pág. 156.

para asegurar que se mantengan encendidos y en uso, a fin de evitar que vuelvan a bloquearse, entorpeciendo el acceso al monedero o resguardando los contenidos mediante encriptación, como ocurrió en el caso que se detalla a continuación[181]:

Caso 14: "Boucher". Pérdida de acceso a datos por error en la manipulación de una computadora:
El sospechoso Boucher fue aprehendido cuando ingresaba a los EE.UU. desde Canadá, cuando un agente de aduanas revisó la computadora portátil del nombrado, que se encontraba encendida y en uso, y visualizó imágenes de explotación sexual infantil en la misma.
Al momento del arresto de Boucher, la computadora fue secuestrada, momento en el cual los agentes a cargo la apagaron. Debido a ello, cuando se la volvió a encender para analizar su contenido se puso en funcionamiento un programa de protección que lo encriptó en su totalidad, impidiendo el acceso al mismo en formato plaintext en ausencia de la contraseña requerida para deshabilitarlo.
Para poder llevar a cabo el análisis forense del contenido, las autoridades estadounidenses debieron requerir una orden judicial para compeler al detenido a suministrar la contraseña, la que inicialmente les fue negada por considerar que violentaba la prohibición contra la autoincriminación compulsiva. Solo en la instancia de apelación les fue otorgada la autorización solicitada.

389. Por añadidura, los/las agentes/as que tomen parte del procedimiento deben tener presente que un monedero de criptomonedas puede alojar múltiples direcciones (en algunos casos, incluso de diferentes criptomonedas) conteniendo AV potencialmente sujetas a incautación. La imagen siguiente muestra la pantalla de un monedero (para el sistema operativo Windows) exhibiendo múltiples direcciones Bitcoin[182]:



390. Los archivos digitales conteniendo monederos virtuales (de escritorio o móviles) deben ser exportados desde el dispositivo de la persona objeto de investigación con ayuda de una

[181] Fuente: fallo dictado *in re* "Boucher", 2007 WL 4246473, Corte de Apelaciones del Distrito de Vermont, 2009.
[182] Fuente: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 36.

herramienta informática forense. Es preciso efectuar una imagen digital del monedero completo, como así también efectuarse copias o imágenes digitales (según el caso) de las claves privadas o palabras semilla encontradas en documentos de papel o en archivos de texto o Word. A continuación, se las debe importar a la computadora de la agencia de investigación que cuente con el software necesario para llevar a cabo la incautación[183].

391. El paso final consiste en la incautación propiamente dicha, que se concreta cuando se transfieren los AV desde la dirección de la persona objeto de investigación a la controlada por la autoridad competente, a cuyo efecto la computadora utilizada por los/las agentes debe estar conectada a Internet y, en su caso, también sincronizada con la correspondiente Blockchain[184]. Para una mayor eficacia en la concreción de la incautación de AV, se recomienda adoptar una serie de buenas prácticas, incluyendo las siguientes:

- En la medida de lo posible, tener convertidas de antemano la/las dirección/es estatales a formato QR, a fin de evitar errores de tipeo (en especial si se la incautación se concreta con monederos móviles, en los que es más factible cometer errores de ese tipo).

- De lo contrario, se recomienda llevar a cabo un doble o triple chequeo individual de la dirección de destino antes de hacer la transferencia. Con relación a ello, cabe recordar que las transacciones con criptomonedas son irrevocables, de modo tal que, si se envían los AV a una dirección equivocada, no se pueden recuperar.

- Conviene utilizar la función “sweep” de los monederos de AV, que simplemente transfiere el saldo completo del monedero que se está incautando al monedero de destino (en este caso, el que previamente hayan constituido las autoridades que llevan a cabo la incautación).

- A los efectos de mayor velocidad, tanto el GAFI como el Consejo de Europa recomiendan, en sus respetivas guías, establecer la comisión (“fee”) más alta que sea autorizada, a fin de procurar que los mineros de la Blockchain la ubiquen en el bloque más cercano y se concrete más rápidamente.

- Si las direcciones controladas por el Estado se almacenan en monederos de papel, es preciso asegurarse de que no sean visibles las claves privadas, o que sean multi firmas, a fin de reducir el riesgo de sustracción de los AV incautados.

[183] Ver: GAFI: “Guidance on financial investigations involving virtual assets”, junio 2019, pág. 29, § 87.
[184] Ver: GAFI: “Guidance on financial investigations involving virtual assets”, junio 2019, pág. 29, § 88.

- En igual sentido, también resulta fundamental que cuando se elabora el acta o reporte referido al procedimiento de incautación de AV, no se consigne en ningún caso la clave privada o la frase semilla que habilita su transferencia.

- Por último, que una vez concretada la incautación, de todas maneras, se verifique periódicamente el saldo de la/las dirección/es de AV previamente vaciadas, toda vez que puede ocurrir que reciban transferencias o pagos con posterioridad al procedimiento.

J. Incautación y decomiso de AV (4): tratamiento post incautación

392. Durante la etapa posterior a la incautación, existe una serie de consideraciones que deben hacer las autoridades competentes a fin de decidir sobre la conveniencia, o no, de liquidar las AV incautadas o convertirlas a moneda fiduciaria, tales como la necesidad de preservar el valor de las criptomonedas en custodia frente a las fluctuaciones en su cotización, o si existe un uso legítimo en el mercado para la clase específica de AV incautado.

393. A grandes rasgos, existen dos alternativas con respecto al tratamiento de los AV incautados. A saber:

a. **Retenerlos hasta que se dicte la resolución final de decomiso**: en este supuesto, una vez incautados los AV, se encomienda su custodia a una autoridad previamente designada, que los administra hasta que se adopta una decisión final sobre su decomiso y se autoriza su liquidación. La ventaja de esta alternativa es que los AV solo son vendidos una vez dictada la resolución de fondo sobre la condena o absolución de los/las acusados/as, y -por ende- se encuentran disponibles si es preciso devolverlos. La desventaja reside en los riesgos inherentes al mantenimiento de AV, y los costos asociados a ello.

b. **Convertirlos inmediatamente (o en un breve lapso) a moneda fiduciaria**: En sentido opuesto a la alternativa reseñada precedentemente, la ventaja de la presente reside en la reducción de los riesgos de seguridad derivados del mantenimiento de los AV, y de los costos asociados a ello. La desventaja reside en la posibilidad de pérdida de cotización con respecto al momento en que eventualmente deban ser devueltos al/la acusado/a en caso de que se lo/la declare inocente. A nivel regional, la OEA recomienda en general, para todos los activos incautados (virtuales o físicos), proceder a la venta anticipada e invertir los fondos resultantes hasta tanto de dicte la resolución sobre el fondo.

394. En tal contexto, en algunas jurisdicciones (Ej.: Países Bajos), se consulta al titular previo de los AV incautados (es decir, a la persona objeto de investigación) a fin de que se expida por escrito en orden a si prefiere que sean mantenidos en su estado original o convertidos en moneda fiduciaria. De ese modo, si con posterioridad deben ser devueltos, el Estado queda liberado de responsabilidad por una eventual pérdida de valor derivada de las fluctuaciones en la cotización de la/s criptomoneda/s de que se trate.

395. Otra alternativa reside en establecer de antemano (sea a través de una norma o de políticas internas escritas) un plazo fijo para la conversión de los AV incautados en moneda fiduciaria (por ejemplo, tres días), de modo tal que la decisión de concretar dicha conversión no dependa de un juicio sobre su conveniencia en términos económicos, a partir de la cotización de la/las criptomoneda/s de que se trate en un momento dado.

396. Una vez adoptada la decisión de liquidar los AV incautados o decomisados, y de conformidad con lo que establezca la legislación aplicable o a lo que decida la autoridad competente, la venta se puede efectuar en forma directa o a través de una subasta pública, siempre en procura de maximizar el valor obtenido. También se puede arribar a un convenio con un operador privado especializado en el intercambio de AV (es decir, un PSAV) a fin de que tome a su cargo todo lo referido a la conversión de las criptomonedas en moneda fiduciaria. En caso de que las autoridades competentes no cuenten con una estructura confiable en materia de ciberseguridad para el almacenamiento de AV, también se puede encomendar a dicho PSAV la administración de los valores incautados.

397. Algunas jurisdicciones (como, por ejemplo, los EE.UU.), han decidido no liquidar ciertos AV decomisados, cuando consideran que no existen usos legítimos para ellos en el mercado. Tal es el caso de las "monedas privadas" como Monero. En el supuesto de que se opte por obrar de esta manera, es preciso adoptar las medidas de seguridad necesarias para garantizar un almacenamiento permanente eficaz de los AV en cuestión.

398. En esa dirección, se recomienda que los AV incautados sean alojados en monederos de almacenamiento en frío (por ejemplo, un monedero físico, o uno virtual, pero contenido en una computadora no conectada a Internet, o incluso en monederos de papel)[185]. En igual sentido, puede optarse por almacenar los AV incautados en monederos multi firmas, de modo tal que no sea posible sustraerlos obteniendo ilícitamente una única clave privada.

399. Asimismo, se recomienda mantener un listado de las contraseñas para el acceso a cada uno de los dispositivos electrónicos (incluyendo computadoras y teléfonos inteligentes), unidades de almacenamiento externo encriptadas y monederos de AV secuestrados en manos de un/una funcionario/a específicamente designado/a, restringiendo el acceso a los mismos tanto como sea posible. Las frases semillas, contraseñas, claves privadas, pins y direcciones de AV obtenidas pueden ser mantenidas en archivos de texto, en una carpeta designada para cada AV incautado en una unidad de almacenamiento externo (por ejemplo, un disco rígido extraíble), en lo posible encriptados para mayor seguridad. Estas unidades deben mantenerse offline en una locación

[185] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, págs. 31/32, § 99. En esa dirección, la guía elaborada por el Consejo de Europa contiene una explicación detallada sobre el modo de uso de los principales monederos físicos, así como de la elaboración de un monedero papel. Ver: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021.

específica segura hasta que sean requeridos por las autoridades competentes para recibir o transferir AV[186].

K. Enfoque multidisciplinario

400. En atención a la constante evolución de las tipologías de LA/FT y el surgimiento de nuevas tecnologías que facilitan la comisión de dichos delitos, las agencias encargadas de prevenir y perseguir el lavado de activos y la financiación del terrorismo necesitan adquirir conocimientos y capacidades actualizadas con respecto al cibercrimen, las herramientas tecnológicas anti-forenses utilizadas por los criminales y los métodos y técnicas disponibles para contrarrestarlas[187]. Más aun teniendo en cuenta el creciente involucramiento, a nivel mundial, de las organizaciones criminales en la actividad delictiva en el ciberespacio (en todas sus variantes), la cual cobró un notable impulso durante la pandemia global del Covid-19, como lo puso de resalto el GAFI en un reporte publicado en 2020[188].

401. La preponderancia que ha ido adquiriendo el cibercrimen en los últimos años (incluyendo a su correlato en materia de LA/FT, el criptolavado) ha forzado a las AOP a repensar sus estructuras organizativas y operacionales, reforzando el personal de las unidades especializadas en delitos que involucran el uso de TICs y la capacitación en el uso de herramientas informáticas. En tal contexto, las capacidades específicas requeridas para la investigación efectiva de esta clase de delitos determinan que no resulte suficiente con la reubicación del personal existente, incluso si se le brinda entrenamiento adicional: es preciso incorporar nuevo personal que cuente con dichas habilidades, incluso proveniente del sector privado[189].

402. En esa dirección, la Reunión de Ministros de Justicia y otros Ministros y Fiscales Generales de las Américas (REMJA) de la Organización de Estados Americanos (OEA) recomienda que los Estados que aún no lo han hecho establezcan, en el menor plazo posible, unidades o entidades encargadas específicamente de dirigir y desarrollar la investigación y procesamiento de delitos cibernéticos y les asignen los recursos humanos, financieros y técnicos necesarios para el desempeño de sus funciones en forma eficaz, eficiente y oportuna.

403. En particular, la investigación de conductas delictivas que involucran AV requiere de investigadores capacitados, familiarizados con las tecnologías que permiten la identificación, rastreo e incautación de dichos activos. En muchos casos, el personal que cuenta con alguna de

[186] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 32, § 101.
[187] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014. A su vez, el citado organismo se refirió a la problemática de las nuevas tecnologías en relación con la ciber criminalidad en un estudio sobre el tema publicado en 2013 (ver: United Nations Office on Drugs and Crime (UNODC), *Comprehensive study on cybercrime*, 2013).
[188] Ver: GAFI: "LA/FT relacionado con el Covid-19. Riesgos y respuestas", mayo 2020.
[189] Ver: Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations", 2018, págs. 54/56. En igual sentido: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, págs. 61/62.

esas capacidades se encuentra en alguna de las unidades de ciberseguridad existentes en los países de la región, cuyo funcionamiento por lo general no está integrado con el de las unidades o agencias encargadas de investigar maniobras de LA/FT, con o sin AV.

404. Con relación a ello, el GAFI señala que, dependiendo de las particularidades de cada país, es posible que diferentes agencias o autoridades sean responsables de la realización de investigaciones patrimoniales, incautación o decomiso de fondos de origen ilícitos, prevención del LA/FT, combate al cibercrimen y análisis informático forense. Por consiguiente, la cooperación entre todas ellas supone una condición fundamental para el éxito de las investigaciones y procesos penales concernientes a esos delitos[190].

405. En tal contexto, organismos como Interpol, Europol[191] y la UNODC[192], destacan la importancia de un enfoque multidisciplinario en las investigaciones sobre de maniobras de LA/FT con AV. Ello así, toda vez que las mismas demandan una combinación entre técnicas investigativas tradicionales y nuevos enfoques basados en las TICs. Así, los/las agentes especializados/as en investigaciones patrimoniales pueden aportar sus conocimientos sobre fraudes financieros y delitos contables o tributarios, además del conocimiento sobre la actividad de grupos criminales organizados; mientras que las unidades de cibercrimen cuentan con conocimientos relevantes en orden al recurso a herramientas tecnológicas avanzadas y el tratamiento de la evidencia digital. La sinergia entre estas dos categorías de investigadores es esencial para la persecución eficaz del criptolavado, motivo por el cual se recomienda enfáticamente la conformación de grupos multidisciplinarios compuestos por profesionales de ambas áreas[193]. Lo cual responde, a su vez, a lo establecido en la Recomendación 30 del GAFI.

406. Por añadidura, dado que el juzgamiento de delitos que involucren el uso de AV demanda conocimientos específicos, se recomienda que las agencias responsables de investigar esa clase de conductas ilícitas actúen en coordinación con fiscales u operadores judiciales capacitados en la materia, en especial en lo concerniente a la obtención, análisis y tratamiento de la evidencia electrónica y a la incautación y decomiso de AV[194]. A lo que cabe añadir lo tocante al uso de técnicas o herramientas avanzadas de investigación tecnológica, como el Chain analysis, la OSINT, el agente encubierto digital y el uso de spyware, allí donde su utilización se encuentre permitida por la legislación procesal local.

[190] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 45, § 151.
[191] Ver: INTERPOL / Basel Institute on Governance / EUROPOL: "Recommendations. 4th Global Conference on Criminal Finances and Cryptocurrencies", noviembre 2020, pág. 3.
[192] Ver: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014, pág. 67.
[193] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 17, § 49.
[194] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 44, § 150.

L. Cooperación internacional

407. El carácter trasnacional de la Internet y el ecosistema de los AV convierte a la cooperación internacional en un elemento esencial de las investigaciones patrimoniales referidas a las conductas delictivas asociados con aquellos. A fin de que dichas investigaciones puedan arrojar resultados satisfactorios, es preciso utilizar todos los canales (formales e informales) de colaboración en forma efectiva y, por, sobre todo, oportuna. Esto último, en atención a la importancia de la celeridad para permitir la preservación de la evidencia digital, ya que ésta a menudo es eliminada en forma rutinaria como consecuencia de procedimientos automatizados.

408. En este escenario, se recomienda que las agencias o autoridades responsables de investigar maniobras de LA/FT con AV utilicen todas las vías que estén a disposición para conectarse con sus pares en el extranjero[195], incluyendo a mecanismos de cooperación entre agencias policíacas (INTERPOL, EUROPOL); puntos de contacto para el intercambio de información vinculada a la incautación y decomiso de activos de origen ilícito (RRAG, CARIN, redes ARIN, StAR y GFPN); puntos de contacto para el intercambio de información vinculada al cibercrimen (Portal Interamericano de Cooperación en Delitos Cibernéticos y Red de contactos 24/7 del G-7); canales para la cooperación jurídica internacional como IberRed; redes de intercambio de información de inteligencia financiera recopilada por las UIF (Grupo Egmont); así como pedidos de asistencia legal mutua.

409. El GAFI[196] destaca la importancia de explotar las herramientas de cooperación internacional con el máximo alcance posible, en especial la posibilidad de requerir medidas de preservación de evidencia digital como las previstas en los instrumentos internacionales sobre cibercrimen reseñados en el apartado § IV.6 de esta guía, a efectos de impedir la pérdida de pruebas relevantes o la fuga de activos que puedan estar sujetos a decomiso. Si bien, en contraste con la celeridad que requieren las investigaciones referidas a actividad ilícita en el ciberespacio, el recurso a herramientas de cooperación jurídica como los pedidos de asistencia legal mutua puede resultar excesivamente lento o engorroso, existen vías para maximizar los resultados posibles. En tal sentido, se recomienda establecer contacto directo con autoridades en la contraparte extranjera que estén familiarizadas con la cuestión objeto del pedido de cooperación (investigaciones por actividad ilícita con AV) y -en general- con la problemática de la evidencia digital, así como el establecimiento de canales informales de comunicación con agencias similares en otros países para facilitar la colaboración.

410. En lo referido a la materia objeto de la presente guía, la RRAG constituye una herramienta fundamental para identificar bienes y personas en el extranjero que puedan ser relevantes en el marco de una investigación sobre maniobras de LA/FT mediante AV y para tomar conocimiento

[195] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 46, § 156.
[196] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 46, § 154.

de procesos penales en trámite en otros países. A tal efecto, pueden requerirse a través de la plataforma segura de la red datos de carácter general, social, tributario, patrimonial y financiero, ya sea a fin de enriquecer la información con la que cuentan los/las investigadores/es en el país requirente, o para facilitar la confección de pedidos de asistencia jurídica internacional con datos precisos, aumentando así las oportunidades de éxito.

411. La RRAG cuenta con 48 puntos de contacto de 22 países con acceso directo a la plataforma RRAG segura de fiscalías, policía, UIF y otras autoridades de orden público. La referida plataforma permite intercambiar información entre los países de la RRAG y las 54 jurisdicciones que pertenecen a la Red CARIN. Adicionalmente, los puntos de contacto de la RRAG pueden acceder, mediante dicha red, a información en poder de otros organismos internacionales vinculados a la incautación de activos, como la Red Interinstitucional para la Recuperación de Activos de Camden (CARIN), la Red Global de Puntos de Contacto sobre Recuperación de Activos (GFPN) y la Iniciativa de Recuperación de Activos Robados (StAR) de Interpol. Asimismo, también se puede acceder, por dicha vía, a la información recolectada por las redes ARIN en todo el mundo, que incluyen a la Red Interinstitucional para la Recuperación de Activos de Asia del Pacífico (ARIN-AP) y Asia Central y Occidental (ARIN-WCA); la Red Interinstitucional para la Recuperación de Activos del Caribe (ARIN-CARIB), la Red Interinstitucional para la Recuperación de Activos de África Oriental (ARIN-EA), del Sur de África (ARIN-SA) y de África Occidental (ARIN-WA)[197].

412. Por otro lado, en el seno de la OEA, la Secretaría Técnica de la Reunión de Ministros de Justicia y otros Ministros y Fiscales Generales de las Américas (REMJA) tiene a su cargo el Portal Interamericano de Cooperación en materia de Delito Cibernético, creado en 1999, cuyos fines son fortalecer la cooperación internacional en la prevención, investigación y enjuiciamiento de los delitos cibernéticos; facilitar el intercambio de información y experiencias entre sus miembros y realizar las recomendaciones necesarias para mejorar y fortalecer la cooperación entre los Estados miembros de la OEA y con organismos internacionales y mecanismos.

413. A su vez, la Secretaría Técnica de las REMJA (Departamento de Cooperación Jurídica de la Secretaría de Asuntos Jurídicos de la OEA) mantiene un directorio actualizado de las autoridades de persecución penal y de policía que sirven como puntos de contacto para la cooperación internacional en materia de delito cibernético y evidencias electrónicas.

414. En lo tocante a la cooperación internacional en materia de cibercrimen (incluyendo el criptolavado mediante AV), en las REMJA se recomendó a los países miembros fortalecer los mecanismos que permitan el intercambio de información y la cooperación con otras organizaciones e instancias internacionales en materia de delito cibernético, tales como las Naciones Unidas, el Consejo de Europa, la Unión Europea, el Foro de Cooperación Económica Asia-Pacífico (APEC), la

[197] Ver: RRAG/GAFILAT: "Inventario de redes existentes a nivel global para la identificación y recuperación de activos productos del delito", junio 2021.

Organización para la Cooperación y el Desarrollo Económicos (OCDE), el G-7, el Commonwealth y la INTERPOL, de manera que los Estados Miembros de la OEA puedan aprovechar los desarrollos dados en dichos ámbitos. Se exhortó, asimismo, a los estados que todavía no lo hicieron a vincularse, en el menor plazo posible, a la "Red de Contactos sobre Delitos de Alta Tecnología 24 horas/7 días" del G-7.

415. En ese orden de ideas, en el marco de la REMJA XI se concluyó que las nuevas tecnologías de la información y la comunicación (TICs) resultan instrumentos útiles para fortalecer la cooperación jurídica internacional en las diversas ramas del derecho y constituyen medios idóneos para facilitar a los Estados establecer mecanismos de contacto, colaboración y coordinación entre las distintas autoridades que tienen a su cargo la tramitación de solicitudes de cooperación jurídica y asistencia recíproca en las distintas áreas del derecho. En atención a ello, se recomendó a los Estados miembros adoptar las medidas necesarias para potenciar el uso de las nuevas TICs, como el trámite electrónico de solicitudes de asistencia jurídica mutua, incluida la aceptación de documentos oficiales con firmas electrónicas o digitales, y las videoconferencias, de modo seguro y responsable, para hacer más efectiva, eficaz y ágil la cooperación jurídica internacional en las Américas.

M. Capacitación y entrenamiento

416. La investigación sobre el uso ilícito de AV involucra el análisis de tecnologías complejas y, por consiguiente, demanda el desarrollo de técnicas investigativas novedosas y la adquisición de nuevos recursos y capacidades. Dado que, por lo general, los actores ilícitos tienden a adaptarse a un contexto cambiante con mayor rapidez que las autoridades, es esencial adoptar los pasos necesarios para que las AOP adquieran los niveles de competencia requeridos para poder investigar con éxito la explotación de los AV con fines criminales[198].

417. A tal efecto, es necesario implementar programas de capacitación dirigidos al rango más amplio posible de personal, a fin de que adquieran los conocimientos mínimos necesarios para llevar a cabo -o, cuanto menos, no comprometer- las investigaciones patrimoniales referidas al uso ilícito de AV.

418. En tal contexto, hay tres categorías de capacitación relevantes para procurar la adaptación de las AOP al nuevo escenario tecnológico[199]. A saber:

a. **Entrenamiento para investigadores** con respecto a las nuevas tecnologías involucradas en las investigaciones patrimoniales sobre el uso ilegal de AV;

[198] Ver: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 64.
[199] Ver, en lo pertinente: Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations", 2018, pág. 59.

b. **Entrenamiento para agentes de policía en general** sobre como reconocer y reaccionar ante la existencia de evidencia digital relevante para esa clase de investigaciones; y

c. **Entrenamiento para investigadores forenses**, en lo tocante a las nuevas tecnologías en juego.

419. En lo referido a la primera categoría, si bien no hace falta que todo el personal dedicado a la investigación se especialice en el uso de AV, si es preciso contar con un número de expertos (proporcional al tamaño de la jurisdicción) que esté capacitado para reconstruir una cadena de transacciones en la Blockchain y/o para incautar o decomisar AV. El resto del personal solo debe contar con los conocimientos mínimos necesarios para reconocer indicios sobre el posible uso de criptomonedas si se topa con ellos en el transcurso de una investigación o al llevar a cabo un registro, así como estar al tanto de como contactar a los/las agentes especializados/as en la materia dentro de su jurisdicción[200].

420. En tal contexto, es importante que un número suficiente de agentes reciba entrenamiento en el uso de las herramientas forenses para la trazabilidad de AV que se encuentran disponibles en el mercado, o en su defecto de las que desarrolle internamente cada país, si decide hacerlo[201]. Ello, toda vez que la participación de agentes que carezcan de la preparación adecuada en estas tareas genera el riesgo de que se interprete en forma errónea la información disponible en la Blockchain, lo cual puede derivar en que se terminen persiguiendo pistas falsas o se pasen por alto datos realmente relevantes[202].

421. De igual manera, es vital que la incautación de AV sea realizada por personal especializado, para evitar errores que puedan conducir a la perdida de los fondos. Por consiguiente, las autoridades relevantes (ya sea que se trate de agencias policíacas o de las fiscalías competentes) debe estar capacitada para manejar las distintas clases de monedero de AV que pueden llegar a utilizarse en estos procedimientos, así como acerca de las cuestiones de ciber seguridad inherentes a la administración de los activos incautados.

422. Sin perjuicio de ello, ante la posibilidad de que agentes no pertenecientes a unidades especializadas se topen con criptomonedas en cumplimiento de órdenes de registro, etc., es preciso que el personal de las AOP que pueda potencialmente encontrarse en dicha situación sepa reconocer cuanto menos los rasgos más importantes del uso de AV. (códigos QR, frases semillas, claves públicas o privadas, diferentes formatos de dirección de criptomonedas y distintos tipos de

[200] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 42, § 139.
[201] Ver: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 65.
[202] Ver: GAFI: "Guidance on financial investigations involving virtual assets", junio 2019, pág. 25, § 79.

monederos, contraseñas, pins, etc)[203]. Como así también que, en un plano más general, sean capaces de reconocer dispositivos que puedan contener evidencia digital[204].

423. Las acciones tendientes a brindar esta capacitación son variadas, comprendiendo la organización de programas de entrenamiento, la elaboración de manuales, programas de intercambio y/o participación en conferencias o seminarios internacionales. En esta dirección, y a fin de ampliar al máximo posible el alcance de los conocimientos sobre AV entre el personal de las fuerzas de seguridad, resulta recomendable distribuir material de consulta (folletos, instructivos) que contenga un detalle páginas o aplicaciones referidas a AV, plataformas de intercambio, procesadores de pagos y proveedores de servicios de monederos de criptomonedas, imágenes de frases semillas, códigos QR, monederos papel o hardware y cajeros de AV, etc.

424. Finalmente, se recomienda también la implementación de instancias de cooperación público-privada con actores del sector privado especializados en estas nuevas tecnologías, dirigidas a procurar que las AOP y las unidades del MPF con competencia en la materia se mantengan actualizadas con respecto a los nuevos desarrollos en dicho ámbito[205].

[203] Ver: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021, pág. 21.
[204] Ver: Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations", 2018, pág. 60.
[205] Ver: INTERPOL / Basel Institute on Governance / EUROPOL: "Reccomendations. 4th Global Conference on Criminal Finances and Cryptocurrencies", noviembre 2020, pág. 2.

ANEXO I: PAUTAS PARA INVESTIGACIÓN, IDENTIFICACIÓN, INCAUTACIÓN Y DECOMISO DE ACTIVOS VIRTUALES

A. CONCEPTOS BÁSICOS

1. **Activo virtual (AV):** Conforme la definición del GAFI, es una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar para pagos o inversiones. Los AV no incluyen a las representaciones digitales de moneda fiduciaria, valores y otros activos financieros que ya están comprendidos en otros tramos de los estándares del organismo.

2. **Dinero fiduciario:** alude a la moneda o dinero real (no virtual), o moneda nacional. Se diferencia de la moneda virtual porque éste funciona como la moneda y el papel moneda de un país, designado como dinero de curso legal; que circula, se utiliza y acepta como medio de intercambio en el país emisor.

3. **Criptomonedas:** son AV de código abierto, convertibles y descentralizados, que funcionan en una red de pares distribuida que aplica principios matemáticos y criptográficos para dotar de seguridad al sistema. Las transferencias entre los/las usuarios/as se llevan a cabo "par a par", sin intermediarios, a partir del juego de claves criptográficas públicas y privadas, y requieren de ser firmadas criptográficamente para concretarse. La transparencia del sistema se garantiza mediante el registro de las transacciones en una suerte de "libro mayor" distribuido (denominado Blockchain en la mayoría de las criptomonedas), llevado por una red de partes mutuamente "desconfiadas" (llamadas "mineros" en el ecosistema del Bitcoin y otras criptomonedas) que elaboran los bloques criptográficos de la cadena y son recompensados por ello con tarifas pagadas por los/las usuarios/as.

Iconos de las principales criptomonedas:

4. **Bitcoin**: lanzado en 2009, fue el primer AV convertible descentralizado, y la primera criptomoneda. Los bitcoins son unidades de cuenta compuestos de secuencias

alfanuméricas únicas que constituyen unidades de moneda (divisibles, a su vez, en unidades más pequeñas, llamadas Satoshis) y que tienen valor sólo porque usuarios individuales están dispuestos a pagar por ellos. Los bitcoins se comercian digitalmente entre los usuarios en forma parcialmente anónima (las personas o entidades que intervienen en cada transacción se identifican solo con pseudónimos alfanuméricos llamados "Direcciones Bitcoin" -Bitcoin adresses-) y pueden ser intercambiados por moneda fiduciaria o por otras criptomonedas. El software requerido para enviar, recibir y almacenar bitcoins o para monitorear las transacciones puede ser descargado gratuitamente. Los/las usuarios/as también pueden obtener sus direcciones Bitcoin (que funcionan como cuentas) en plataformas de intercambio de Bitcoin o en servicios de monederos online. Las transacciones (flujos de fondos) se consignan en un registro público compartido (la cadena de bloques o "Blockchain"), en el que se las identifica por medio de las direcciones Bitcoin.

5. **Dirección de AV o de criptomonedas (Ej.: dirección Bitcoin):** es un código alfanumérico que identifica el lugar virtual asociado a una determinada cantidad de AV, necesario para poder enviar o recibir criptomonedas. Funciona como una cuenta bancaria en el sistema financiero tradicional, para recibir o enviar transferencias. Por ejemplo, las direcciones Bitcoin tienen una longitud de entre 26 y 32 caracteres. Empiezan por el número 1 para direcciones estándar y por el número 3 para las direcciones de multi firmas. Otras criptomonedas tienen sus propios sistemas para representar sus direcciones. Las direcciones de AV también pueden representarse por medio de códigos QR.

6. **Blockchain:** es una forma de registro o "libro mayor" utilizada por Bitcoin y la mayoría de las criptomonedas, y funciona encadenando bloques de datos. Cada uno de estos bloques contiene información acerca de la operación que se están realizando. Los elementos iniciales y finales del bloque se relacionan, respectivamente, con el bloque anterior y posterior. De este modo, la modificación del bloque corrompería la cadena al completo, aunque es prácticamente imposible su alteración. Además, la tecnología basada en cadenas de bloques funciona de modo distribuido, con múltiples computadoras que operan simultáneamente con la cadena, lo cual hace extremadamente difícil comprometerla mediante un ataque informático. Cada criptomoneda tiene su propia Blockchain.

7. **Clave privada ("private key")**: es un número aleatorio que funciona como clave secreta, generado a través de un proceso de criptografía asimétrica, y se utiliza para resguardar la propiedad y el manejo de las criptomonedas. Durante el proceso de creación de un monedero de AV, la clave privada se genera en primer término y luego, a partir de ella, la clave pública, que está relacionada matemáticamente con la anterior. El proceso, sin embargo, es imposible de concretar en sentido inverso (deduciendo la clave privada a partir de la pública), lo cual brinda un alto nivel de seguridad. La clave privada es la que asigna al/la titular el control de los fondos asociados a una determinada dirección de AV.

8. **Monederos (Wallets) de criptomonedas:** son aplicaciones de software que permiten interactuar con la Blockchain de las AV a fin de generar y/o almacenar las direcciones de criptomonedas y sus correspondientes juegos de claves público/privada. Es una interfaz que permite a los/las usuarios/as administrar, transferir o recibir AV. Existen varias clases de monederos de AV.

9. **Monederos alojados o en custodia (Hosted / Custodial wallets):** son monederos virtuales que están alojados en un servidor externo (es decir, en "la nube"), y se ofrecen a través de proveedores de servicios de monedero de AV. Su denominación refiere a que las claves privadas no están en poder del/la titular de las AV, sino "en custodia" del prestador del servicio.

10. **Monederos no en custodia o auto alojados (Self-custody / Self Hosted)**: son los monederos que los/las propios usuarios/as de criptomonedas mantienen en su poder, para uso propio de los AV asociados a las direcciones almacenadas en los mismos. Estos monederos pueden ser virtuales o físicos.

11. **Monederos virtuales (Software wallets)**: son aplicaciones descargables, de escritorio o móviles, que pueden mantenerse en una computadora de escritorio o en un dispositivo móvil (un teléfono inteligente o smartphone) para permitir el almacenamiento seguro de las claves en el dispositivo.

12. **Monederos físicos (Hardware wallets)**: son aplicaciones de monedero alojadas en dispositivos físicos como pendrives o USBs, que le permiten al/la usuario/a almacenar sus claves offline, en dispositivos físicos portátiles como pendrives.

13. **Monederos de papel (paper wallets)**: se trata de planchas de papel o de otro material en el que se imprimen, mediante un programa de monedero de AV, las direcciones de criptomonedas y el juego de claves pública/privada con las que se gestiona el intercambio de criptomonedas, ya sea en formato plaintext o en forma de código QR. Se recurre a los mismos para el almacenamiento y resguardo de fondos que no van a ser utilizados o movidos en mucho tiempo, ya que ofrecen un nivel mayor de seguridad, al no ser susceptibles al robo cibernético.

14. **Las "palabras semilla" o "frase semilla" ("Seed words" o "Seed phrase")**: son utilizadas por muchas aplicaciones de monedero de AV para generar claves privadas a partir de una única "semilla", que toma la forma de un mnemónico conformado por una secuencia de entre 12 y 24 palabras en distintos idiomas (inglés, japonés, coreano, español, chino, francés e italiano), que funcionan como un respaldo (back up) para el monedero, permitiendo que en caso de pérdida de control sobre el mismo (por ejemplo, debido al robo, pérdida o desperfecto técnico del dispositivo en el que se encuentra almacenada), sea posible recrearlo introduciendo en la aplicación correspondiente las palabras en el orden provisto originalmente.

15. **Proveedores/as de servicios de activos virtuales (PSAV)**: conforme la definición del GAFI, comprende a cualquier persona física o jurídica (no alcanzada por otra definición dentro de las recomendaciones del citado organismo) que, como negocio, lleve a cabo una o más de las siguientes actividades u operaciones para / en nombre de otra persona física o jurídica:

a. intercambio entre activos virtuales y moneda fiduciaria;

b. intercambio entre una o más formas de AV;

c. transferencia de AV;

d. custodia y / o administración de AV o instrumentos que permitan el control sobre AV; y

e. participación y provisión de servicios financieros relacionados con la oferta de un emisor y / o venta de un AV.

16. **Plataformas de intercambio de AV / criptomonedas (cryptocurrency exchanges)**: son las operadas por personas o entidades que se dedican comercialmente al intercambio de criptomonedas por moneda fiduciaria, fondos, metales preciosos u otras criptomonedas (o viceversa), a cambio de una tarifa (comisión). Por lo general aceptan una amplia variedad de métodos de pago (efectivo, transferencias, tarjetas de crédito u otras criptomonedas) y son utilizados para depositar o extraer fondos de cuentas de AV. Están comprendidos en la definición de PSAV del GAFI.

17. **Mezcladores (Mixers)**: Son plataformas que ofrecen a los/las usuarios/as de criptomonedas la posibilidad de oscurecer la cadena de transacciones en la Blockchain mediante el recurso a herramientas informáticas de anonimato que vinculan múltiples transacciones a una única dirección de AV y las envían en conjunto de un modo que hace aparecer como que provienen de una dirección diferente. El mezclador o conmutador (Tumbler) interviene cuando recibe la instrucción del/la cliente de enviar fondos a una determinada dirección. A fin de ocultar el origen y destino de dicha transacción, el mezclador la combina con una serie compleja y semi-aleatoria de transacciones ficticias, de modo tal de impedir que la transferencia al destino final pueda ser asociada con la dirección de origen.

18. **TOR (The Onion Router)** es una red distribuida de computadoras en la Internet que se utiliza para ocultar las verdaderas direcciones IP (y, por consiguiente, la verdadera identidad) de los/las usuarios/as, enrutando las comunicaciones a través de múltiples nodos (elegidos aleatoriamente para cada comunicación) en todo el mundo y resguardando los paquetes de datos que indican el origen y destino de la comunicación en varias capas de encriptación.

19. **Servicios ocultos (Hidden services)**: son páginas web localizadas en la "Red oscura", a las que sólo puede accederse mediante el uso de sistemas de comunicación anónima como TOR. Ello impide que su verdadera ubicación (dirección IP) pueda ser identificada, toda vez que se encuentra enmascarada por el enrutamiento "en capas" provisto por el TOR. La comunicación entre estas páginas y sus usuarios/as tiene lugar a través de un "punto de encuentro" ("rendezvous point") que ofrece una capa adicional de protección frente al análisis de tráfico.

20. **Encriptación:** es un método de cifrado de datos que consiste en codificar los contenidos usando una fórmula o algoritmo matemático que los desordena, de manera tal que si no se cuenta con la correspondiente clave (denominada "llave criptográfica") aquellos lucen como un conjunto de caracteres alfanuméricos sin sentido ni lógica de lectura.

21. **Análisis de la Blockchain (Chain analysis):** es el proceso de inspección, identificación, segmentación y elaboración de modelos para la representación visual de los datos públicos contenidos en la Blockchain, a fin de obtener información útil sobre quienes llevan a cabo transacciones con criptomonedas. Este análisis por lo general es llevado a cabo por compañías privadas que utilizan algoritmos propios para mapear los gastos efectuados por los/las usuarios/as de criptomonedas y vincular a unos con otros.

22. **Inteligencia de fuente abierta (Open Source Intelligence u OSINT)**: denominación que alude a la recolección, procesamiento y análisis sistemático de información de acceso abierto. Esto es: la información disponible para el público en general sin restricciones (en redes sociales, páginas web, buscadores, portales de noticias, registros públicos, etc.).

23. **Spyware:** es un tipo de malware (programa malicioso) diseñado para funcionar en forma subrepticia dentro de un sistema informático y registrar información en secreto. Puede supervisar y copiar los que se escribe ("registrador de teclas" o "keylogger"), lo que ingresa o egresa del sistema, capturar la información almacenada o incluso activar los micrófonos o cámaras del equipo.

24. **Evidencia electrónica (o digital):** es la información generada, almacenada o transmitida mediante dispositivos electrónicos que puede ser utilizada como prueba ante un tribunal.

B. INVESTIGACIÓN E IDENTIFICACIÓN DE ACTIVOS VIRTUALES

25. Las agencias que lleven a cabo investigaciones patrimoniales sobre maniobras de LA/FT con AV deben tener a su disposición el rango más amplio posible de información, ya sea a partir de fuentes propias, del intercambio con otras autoridades nacionales o de la cooperación con terceros (por ejemplo, en el ámbito privado). La información debe incluir:

- Información recolectada por las AOP respecto de personas objeto de investigación por presunta actividad ilícita en la Dark Web; sus pseudónimos o alias; direcciones de criptomonedas o cómplices conocidos (y sus pseudónimos o alias); arrestos o condenas previas; direcciones físicas o electrónicas, números de teléfono o direcciones de correo electrónico que hayan podido utilizar en conexión con actividad delictiva.

- Información proveniente de los sujetos obligados a cumplir tareas de ALA/CFT, incluyendo tanto la proveniente de reportes de operación sospechosa (ROS), como la obtenida en el marco de las políticas de "conozca a su cliente" (KYC). Esta incluye a registros de transacciones realizadas mediante PSAV, o de PSAV con entidades financieras tradicionales, o cualquier otra actividad patrimonial que pueda generar sospechas sobre el posible uso de AV para reciclar fondos de origen ilícito.

- Información de entes regulatorios como los bancos centrales, autoridades tributarias, reguladores de actividad bursátil o de seguros, etc.

- Información de fuentes abiertas, incluyendo datos sobre la cotización de las distintas criptomonedas, información de contacto o datos sobre PSAV, o nexos entre las personas objeto de investigación y potencial información identificatoria (direcciones de criptomonedas, monederos, vinculaciones con actividad criminal o con criminales, etc.).

- Información en poder de las unidades nacionales especializadas en ciber seguridad, incluyendo reportes sobre incidentes que involucren al sector financiero; sobre malware dirigido al robo de identidad o a la obtención no autorizada de información confidencial y/o financiera (incluyendo datos o programas utilizados para el manejo de AV) e información de inteligencia sobre la comunidad hacker o sobre amenazas a la ciberseguridad

26. A los efectos de la recolección de información sobre personas objeto de investigación que tengan actividad o nexos con otras personas de interés fuera de sus fronteras, las agencias de investigación de los países miembros del GAFILAT pueden consultar el listado de fuentes abiertas de los países miembros compilado por la RRAG.

27. Debe ponerse especial atención en los nexos entre el posible uso ilícito de AV para LA/FT y los PSAV, a través de los cuales se suele producir el intercambio entre los AV y la moneda fiduciaria, dado que se trata del punto vulnerable de cualquier esquema de LA/FT que involucre esos valores, en especial cuando se manejan montos importantes, dado que el carácter (relativamente) reducido de los mercados de criptomonedas lo torna más sensible al ingreso o egreso masivo de fondos.

28. Los países que todavía no lo hayan hecho deben adecuar su normativa interna a fin de imponer a los PSAV obligaciones de registro y cumplimiento de funciones de ALA/CFT, de conformidad con lo establecido en la nueva Recomendación 15 del GAFI.

29. Se debe tener presente que los PSAV que estén sujetos al cumplimiento de obligaciones de ALA/CFT constituyen una fuente de información de gran importancia para las investigaciones patrimoniales sobre LA/FT con AV (en tanto pueden conectar transacciones pseudo anónimas con AV con clientes identificados) y, además, pueden facilitar el congelamiento, incautación y decomiso de los fondos involucrados o derivados de conductas ilícitas.

30. Los ROS que presentan los PSAV son de gran utilidad para las investigaciones patrimoniales objeto de esta guía, toda vez que contienen tanto información sobre transacciones (cliente/a emisor/a, beneficiario/a, direcciones de los monederos del/la cliente/a, saldo en los monederos, fecha y hora de las transacciones, tipo de AV transferido, locación de la transferencia, transacciones canceladas, cuentas bancarias registradas o verificadas y tipo de dispositivos utilizados); como información sobre los/las clientes/as (nombre, identificación como usuario, dirección/nes IP, domicilio -físico- de facturación, dirección de correo electrónico, fecha de nacimiento, nacionalidad, ciudadanía, perfil económico y actividad comercial).

31. Para la detección de posibles maniobras de LA/FT con AV por medio de PSAV, se deben tomar como referencia las “señales de alerta” reseñadas en el informe del GAFI sobre “Señales de alerta de lavado de activos y financiamiento del terrorismo con activos virtuales”, publicado en 2020.

32. Las agencias de investigación deben prestar especial atención a la actividad de PSAV no registrados, o que oculten su verdadera localización a fin de eludir la regulación establecida a nivel local en orden al cumplimiento de obligaciones de ALA/CFT, toda vez que dichos actores del ecosistema de AV suelen procesar un alto porcentaje de las transacciones con AV de origen ilícito.

33. En particular, debe investigarse la actuación de mezcladores, conmutadores y casas de apuestas online que operen por fuera de la ley. Con relación a ellos, las investigaciones referidas al uso de AV deben tener, como objetivo, no sólo identificar y perseguir a las personas que exploten el recurso a las criptomonedas para desarrollar conductas delictivas, sino también perseguir y eventualmente hacer cesar la actividad de los PSAV u otros proveedores de servicios, cuando esté dirigida a favorecer o facilitar el accionar criminal.

34. Es importante tener presente que, por lo general, la actividad delictiva con AV se encuentra concentrada en unos pocos PSAV que facilitan la comisión de maniobras de LA/FT con criptoactivos. Por consiguiente, si se descubre cuáles son los PSAV que reciben el mayor volumen de operaciones con AV de origen ilícito, las investigaciones centradas en ellos tienen mayores

posibilidades de generar resultados positivos en términos de identificación de personas involucradas en conductas delictivas e incautación y decomiso de AV.

35. Se debe tomar en cuenta que el intercambio entre AV y moneda fiduciaria también puede llevarse a cabo por medio de plataformas de intercambio P2P, que no se encuentran alcanzadas por la normativa de ALA/CFT de conformidad con lo establecido en la Recomendación 15 del GAFI. Si bien, por el momento, dichas plataformas procesan un porcentaje bajo de las operaciones con AV de origen ilícito, si pueden realizarse por su intermedio operaciones que dificultan el rastreo de AV y enmascaran su origen, como el "salto de cadenas" ("Chain hopping") o la "combinación de monedas" ("Coinjoin").

36. Las agencias de investigación deben estar atentas al posible uso, por parte de las personas objeto de investigación, de quioscos de criptomonedas o "Cajeros Bitcoin" para el intercambio de AV y moneda fiduciaria. Al respecto, cabe tener presente que las compañías que operan dichos cajeros se encuentran comprendidas en la definición de PSAV del GAFI, por lo que están obligadas a obtener información sobre sus clientes y reportar operaciones consideradas sospechosas.

37. La localización de los cajeros de AV presuntamente utilizados por las personas objeto de investigación puede tomarse como punto de partida para la realización de tareas de vigilancia o seguimiento de esa persona o sus posibles cómplices, ya sea físicamente o recurriendo a medios electrónicos.

38. Si la vigilancia del cajero de AV permite determinar la fecha y horario preciso de una operación de intercambio realizada por la persona objeto de investigación, ese dato se puede utilizar para requerir a la compañía responsable la información referida a dicha transacción, incluyendo el monto, el tipo de criptomoneda transado y las direcciones de AV de los participantes. A partir de ello, se puede efectuar una reconstrucción del origen y destino de los AV involucrados.

39. A los efectos del rastreo de la procedencia y destino de AV presuntamente asociados a actividad ilícita, la Blockchain ofrece una fuente importante de información que es a la vez relevante y confiable (toda vez que la estructura descentralizada de las criptomonedas impide la alteración de los registros en la Blockchain).

Rastreo de activos virtuales

40. A partir de los datos consignados en la Blockchain, las agencias de investigación pueden conocer el historial completo de transacciones de una determinada dirección de AV, incluyendo las direcciones de todos los usuarios/as con los/las que efectuó transacciones y la fecha, hora y monto exacto transferidos (lo cual puede resultar útil como criterio de búsqueda, cuando se analizan en simultaneo muchas operaciones), la cadena completa de transacciones efectuada por cada AV desde su creación y las direcciones IP asociadas a cada dirección de AV (a menos que el/la

usuario/a se conecte con la red a través de una herramienta de anonimato como un VPN o el sistema TOR).

41. El análisis de este conjunto de datos, y su entrecruzamiento con la información que se obtenga de otras fuentes (en especial si se lleva a cabo por medio de herramientas informáticas de "Big data") puede resultar fundamental para detectar la actividad delictiva con AV, identificar a sus responsables y conseguir evidencia incriminatoria. Al respecto, reviste especial relevancia la posibilidad de rastrear los movimientos de AV desde y hacia un PSAV. Ello, toda vez que, si el mismo se encuentra registrado en una jurisdicción que impone obligaciones de ALA/CFT, lo más probable es que cuente con información que permita la identificación de los/las usuarios/as involucrados en las operaciones con AV.

42. A los efectos de la identificación presente o futura de personas objeto de investigación por la presunta actividad ilegal con AV, es importante registrar, ordenar y catalogar todas las direcciones de AV de las plataformas de intercambio de criptomonedas, mezcladores, casas de apuestas online, mercados ilícitos en la Red oscura, personas ya identificadas como probables sospechosas de dedicarse a actividad ilícita generadora de fondos, o al LA/FT, entre otras, que hayan sido identificadas en el transcurso de investigaciones.

43. Las agencias de investigación deben contar con una base lo más amplia posible de direcciones de AV con titulares identificados, ya que ello facilita el uso de la Blockchain para permitir la identificación de otros/as usuarios/as que tengan contacto con aquellos.

Herramientas o técnicas pueden utilizarse para identificar activos virtuales y transacciones relacionadas

(i) Análisis de la Blockchain

44. El análisis de la Blockchain (o "Chain analysis") requiere del uso de las herramientas tecnológicas adecuadas, además de los conocimientos técnicos necesarios para utilizarlas.

45. Una herramienta que puede encontrarse en versiones de fuente abierta disponibles gratuitamente en internet son los exploradores de Blockchain, aplicaciones de red que operan como motores de búsqueda en el ecosistema AV, permitiendo la localización de direcciones, transacciones y otros datos vinculados a aquellas.

46. A la vez, existen recursos informáticos de mayor sofisticación, específicamente diseñados para las necesidades de las agencias de investigación, en manos de compañías privadas especializadas en el análisis de la Blockchain. CARIN y otros organismos internacionales recomiendan el establecimiento de instancias de cooperación público-privada a partir de la

contratación de los servicios de estas compañías, que han probado ser eficaces en investigaciones patrimoniales sobre maniobras de LA/FT con AV.

47. En este último supuesto, las autoridades deben contar con agentes o funcionarios preparados para explicar los hallazgos de estas compañías en el marco de los procesos judiciales que tengan lugar en conexión con las conductas delictivas con AV objeto de investigación. Se recomienda, en tal sentido, mantener una buena relación de trabajo con el personal de las empresas prestadoras del servicio, en especial si estos pueden llegar a ser llamados a testificar sobre el modo en que se arribó a las conclusiones presentadas.

48. La información que se obtenga del análisis de la Blockchain puede complementarse con técnicas de "Inteligencia de fuentes abiertas" (OSINT, por sus siglas en inglés), que comprenden la recolección, procesamiento y análisis sistemático la información disponible para el público en general, sin restricciones.

(ii) OSINT

49. En el contexto de las investigaciones patrimoniales objeto de esta guía, la OSINT puede utilizarse para obtener datos sobre los titulares de direcciones de AV ya conocidas por los/las investigadores/as. A tal efecto, puede intentarse colocar la dirección de AV en los motores de búsqueda en la Internet, ya que es bastante usual que las personas que se dedican al comercio ilícito en la Red (o las organizaciones terroristas que busquen captar fondos a través de AV) publiquen su dirección (asociándola a su perfil y pseudónimo online) ya sea en foros (como Reddit, 4Chan y 8Chan) o en las secciones de comentarios de páginas web especializadas en criptomonedas o en tecnología informática. Por añadidura, pueden consultarse páginas de Internet específicamente dedicadas a la identificación de usuarios de AV y de direcciones asociadas a aquellos.

50. La misma técnica puede utilizarse para obtener información en la Red oscura, en la que existen múltiples foros en los que, aprovechando el anonimato que confiere el ingreso mediante TOR, las personas comparten libremente información sobre los servicios ocultos, incluyendo sus direcciones, los productos y servicios que ofrecen, comentarios sobre la calidad del servicio, apodos de los comerciantes más (o menos) exitosos, etc.

51. Debe tenerse presente que los pseudónimos online muchas veces tienen un correlato ya sea en la Internet superficial (cuando el individuo actúa sobre todo en la Red oscura) o incluso en la vida real, el cual -en caso de ser descubierto- puede permitir vincular a la actividad ilícita con su verdadera identidad. En tal contexto, los/las investigadores/as pueden sacar provecho de los errores que las personas suelen cometer al momento de escindir su identidad online de su identidad (secreta) en la vida real, como no recordar utilizar herramientas de navegación anónima en alguna oportunidad, usar la misma dirección de AV para actividades ilícitas y lícitas o emplear

una dirección de correo electrónico asociada a su verdadero nombre en conexión con su identidad online.

52. Las técnicas de OSINT también pueden resultar efectivas para obtener información sobre PSAV no registrados que presten servicios a personas involucradas en conductas ilícitas con AV, incluyendo a mezcladores o plataformas P2P de intercambio de criptomonedas, sea en la Internet superficial o en la Red oscura, dado que se manejan con el mismo sistema basado en la reputación que los mercados ilegales online.

53. Por añadidura, se puede recurrir a las técnicas de OSINT a fin de obtener información que permita vincular a las personas sospechadas de estar involucradas en conductas ilícitas generadoras de fondos con los/las presuntos/as lavadores/as de dichos fondos. Asimismo, la información existente en fuentes abiertas puede resultar útil para comprender mejor el estilo de vida, los activos con los que cuenta la persona sospechosa, o los lugares en los que reside o desarrolla su actividad comercial o social.

54. También se puede obtener información ya procesada sobre personas de interés o sospechadas de estar involucradas en actividades ilegales con AV, recurriendo a los servicios de las denominadas “Data brokers”, que son compañías dedicadas a la recopilación y procesamiento de información de múltiples fuentes y la elaboración de minuciosos perfiles personales.

55. En procura de una mayor efectividad en las investigaciones patrimoniales, se recomienda combinar las técnicas reseñadas con el uso de medidas de investigación tradicionales, como los seguimientos o la vigilancia física, la inspección de los residuos que desechan las personas objeto de interés, los pedidos de informes, las órdenes de presentación y/o los registros personales o domiciliarios. También el interrogatorio de testigos, que pueden ofrecer conocimientos valiosos con respecto del estilo de vida, las actividades y los activos de los/las sospechosos/as.

56. En tal contexto, pueden emplearse medios electrónicos de vigilancia a fin de obtener datos relevantes para las investigaciones sobre conductas ilícitas con AV, como por ejemplo las conexiones de la persona objeto de sospecha con plataformas de intercambio de criptomonedas, mezcladores, páginas de apuestas online, redes P2P dedicadas a la transferencia de AV o servicios de almacenamiento en la nube. Asimismo, se puede averiguar por esa vía qué tipo de dispositivos informáticos usan las personas objeto de investigación, si cuentan con uno o más monederos online, los métodos preferidos de comunicación o si utilizan conexiones públicas de Wi-Fi u otros medios electrónicos a los que puedan acceder las autoridades.

(iii) Herramientas de monitoreo de red

57. Se puede recurrir, a tal efecto, a herramientas informáticas de monitoreo de red. Dichas herramientas facilitan la obtención de información relevante en distintos formatos: documentos

digitales voluminosos, imágenes, archivos de audio, videos e incluso comunicaciones telefónicas realizadas a través de internet. Incluso si el contenido de las comunicaciones interceptadas se encuentra encriptado, será posible capturar los denominados "datos de envoltorio", es decir todos aquellos que no forman parte del contenido de la comunicación, sino que se refieren a los mecanismos para su concreción (direcciones IP de origen y destino, volumen de los datos, nodos de Internet involucrados en el intercambio de paquetes de datos, etc.).

58. El uso de herramientas tecnológicas también facilita el seguimiento de las personas objeto de investigación, ya sea por medio de la instalación de dispositivos de GPS o explotando los datos provenientes de las aplicaciones móviles en los "teléfonos inteligentes" (para navegación, redes sociales, compra o banca online, etc.), asociados a los GPS insertos en los propios teléfonos móviles. Por añadidura, se puede efectuar un seguimiento prospectivo o retrospectivo a partir de la información que las compañías de telecomunicaciones recopilan como resultado del contacto constante entre los teléfonos móviles y las torres de telefonía celular, vinculadas al funcionamiento del 3G o 4G.

(iv) Análisis forense

59. A los efectos de identificar información o evidencia relevante para las investigaciones patrimoniales sobre LA/FT con AV, se recomienda llevar a cabo un análisis forense de los dispositivos electrónicos propiedad de (o utilizados por) las personas objeto de investigación que se obtengan en el marco de la misma. En esa dirección, puede encontrarse evidencia o información de interés en computadoras de escritorio, laptops, tabletas, teléfonos inteligentes, lectores inteligentes, equipos GPS portátiles, cámaras digitales, memorias flash, tarjetas SD, pendrives, discos rígidos extraíbles, servidores externos en la "nube", discos compactos y en los dispositivos inteligentes comprendidos dentro de la llamada "Internet de las cosas".

60. La información o evidencia importante que es posible encontrar en dichos dispositivos comprende:

- Evidencia o indicios de uso de AV.
- Evidencia o indicios de contactos con plataformas de intercambio de criptomonedas (ya sean PSAV o plataformas P2P), mezcladores, páginas de apuestas online, etc.
- Evidencia o indicios de uso de servicios de almacenamiento en la nube.
- Evidencia o indicios del empleo de herramientas de anonimato (TOR, I2P, VPNs).
- Evidencia o indicios de la utilización de herramientas informáticas de encriptación.

- Claves o contraseñas para el acceso a información almacenada en la nube o para deshabilitar encriptación.

- Evidencia o indicios sobre comunicaciones con otras personas sospechosas (titulares de fondos de origen ilícito, organizaciones terroristas, lavadores de activos, etc.).

- Documentación patrimonial u otra evidencia relevante en formato digital (documentos de constitución de sociedades, registros contables, imágenes o datos sobre activos, agendas, etc.).

Técnicas especiales de investigación

61. Cuando las características de la operatoria objeto de investigación así lo requiera (debido a su sofisticación o a la dificultad de obtener información o evidencia relevante por medios tradicionales), puede recurrirse al empleo de técnicas especiales de investigación como la actuación encubierta, siempre dentro del marco de lo permitido por la legislación procesal vigente en cada país.

62. En esa dirección, es posible aprovechar los programas y técnicas evasivas que utilizan los/las criminales para llevar adelante en forma anónima sus conductas delictivas en el ciberespacio (como el uso de herramientas como TOR o las VPNs para navegar anónimamente por Internet, o la asunción de identidades alternativas en la Red) para infiltrar agentes de las AOP dentro de organizaciones criminales que actúan en el ciberespacio, o interactuar con personas que ofrecen bienes o servicios ilegales en Internet.

63. En estos casos, dado que las herramientas de análisis de la Blockchain también pueden ser utilizadas por los criminales, se recomienda generar previamente un historial de transacciones que guarde relación con el "perfil" que va a asumir el/la agente que pretenda actuar en forma encubierta en Internet llevando a cabo operaciones con AV.

Uso de programas espías

64. Otra técnica avanzada de investigación a la que puede recurrirse en el contexto de investigaciones patrimoniales complejas sobre LA/FT con AV consiste en el uso, por parte de las AOP, de programas espías (spyware) o "troyanos". Dicha herramienta puede utilizarse para acceder remotamente a información o evidencia digital cuya localización física se desconozca o a la que resulte imposible acceder en forma efectiva (por ejemplo; para obtener las contraseñas necesarias para poder acceder al contenido de documentos encriptados, o a información almacenada en servidores externos; para monitorear comunicaciones realizadas a través de la Internet, mediante tecnologías de comunicación que imposibilitan la interceptación por medios tradicionales (sistemas de VoIP, o de mensajería encriptada); a fin de llevar a cabo vigilancia acústica o audiovisual,

utilizando el programa espía para habilitar remotamente los micrófonos o cámaras de dispositivos en poder de (o en las cercanías de) las personas objeto de investigación; o para localizar o seguir en tiempo real a las personas objeto de investigación.

65. La implementación del uso estatal de programas espías requiere de tres etapas: *(i)* análisis del uso que la persona objeto de investigación hace de las redes, para determinar que plataformas o aplicaciones utiliza (y las posibles vulnerabilidades de dichas plataformas o aplicaciones que puedan ser explotadas para introducirse en el sistema); *(ii)* compromiso de la plataforma mediante el "exploit" más apropiado, a fin de introducir el spyware; y *(iii)* monitoreo de la información capturada desde el objetivo.

66. Las herramientas informáticas necesarias para el uso de spyware con fines investigativos pueden obtenerse por medio de un desarrollo tecnológico del propio Estado, o adquiriendo los programas ofrecidos por las compañías privadas dedicadas al desarrollo y comercialización de programas espías para uso estatal.

Recaudos relacionados con el uso de programas espías

67. A fin de reducir el riesgo de proliferación inherente a la utilización de spyware, se recomienda adoptar medidas paliativas como la implementación de medidas técnicas para prevenir el redescubrimiento de la vulnerabilidad explotada para introducir el spyware; la notificación a la autoridad que corresponda del descubrimiento (estatal) de una vulnerabilidad y el pedido de autorización para explotarla; y la regulación del uso dual de vulnerabilidades.

68. Asimismo, se sugiere adoptar, a los efectos de la implementación del uso estatal de programas espías, el modelo "lanzador/carga" ("dropper/payload"), que consiste en el uso de un software (confidencial) para lograr la intrusión en el sistema o dispositivo del objetivo (el "lanzador"), y otro distinto (la "carga") para concretar la captura de la información o evidencia digital comprendida en la autorización judicial, cuyo funcionamiento si puede ser relevado o divulgado a la defensa de los eventuales imputados.

69. En todos los casos, debe procurarse que la herramienta informática este encriptada a partir de las características específicas del sistema objetivo (a fin de evitar que se descargue por error en otro sistema o dispositivo), y que se lo programe para autodestruirse una vez que concluya la medida de investigación.

70. Se deben documentar todos los pasos y acciones adoptados para introducir el programa espía dentro del equipo del sujeto investigado. Asimismo, es preciso dejar constancia de las características del programa usado para llevar a cabo el monitoreo y los cambios que este programa debió efectuar en el sistema a fin de permitir la interceptación y evitar ser detectado. Ello, a fin de poder demostrar que no se ha destruido ni alterado evidencia durante el transcurso de la medida.

71. En atención al impacto potencial que el uso de spyware con fines de investigación puede tener respecto del derecho a la intimidad de los/las ciudadanos/as, se recomienda que el recurso a esta medida sea regulado en forma expresa en la normativa procesal, estableciendo con la mayor claridad posible los requisitos exigidos para que pueda utilizarse dicha herramienta informática y los recaudos a adoptar en su implementación, de conformidad con los principios legales vigentes en cada Estado. Si el uso estatal de spyware se lleva a cabo aplicando analógicamente otras normas procesales o en virtud del principio de libertad probatoria, se sugiere adoptar ciertos recaudos para que la medida de investigación mediante el uso de spyware afecte lo menos posible el derecho a la intimidad y privacidad de las personas objeto de la misma. Entre ellas:

- Que la autorización judicial especifique: a) los dispositivos y los datos o contenido digital objeto de la medida; b) el alcance de la misma; y c) la forma en que la información relevante va a ser accedida y recogida.

- Que el uso de este método se limite solo a la investigación de delitos graves.

- Que se establezca un proceso de certificación del software utilizado, disponiéndose la posibilidad de verificar su funcionamiento para garantizar la imparcialidad y confidencialidad.

- Que los abogados defensores puedan acceder a la documentación vinculada a las medidas de investigación concretadas mediante programas informáticos y verificar si los programas usados han sido certificados.

- Que se establezca la obligación de desinstalar los programas al terminar su uso.

C. INCAUTACIÓN Y DECOMISO DE ACTIVOS VIRTUALES

Aspectos generales – AV centralizadas y descentralizadas

72. A los efectos de la incautación o decomiso de AV, corresponde distinguir según se trate de monedas virtuales centralizadas o descentralizadas. En el primer supuesto, la medida sobre los AV puede concretarse dirigiendo una orden judicial a la autoridad administrativa central que mantiene el control exclusivo sobre los activos, disponiendo la inmovilización o incautación de los fondos.

73. Cuando se trata de monedas descentralizadas (como las criptomonedas), la inexistencia de un banco central o institución similar que pueda inmovilizar los fondos en cumplimiento de una orden judicial determina que, en muchos casos, la autoridad estatal interviniente deberá llevar a cabo la incautación o decomiso por sus propios medios, sin intervención de ningún intermediario.

74. Una excepción está dada por los supuestos en los que los AV objeto de incautación o decomiso se encuentran alojados en un monedero "en custodia" (en los que la clave privada que controla el movimiento de los AV está en manos de un PSAV y no del/la titular de los mismos). En ese caso, al igual que con las monedas centralizadas, la medida patrimonial se puede concretar dirigiendo una requisitoria judicial al PSAV, disponiendo el congelamiento o incautación de los activos.

75. Cuando las claves privadas que controlan los AV se encuentran en manos de sus titulares, en cambio, el congelamiento de los fondos no es viable. Ello, desde que, en la práctica, cualquier persona que tenga la clave privada puede disponer los fondos asociados con la dirección de AV correspondiente a dicha clave, a la vez que pueden existir múltiples copias de cada clave privada, almacenadas en distintos lugares y en distintos formatos, y a las cuáles pueden tener acceso diferentes personas. Por consiguiente, mientras las criptomonedas se encuentren en el monedero de la persona sospechosa, incluso si esa persona se encuentra en custodia, cualquier tercero que cuente con la clave puede transferir los AV de modo irrevocable.

Medidas de aseguramiento

76. En este supuesto, el único modo de salvaguardar la posibilidad de las autoridades estatales de decomisar los AV es transfiriéndolos a un monedero controlado por ellas a la mayor brevedad posible, de modo tal de evitar que algún tercero sustraiga los fondos antes de que puedan pasar a manos del Estado. A tal efecto, es preciso obtener o bien la clave privada asociada a la dirección de AV correspondiente a los activos que se pretende incautar o decomisar, o bien la "frase semilla" que permite reconstruir el monedero en el que dichos AV están alojados.

Políticas o protocolos

77. Se recomienda que las agencias que puedan tener que ejecutar esta clase de medidas establezcan de antemano políticas o protocolos internos que regulen la incautación de AV y su tratamiento posterior. En tal sentido, debería preverse, como mínimo:

- La identificación de los/las funcionarios/as autorizados/as a llevar a cabo incautaciones o transacciones con AV.
- El detalle de las notificaciones internas y externas que es preciso efectuar cuando un caso involucra AV.
- Los procedimientos estándar para recolectar y preservar evidencia electrónica.
- Los protocolos de cadena de custodia que deben regir para todos los dispositivos que puedan contener evidencia electrónica.

Medidas preparatorias o previas a la incautación de AV

78. En el marco de la preparación previa del procedimiento de incautación o decomiso, se recomienda averiguar, antes de proceder, con qué clase de monederos y AV opera la persona objeto de investigación. La identificación del monedero es necesaria, toda vez que no todos los monederos admiten múltiples criptomonedas, a la vez que las diferencias entre las distintas clases de monederos influyen sobre la metodología técnica a utilizar para concretar la transferencia de los AV contenidos en el mismo, a los efectos de la incautación y decomiso. Por otro lado, la identificación de la clase específica de criptomoneda/s involucrada/s es imprescindible, ya que estas sólo pueden ser transferidas a una dirección correspondiente a su propia Blockchain.

79. Dicha información puede obtenerse de diversas maneras. Por ejemplo, si se investiga la actividad de un vendedor en un mercado ilícito online, el tipo de AV aceptado como pago va a figurar en su perfil. Los datos también pueden obtenerse a través de técnicas de OSINT, análisis de las Blockchain, etc.

80. Se recomienda, asimismo, la adopción de ciertas “buenas prácticas” en anticipación a un registro que pueda derivar en la incautación de AV, incluyendo:

- Estar al tanto de cuando los dispositivos de la persona sospechosa se encuentran logueados o en uso (mediante la determinación de patrones de conducta, monitoreo de red, vigilancia o actuación encubierta, según el caso).

- El monitoreo constante de la actividad de la persona objeto de investigación y del comportamiento de su/s dirección/es de AV.

- Prepararse para la posibilidad de encontrar cuentas que requieran autenticación de doble factor.

- En la medida de lo posible, asegurarse de contar con el acceso a las huellas digitales u otros datos biométricos que permitan el acceso a dispositivos protegidos por ese medio (por ejemplo, teniendo en custodia al titular de dichos dispositivos o contando con autorización para arrestarlo durante el registro y compeler la apertura de los dispositivos).

81. Dada la importancia de la celeridad en la incautación de AV, es importante contar con autorización judicial para llevarla a cabo antes de procedera la realización de cualquier registro que pueda derivar en el hallazgo del/los monedero/s de la persona objeto de investigación. Asimismo, es importante que la autorización judicial comprenda lo siguiente:

- Permiso para secuestrar, en el transcurso del registro, todos los dispositivos de almacenamiento de datos que puedan encontrarse en el domicilio o las oficinas de la persona objeto de investigación (discos rígidos extraíbles, CDRs, DVDRs, memory sticks, pendrives, etc). Ello, toda vez que puede tratarse de "monederos hardware" o en su defecto contener información importante en formato digital, como las "palabras semilla" que permiten reconstruir un monedero AV, las contraseñas utilizadas por el/la usuario/a para acceder a un monedero híbrido, etc.

- Permiso para que, en el caso que durante el registro de un domicilio -o el arresto de un/a sospechoso/a- se constate que la computadora de aquél/la o su smartphone o tableta se encuentran desbloqueados y activos, se aproveche dicha circunstancia para analizar su contenido en busca de monederos de AV. Ello así, desde que la oportunidad ideal para concretar la incautación de criptomonedas es cuando el monedero que contiene la/las clave/s privada/s se encuentra abierto, o cuando durante el registro se encuentra la contraseña para abrirlo o la "frase semilla" que permite reconstruirlo.

- Permiso para aislar a las personas que se encuentren presentes durante el procedimiento a fin de impedir que se conecten a Internet o puedan tomar contacto con el exterior, hasta tanto se haya concretado la incautación. Ello, a fin de impedir que mientras la medida se está desarrollando, algún cómplice de la persona objeto de investigación transfiera los fondos que se pretende obtener.

Registros o allanamientos de domicilios

82. En la planificación de los registros domiciliarios que puedan culminar en una incautación o decomiso de AV, también se debe tomar en consideración la necesidad de neutralizar, tan pronto como sea posible, toda posibilidad de que la persona objeto de investigación destruya, altere u oculte información útil para acceder al monedero de AV (contraseñas o pins manuscritos, monederos físicos, etc.) antes de que las autoridades lleguen hasta el mismo, transfiera su contenido o de aviso a un tercero para que lo haga por él.

83. La planificación previa a la incautación o decomiso comprende también la generación de direcciones de AV controladas por la AOP o autoridad que esté a cargo del procedimiento de conformidad con la legislación local. A tal efecto, se recomienda que las claves públicas y privadas se generen con una aplicación de monedero en una computadora no conectada a Internet, y utilizar luego un explorador de Blockchain para verificar que no haya registro de la dirección pública en la misma. Finalmente, la clave pública (no así la privada) debe transferirse de la computadora inicial a una computadora portátil equipada con las aplicaciones necesarias para efectuar una transferencia de AV, que es la que va a llevarse al procedimiento para concretar la incautación.

84. Si se lleva a cabo el registro de una propiedad (sea un domicilio, una oficina o incluso automóviles, embarcaciones, etc.), en el marco de una investigación por posible uso ilícito de AV que puede derivar en la incautación de los mismos, corresponde poner énfasis en la detección de distintos elementos que pueden resultar relevantes ya sea como evidencia, como información que conduzca a evidencia o como llave para permitir la incautación o decomiso de AV de origen ilícito. Por ejemplo:

- Computadoras u otros dispositivos que contengan información en formato electrónico, como teléfonos móviles, tabletas, pendrives, discos rígidos extraíbles, etc.

- Monederos de AV, ya sea en formato virtual (como aplicaciones dentro de los equipos electrónicos antes mencionados) o en formato físico, como por ejemplo monederos hardware o de papel.

- Información que permita el acceso a los monederos o la transferencia de AV, como contraseñas o pins para acceder a monederos encriptados o a monederos online alojados en servidores externos, direcciones de AV y -en especial- las claves privadas o "palabras semilla".

Monederos

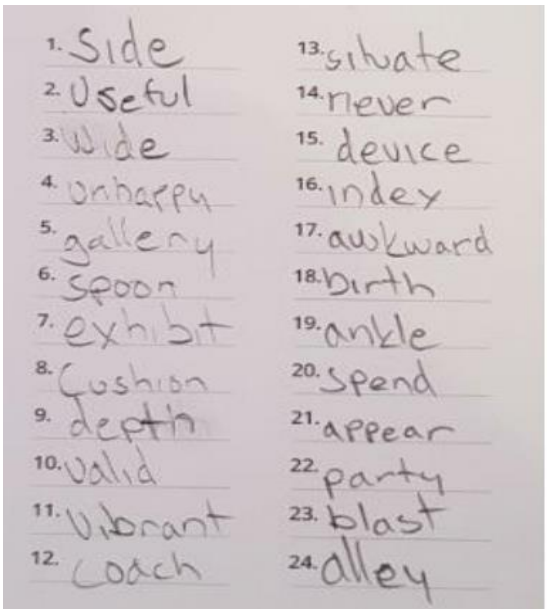
85. Los monederos virtuales (de escritorio o móviles) en general están identificados con un ícono en el escritorio de la computadora o la página de inicio del teléfono móvil. De lo contrario, se los puede localizar utilizando el buscador de la computadora para identificar los archivos con la palabra "wallet" o una extensión ".dat" (aunque en algunos casos, el/la usuario/a puede haberlos guardado con otro nombre o extensión). En la siguiente imagen se ilustran los íconos de algunos de los monederos más populares:

86. Si se descubre un monedero de papel (como el que se ilustra en la siguiente imagen), es posible verificar si existen fondos escaneando el código QR y utilizando una aplicación móvil para

contrastarlo con la información disponible en la Blockchain de la criptomoneda de que se trate. La misma aplicación puede utilizarse para transferir los AV a un monedero controlado por las autoridades, concretando de ese modo la incautación de los fondos.

87. Dado que los monederos de AV suelen estar protegidos por contraseñas (para lograr el acceso) o por pins (para habilitar la realización de transacciones), se debe revisar cuidadosamente el lugar objeto de registro -y, en especial, el entorno en derredor de la ubicación de la computadora de la persona investigada- en busca de notas manuscritas, cuadernos, apuntes, agendas, notas autoadhesivas, etc., en las que puedan haberse consignado las contraseñas o pins necesarias/os para concretar transacciones.

88. Si durante el registro, los/las investigadores/as encuentran las “palabras semillas” (como se muestran en la siguiente imagen), las pueden utilizar para reconstruir el monedero (incluyendo su clave privada) y transferir, por ese medio, los AV a un monedero bajo control estatal, concretando la incautación. A tal efecto, se introducen las 12 o 24 palabras y al término de la última, se obtiene una copia exacta del monedero original.



89. No todos los monederos siguen los mismos protocolos. Por consiguiente, dependiendo del tipo de monedero de que se trate, su reconstrucción a partir de la frase semilla puede arrojar el mismo resultado que si se accediera al original (la totalidad de los AV contenidos en aquella), o un monedero vacío. Existen aplicaciones que permiten determinar qué tipo de resultado habrá de arrojar la reconstrucción de un determinado monedero mediante la frase semilla.

90. Resulta de utilidad también el posible hallazgo del "Número de usuario retornante" ("Returning customer number") con el que algunos mezcladores de AV identifican a las personas que utilizan sus servicios más de una vez. Si bien dicho número no sirve para facilitar la incautación de las criptomonedas de origen ilícito, si es útil como evidencia del uso de mezcladores, como así también -potencialmente- para identificar al mezclador específico que procesó los AV de la persona objeto de investigación y permitir un eventual rastreo mediante técnicas de "Chain analysis".

91. Debido a su dificultad técnica, es preferible que ejecución de la incautación de AV sea llevada a cabo por personal especializado y capacitado, siendo que -además- la celeridad puede ser esencial para garantizar el éxito de la incautación. Por consiguiente, es necesario que quienes concreten la medida estén al tanto de las distintas variedades de monedero de AV existentes y de los mecanismos de seguridad con los que estos cuentan.

92. El mejor modo de concretar la incautación de AV contenidos en un monedero controlado por la persona objeto de investigación es llevándola a cabo mientras el mismo se encuentra desbloqueado y en uso. A tal efecto, debe procurarse, en caso de ser posible, que el procedimiento dirigido a obtener el control sobre el dispositivo que contiene el monedero se lleve a cabo de forma tal de sorprender a la persona objeto de investigación en el momento en que lo está utilizando.

93. Una vez conseguido el acceso al monedero, resulta fundamental adoptar los recaudos necesarios para asegurar que se mantengan encendidos y en uso, a fin de evitar que vuelvan a bloquearse, entorpeciendo el acceso al monedero o resguardando los contenidos mediante encriptación.

94. Es importante tener presente que un monedero de criptomonedas puede alojar múltiples direcciones (en algunos casos, incluso de diferentes monedas) conteniendo AV potencialmente sujetas a incautación.

95. Los archivos digitales conteniendo monederos virtuales (de escritorio o móviles) deben ser exportados desde el dispositivo de la persona objeto de investigación con ayuda de una herramienta informática forense. Es preciso efectuar una imagen digital del monedero completo, como así también efectuar copias o imágenes digitales (según el caso) de las claves privadas o palabras semilla encontradas en documentos de papel o en archivos de texto o Word. A

continuación, se las debe importar a la computadora de la agencia de investigación que cuente con el software necesario para llevar a cabo la incautación.

Perfeccionamiento de la incautación

96. La incautación propiamente dicha se concreta transfiriendo los AV desde la dirección de la persona objeto de investigación a la controlada por la autoridad competente, a cuyo efecto la computadora utilizada por los/las agentes debe estar conectada a Internet y, en su caso, también sincronizada con la correspondiente Blockchain.

Recomendaciones adicionales para incautación y decomiso efectivos de los AV

97. En relación con la incautación y decomiso de AV, se recomienda adoptar una serie de buenas prácticas, incluyendo las siguientes:

- En la medida de lo posible, tener convertidas de antemano la/las dirección/es estatales a formato QR, a fin de evitar errores de tipeo (en especial si se la incautación se concreta con monederos móviles, en los que es más factible cometer errores de ese tipo).

- De lo contrario, se recomienda llevar a cabo un doble o triple chequeo individual de la dirección de destino antes de hacer la transferencia.

- Utilizar la función “sweep” de los monederos de AV, que transfiere el saldo completo del monedero que se está incautando al monedero de destino (en este caso, el que previamente hayan constituido las autoridades que llevan a cabo la incautación).

- A los efectos de mayor velocidad, establecer la comisión (“fee”) más alta que sea autorizada, a fin de procurar que los mineros de la Blockchain la ubiquen en el bloque más cercano y se complete la operación más rápidamente.

- Si las direcciones controladas por el Estado se almacenan en monederos de papel, asegurar que no sean visibles las claves privadas, o que sean multi firmas, a fin de reducir el riesgo de sustracción de los AV incautados.

- Cuando se elabora el acta o reporte referido al procedimiento de incautación de AV, no consignar en ningún caso la clave privada o la frase semilla que habilita su transferencia.

- Una vez concretada la incautación, verificar periódicamente el saldo de la/las dirección/es de AV previamente vaciadas, toda vez que puede ocurrir que reciban transferencias o pagos con posterioridad al procedimiento.

98. Si el monedero se encuentra bloqueado y no se logra encontrar la contraseña requerida para acceder, corresponde secuestrar el dispositivo que lo contiene como se haría con cualquier otro dispositivo que contenga evidencia digital relevante, adoptando las precauciones establecidas en los protocolos sobre tratamiento de prueba electrónica. Posteriormente, y teniendo presente la necesidad de obrar con la mayor celeridad posible, deben adoptarse las medidas investigativas que resulten pertinentes para obtener las contraseñas y concretar la incautación de los AV asociados al mismo.

99. Si la incautación de AV resulta imposible, puede recurrirse a la información contenida en la Blockchain para establecer cuál era el valor de los fondos sujetos a decomiso y proceder a la incautación de bienes por valor equivalente.

Pasos posteriores a la incautación

100. Una vez incautados los AV, puede optarse por: a) retenerlos hasta que se dicte la resolución final de decomiso; o b) convertirlos inmediatamente (o en un breve lapso) a moneda fiduciaria. A fin de optar por una u otra opción, debe tenerse presente, por un lado, el riesgo de depreciación de los AV debido a la fluctuación en la cotización de las criptomonedas; y, por el otro, los riesgos y costos de seguridad asociados al almacenamiento de AV.

Administración de los AV durante el curso del proceso

101. Puede resultar conveniente establecer un procedimiento de consulta con el titular previo de los AV incautados (es decir, a la persona objeto de investigación) a fin de que se expida por escrito en orden a si prefiere que sean mantenidos en su estado original o convertidos en moneda fiduciaria. De ese modo, si con posterioridad deben ser devueltos, el Estado queda liberado de responsabilidad por una eventual pérdida de valor.

102. También se puede establecer de antemano (sea a través de una norma o de políticas internas escritas) un plazo fijo para la conversión de los AV incautados en moneda fiduciaria (por ejemplo, tres días), de modo tal que la decisión de concretar dicha conversión no dependa de un juicio sobre su conveniencia en términos económicos.

Liquidación de los AV

103. Una vez adoptada la decisión de liquidar los AV incautados o decomisados, la venta se puede efectuar directamente o en una subasta pública en procura de maximizar el valor obtenido, de conformidad con lo que establezca la legislación aplicable o a lo que decida la autoridad competente. También se puede arribar a un convenio con un operador privado especializado en el intercambio de AV (es decir, un PSAV) a fin de que tome a su cargo todo lo referido a la conversión de las criptomonedas en moneda fiduciaria.

104. Si se decide no liquidar ciertos AV decomisados (por ejemplo, monedas privadas como Monero), por considerarse que no existen usos legítimos para ellos en el mercado, es preciso adoptar las medidas de seguridad necesarias para garantizar un almacenamiento permanente eficaz de los AV en cuestión.

105. Se recomienda que los AV incautados sean alojados en monederos de almacenamiento en frío (por ejemplo, un monedero físico, o uno virtual, pero contenido en una computadora no conectada a Internet, o incluso en monederos de papel). En igual sentido, puede optarse por almacenar los AV incautados en monederos multi firmas, de modo tal que no sea posible sustraerlos obteniendo ilícitamente una única clave privada.

106. También se recomienda mantener un listado de las contraseñas para el acceso a cada uno de los dispositivos electrónicos (incluyendo computadoras y teléfonos inteligentes), unidades de almacenamiento externo encriptadas y monederos de AV secuestrados en manos de un/una funcionario/a específicamente designado/a, restringiendo el acceso a los mismos tanto como sea posible. Las frases semillas, contraseñas, claves privadas, pins y direcciones de AV obtenidas pueden ser mantenidas en archivos de texto, en una carpeta designada para cada AV incautado en una unidad de almacenamiento externo (por ejemplo, un disco rígido extraíble), en lo posible encriptados, para mayor seguridad. Estas unidades deben mantenerse offline en una locación específica segura hasta que sean requeridos por las autoridades competentes para recibir o transferir AV.

D. CONSIDERACIÓNES FINALES

Enfoque multidisciplinario

107. A los efectos de obtener una mayor eficiencia en la investigación de maniobras de LA/FT con AV, resulta fundamental adoptar un enfoque multidisciplinario que combine los conocimientos de agentes con experiencia en investigaciones patrimoniales con los del personal de las unidades especializadas en cibercrimen o ciberseguridad. Se recomienda enfáticamente la conformación de grupos multidisciplinarios compuestos por profesionales de ambas áreas, en línea con lo establecido en la Recomendación 30 del GAFI.

108. Resulta importante, asimismo, que las agencias responsables de investigar esa clase de conductas ilícitas actúen en coordinación con fiscales u operadores judiciales capacitados en la materia, en especial en lo concerniente a la obtención, análisis y tratamiento de la evidencia electrónica y a la incautación y decomiso de AV; así como el uso de técnicas o herramientas avanzadas de investigación tecnológica, como el Chain analysis, la OSINT, el agente encubierto digital y el uso de spyware, allí donde su utilización se encuentre permitida por la legislación procesal local.

Cooperación internacional

109. El carácter trasnacional de la Internet y del ecosistema de los AV convierte a la cooperación internacional en un elemento esencial de las investigaciones patrimoniales referidas a las conductas delictivas asociados con aquellos.

110. Se recomienda que las agencias o autoridades responsables de investigar maniobras de LA/FT con AV utilicen todas las vías que estén a disposición para conectarse con sus pares en el extranjero, incluyendo a mecanismos de cooperación entre agencias policíacas (INTERPOL, EUROPOL); puntos de contacto para el intercambio de información vinculada a la incautación y decomiso de activos de origen ilícito (RRAG, CARIN, redes ARIN, StAR y GFPN); puntos de contacto para el intercambio de información vinculada al cibercrimen (Portal Interamericano de Cooperación en Delitos Cibernéticos y Red de contactos 24/7 del G-7); canales para la cooperación jurídica internacional como IberRed; redes de intercambio de información de inteligencia financiera recopilada por las UIF (Grupo Egmont); así como pedidos de asistencia legal mutua.

111. Es importante también establecer contacto directo con autoridades en la contraparte extranjera que estén familiarizadas con la cuestión objeto del pedido de cooperación (investigaciones por actividad ilícita con AV) y -en general- con la problemática de la evidencia digital, así como el establecimiento de canales informales de comunicación con agencias similares en otros países para facilitar la colaboración.

112. Se recomienda enfáticamente utilizar la RRAG para identificar bienes y personas en el extranjero que puedan ser relevantes en el marco de una investigación sobre maniobras de LA/FT mediante AV y para tomar conocimiento de procesos penales en trámite en otros países. A tal efecto, pueden requerirse a través de la plataforma segura de la RRAG datos de carácter general, social, tributario, patrimonial y financiero, ya sea a fin de enriquecer la información con la que cuentan los/las investigadores/es en el país requirente, o bien para facilitar la confección de pedidos de asistencia jurídica internacional con datos precisos, a fin de incrementar las oportunidades de éxito.

113. La referida plataforma permite intercambiar información entre los países de la RRAG y las 54 jurisdicciones que pertenecen a la Red CARIN de forma segura. Adicionalmente, los puntos de contacto de la RRAG pueden acceder, mediante dicha red, a información en poder de otros organismos internacionales vinculados a la incautación de activos, como la Red Interinstitucional para la Recuperación de Activos de Camden (CARIN), la Red Global de Puntos de Contacto sobre Recuperación de Activos (GFPN) y la Iniciativa de Recuperación de Activos Robados (StAR) de Interpol.

114. También se puede acceder, por dicha vía, a la información recolectada por las redes ARIN en todo el mundo, que incluyen a la Red Interinstitucional para la Recuperación de Activos de Asia del Pacífico (ARIN-AP) y Asia Central y Occidental (ARIN-WCA); la Red Interinstitucional para la Recuperación de Activos del Caribe (ARIN-CARIB), la Red Interinstitucional para la Recuperación de Activos de África Oriental (ARIN-EA), del Sur de África (ARIN-SA) y de África Occidental (ARIN-WA).

115. Asimismo, puede recurrirse a los intercambios de información mediante el Portal Interamericano de Cooperación en materia de Delito Cibernético a cargo de la Secretaría Técnica de la Reunión de Ministros de Justicia y otros Ministros y Fiscales Generales de las Américas (REMJA) de la OEA. A tal efecto, el Departamento de Cooperación Jurídica de la Secretaría de Asuntos Jurídicos de la OEA mantiene un directorio actualizado de las autoridades de persecución penal y de policía que sirven como puntos de contacto para la cooperación internacional en materia de delito cibernético y evidencias electrónicas.

116. Se recomienda que los estados que todavía no lo hayan hecho se vinculen, en el menor plazo posible, con la "Red de Contactos sobre Delitos de Alta Tecnología 24 horas/7 días" del G-7; y que fortalezcan los mecanismos que permitan el intercambio de información y la cooperación con otras organizaciones e instancias internacionales en materia de delito cibernético, tales como las Naciones Unidas, el Consejo de Europa, la Unión Europea, el Foro de Cooperación Económica Asia-Pacífico (APEC), la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el Commonwealth y la INTERPOL.

Desarrollo y perfeccionamiento de capacidades

117. Habida cuenta que la investigación sobre el uso ilícito de AV involucra el análisis de tecnologías complejas y, por consiguiente, demanda el desarrollo de técnicas investigativas novedosas y la adquisición de nuevos recursos y capacidades, es necesario implementar programas de capacitación dirigidos al rango más amplio posible de personal, a fin de que adquieran los conocimientos mínimos necesarios para llevar a cabo -o, cuanto menos, no comprometer- las investigaciones patrimoniales referidas al uso ilícito de AV.

118. En tal contexto, es preciso capacitar:

a. A los investigadores, con respecto a las nuevas tecnologías involucradas en las investigaciones patrimoniales sobre el uso ilegal de AV;

b. A los agentes de policía en general, sobre como reconocer y reaccionar ante la existencia de evidencia digital relevante para esa clase de investigaciones; y

c. A los investigadores forenses, en lo tocante a las nuevas tecnologías en juego.

119. No hace falta que todo el personal dedicado a la investigación se especialice en el uso de AV. Sin embargo, si es preciso contar con un número de expertos (proporcional al tamaño de la jurisdicción) que esté capacitado para reconstruir una cadena de transacciones en la Blockchain y/o para incautar o decomisar AV. El resto del personal solo debe contar con los conocimientos mínimos necesarios para reconocer indicios sobre el posible uso de criptomonedas si se topa con ellos en el transcurso de una investigación o al llevar a cabo un registro, y para poder contactar a los/las agentes especializados/as en la materia dentro de su jurisdicción.

120. En tal contexto, es importante que un número suficiente de agentes reciba entrenamiento en el uso de las herramientas forenses para la trazabilidad de AV que se encuentran disponibles en el mercado, o en su defecto de las que desarrolle internamente cada país, si decide hacerlo.

121. Asimismo, las autoridades relevantes (ya sea que se trate de agencias policíacas o de las fiscalías competentes) deben estar capacitadas para manejar las distintas clases de monederos de AV que pueden llegar a utilizarse en estos procedimientos, así como en las cuestiones de ciberseguridad inherentes a la administración de los activos incautados.

122. Ante la posibilidad de que agentes no pertenecientes a unidades especializadas se topen con criptomonedas en cumplimiento de órdenes de registro, etc., es preciso que el personal de las AOP que puedan potencialmente encontrarse en dicha situación sepa reconocer, cuanto menos, los rasgos más importantes del uso de AV. (códigos QR, frases semillas, claves públicas o privadas, diferentes formatos de dirección de criptomonedas y distintos tipos de monederos, contraseñas, pins, etc). Como así también que, en un plano más general, sean capaces de reconocer dispositivos que puedan contener evidencia digital.

123. La capacitación del personal puede llevarse a cabo mediante la organización de programas de entrenamiento, la elaboración de manuales, programas de intercambio y/o participación en conferencias o seminarios internacionales.

124. A fin de ampliar al máximo posible el alcance de los conocimientos sobre AV entre el personal de las fuerzas de seguridad, resulta recomendable distribuir material de consulta (folletos, instructivos) que contenga un detalle páginas o aplicaciones referidas a VAs, plataformas de intercambio, procesadores de pagos y proveedores de servicios de monederos de criptomonedas, imágenes de frases semillas, códigos QR, monederos papel o hardware y cajeros de AV, etc.

Cooperación público-privada

125. Finalmente, se recomienda también la implementación de instancias de cooperación público-privada con actores del sector privado especializados en estas nuevas tecnologías, dirigidas a procurar que las AOP y las unidades del MPF con competencia en la materia se mantengan actualizadas con respecto a los nuevos desarrollos en dicho ámbito.

ANEXO 2: LEGISLACIÓN COMPARADA SOBRE EL USO DE TÉCNICAS AVANZADAS DE INVESTIGACIÓN (AGENTE ENCUBIERTO DIGITAL / SPYWARE)

1. En este apartado se acompañan, a efectos de ilustrar los parámetros establecidos en la legislación comparada con respecto a la regulación de técnicas avanzadas de investigación (en especial, el agente encubierto informático o digital y el uso estatal de spyware).

2. A tal efecto, se reproduce, por un lado, un artículo que forma parte de los Textos Legislativos Modelo de la Comunidad del Caribe (ITU/CARICOM/CTU Model Legislative Texts), por tratarse del primer instrumento multilateral internacional que contempla en forma expresa la incorporación del uso de un "software forense remoto" (es decir, de un programa espía o spyware) como herramienta de investigación.

3. Asimismo, se reproducen los artículos pertinentes de la Ley de Enjuiciamiento Criminal (LEC) de España, conforme la reforma introducida mediante la Ley Orgánica (LO) 13/2015. En esta última reforma, se incorporó a la normativa procesal española, por un lado, el instituto del "agente encubierto informático" en el apartado 6° del artículo 282 bis, en el que ya se regulaba lo referido al agente encubierto "tradicional".

4. Por otra parte, se reproduce el contenido de los capítulos IV a X de la LEC, que comprende a las disposiciones referidas a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

5. Si bien en estas disposiciones sólo se alude en forma expresa al uso de software forense en relación con el registro remoto de equipos informáticos (Capítulo IX, art. 588 septies a), se transcribe la totalidad de los capítulos mencionados por cuanto, por un lado, la normativa no excluye la posibilidad de emplear spyware también para concretar la interceptación de comunicaciones telemáticas, la grabación de comunicaciones orales, el seguimiento y o la captación de imágenes[206]; y, por el otro, resulta valiosa por la minuciosidad con la que se han establecido los requisitos para llevar a cabo esta clase de medidas, a fin de minimizar el impacto potencial sobre el derecho a la privacidad de los ciudadanos derivado de la utilización de programas espías.

Textos Legislativos Modelo de la Comunidad del Caribe (ITU/CARICOM/CTU Model Legislative Texts): Modelo de Lineamientos de Regulación y Textos Legislativos sobre Cibercrímenes – HIPCAR:

Art. 27:

(1): Si un [Juez] [Magistrado] llega a la conclusión, con base en [información en una declaración jurada o testimonio] que en el marco de una investigación respecto de alguno de los delitos enumerados en el parágrafo 7, existen motivos razonables para creer que evidencia esencial no puede ser obtenida aplicando otros medios enumerados en la parte IV pero son razonablemente necesarios para los fines de la investigación, el [Juez] [Magistrado] [puede] [debe] autorizar a pedido de parte a un funcionario [judicial] [policial] a utilizar un software forense remoto para llevar a cabo la tarea específica requerida para la investigación e instalarlo en el sistema informático del sospechoso a fin de obtener la evidencia relevante. La requisitoria debe contener la siguiente información:

a. la identificación del sospechoso, de ser posible con su nombre y domicilio; y
b. la descripción del sistema informático objeto de la medida; y
c. la descripción de la medida de investigación, su alcance y su duración; y
d. los motivos por los que es necesaria su implementación.

(2) En el marco de esta investigación es necesario garantizar que las modificaciones al sistema informático del sospechoso se restrinjan a las que resulten esenciales para la investigación y que,

[206] Ver: Blanco, Hernán: "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre", en InDret, N° 1/2020, enero de 2020.

en la medida de lo posible, puedan ser revertidos al finalizar la misma. Durante la investigación, es necesario registrar:
a. el medio técnico utilizado y la fecha y hora de su implementación; y
b. la identificación del sistema informático y el detalle de las modificaciones realizadas durante la investigación; y
c. la información obtenida. La información obtenida mediante el uso del software debe ser protegida contra modificaciones y destrucción o acceso no autorizados.

(3) La duración de la autorización prevista en el art. 27 (1) se limita a [3 meses]. Si las condiciones que justificaron la autorización dejan de concurrir, la medida debe cesar inmediatamente.

(4) La autorización para instalar el software comprende el acceso remoto al sistema informático del sospechoso.

(5) Si el proceso de instalación requiere del acceso físico a un espacio deben cumplirse los requisitos establecidos en el art. 20.

(6) De ser necesario, un funcionario [judicial] [policial] puede requerir, de conformidad con la autorización judicial impartida en (1), que se ordene al proveedor de servicio de internet brindar apoyo para el proceso de instalación.

(7) [Listado de delitos].

Texto original (en inglés):

Art. 27. (1) If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence can not be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] on application authorize a [law enforcement] [police] officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information:
a. suspect of the offence, if possible, with name and address; and
b. description of the targeted computer system; and
c. description of the intended measure, extent, and duration of the utilization; and
d. reasons for the necessity of the utilization.

(2) Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible, can be undone after the end of the investigation. During the investigation it is necessary to log:
a. the technical mean used and time and date of the application; and
b. the identification of the computer system and details of the modifications undertaken within the investigation;
c. any information obtained. Information obtained using such software need to be protected against any modification, unauthorized deletion, and unauthorized access.

(3) The duration of authorization in section 27 (1) is limited to [3 months]. If the conditions of the authorization is no longer met, the action taken are to stop immediately.

(4) The authorization to install the software includes remotely accessing the suspects computer system.

(5) If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled.

(6) If necessary, a [law enforcement] [police] officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process.

(7) [List of offences].

LEY DE ENJUICIAMIENTO CRIMINAL – ESPAÑA: DISPOSICIONES INCORPORADAS POR LEY ORGANICA 13/2015:

Artículo 282 bis.

1. A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos. La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad. La resolución por la que se acuerde deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad. La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente.

2. Los funcionarios de la Policía Judicial que hubieran actuado en una investigación con identidad falsa de conformidad a lo previsto en el apartado 1, podrán mantener dicha identidad cuando testifiquen en el proceso que pudiera derivarse de los hechos en que hubieran intervenido y siempre que así se acuerde mediante resolución judicial motivada, siéndole también de aplicación lo previsto en la Ley Orgánica 19/1994, de 23 de diciembre.

Ningún funcionario de la Policía Judicial podrá ser obligado a actuar como agente encubierto.

3. Cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables.

4. A los efectos señalados en el apartado 1 de este artículo, se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes:
a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.
b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.
c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.
d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.
e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.
f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.
g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.
h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.
i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.
j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.
k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.
l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.
m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.
n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.
o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.
5. El agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito. Para poder proceder penalmente contra el mismo por las actuaciones realizadas a los fines de la investigación, el Juez competente para conocer la causa deberá, tan pronto tenga conocimiento de la actuación de algún agente encubierto en la misma, requerir informe relativo a tal circunstancia de quien hubiere autorizado la identidad supuesta, en atención al cual resolverá lo que a su criterio proceda.
6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a. El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su

contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.
7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio.

CAPÍTULO IV
Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos

Artículo 588 bis a. *Principios rectores.*
1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.
2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.
3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.
4. En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:
a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o
b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.
5. Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

Artículo 588 bis b. *Solicitud de autorización judicial.*

1. El juez podrá acordar las medidas reguladas en este capítulo de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial.
2. Cuando el Ministerio Fiscal o la Policía Judicial soliciten del juez de instrucción una medida de investigación tecnológica, la petición habrá de contener:
1.º La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.
2.º La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo con los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.
3.º Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.
4.º La extensión de la medida con especificación de su contenido.
5.º La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.
6.º La forma de ejecución de la medida.
7.º La duración de la medida que se solicita.

8.º El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

Artículo 588 bis c. *Resolución judicial.*
1. El juez de instrucción autorizará o denegará la medida solicitada mediante automotivado, oído el Ministerio Fiscal. Esta resolución se dictará en el plazo máximo de veinticuatro horas desde que se presente la solicitud.
2. Siempre que resulte necesario para resolver sobre el cumplimiento de alguno de los requisitos expresados en los artículos anteriores, el juez podrá requerir, con interrupción del plazo a que se refiere el apartado anterior, una ampliación o AOParación de los términos de la solicitud.
3. La resolución judicial que autorice la medida concretará al menos los siguientes extremos:
a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.
b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.
c) La extensión de la medida de injerencia, especificando su alcance, así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a.
d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.
e) La duración de la medida.
f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.
g) La finalidad perseguida con la medida.
h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

Artículo 588 bis d. *Secreto.*
La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.

Artículo 588 bis e. *Duración.*
1. Las medidas reguladas en el presente capítulo tendrán la duración que se especifique para cada una de ellas y no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos.
2. La medida podrá ser prorrogada, mediante automotivado, por el juez competente, de oficio o previa petición razonada del solicitante, siempre que subsistan las causas que la motivaron.
3. Transcurrido el plazo por el que resultó concedida la medida, sin haberse acordado su prórroga, o, en su caso, finalizada ésta, cesará a todos los efectos.

Artículo 588 bis f. *Solicitud de prórroga.*
1. La solicitud de prórroga se dirigirá por el Ministerio Fiscal o la Policía Judicial al juez competente con la antelación suficiente a la expiración del plazo concedido. Deberá incluir en todo caso:
a) Un informe detallado del resultado de la medida.
b) Las razones que justifiquen la continuación de la misma.
2. En el plazo de los dos días siguientes a la presentación de la solicitud, el juez resolverá sobre el fin de la medida o su prórroga mediante automotivado. Antes de dictar la resolución podrá solicitar AOParaciones o más información.
3. Concedida la prórroga, su cómputo se iniciará desde la fecha de expiración del plazo de la medida acordada.

Artículo 588 bis g. *Control de la medida.*
La Policía Judicial informará al juez de instrucción del desarrollo y los resultados de la medida, en la forma y con la periodicidad que este determine y, en todo caso, cuando por cualquier causa se ponga fin a la misma.

Artículo 588 bis h. *Afectación de terceras personas.*
Podrán acordarse las medidas de investigación reguladas en los siguientes capítulos aun cuando afecten a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas.

Artículo 588 bis i. *Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales.*
El uso de las informaciones obtenidas en un procedimiento distinto y los descubrimientos casuales se regularán con arreglo a lo dispuesto en el artículo 579 bis.

Artículo 588 bis j. *Cese de la medida.*
El juez acordará el cese de la medida cuando desaparezcan las circunstancias que justificaron su adopción o resulte evidente que a través de la misma no se están obteniendo los

resultados pretendidos, y, en todo caso, cuando haya transcurrido el plazo para el que hubiera sido autorizada.

Artículo 588 bis k. *Destrucción de registros.*
1. Una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo custodia del secretario judicial.
2. Se acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal.
3. Los tribunales dictarán las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados.

CAPÍTULO V
La interceptación de las comunicaciones telefónicas y telemáticas

Sección 1.ª Disposiciones generales

Artículo 588 ter a. *Presupuestos.*
La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

Artículo 588 ter b. *Ámbito.*
1. Los terminales o medios de comunicación objeto de intervención han de ser aquellos habitual u ocasionalmente utilizados por el investigado.
2. La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario.
También podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.
A los efectos previstos en este artículo, se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la

prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga.

Artículo 588 ter c. *Afectación a tercero.*
Podrá acordarse la intervención judicial de las comunicaciones emitidas desde terminales o medios de comunicación telemática pertenecientes a una tercera persona siempre que:
1.º exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o
2.º el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad.
También podrá autorizarse dicha intervención cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular.

Artículo 588 ter d. *Solicitud de autorización judicial.*
1. La solicitud de autorización judicial deberá contener, además de los requisitos mencionados en el artículo 588 bis b, los siguientes:
a) la identificación del número de abonado, del terminal o de la etiqueta técnica,
b) la identificación de la conexión objeto de la intervención o
c) los datos necesarios para identificar el medio de telecomunicación de que se trate.
2. Para determinar la extensión de la medida, la solicitud de autorización judicial podrá tener por objeto alguno de los siguientes extremos:
a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.
b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.
c) La localización geográfica del origen o destino de la comunicación.
d) El conocimiento de otros datos de tráfico asociados o no asociados, pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que han de ser obtenidos.
3. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.

Artículo 588 ter e. *Deber de colaboración.*
1. Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar

al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones.

2. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.
3. Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en delito de desobediencia.

Artículo 588 ter f. *Control de la medida.*
En cumplimiento de lo dispuesto en el artículo 588 bis g, la Policía Judicial pondrá a disposición del juez, con la periodicidad que este determine y en soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas. Se indicará el origen y destino de cada una de ellas y se asegurará, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas.

Artículo 588 ter g. *Duración.*
La duración máxima inicial de la intervención, que se computará desde la fecha de autorización judicial, será de tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

Artículo 588 ter h. *Solicitud de prórroga.*
Para la fundamentación de la solicitud de la prórroga, la Policía Judicial aportará, en su caso, la transcripción de aquellos pasajes de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida.
Antes de dictar la resolución, el juez podrá solicitar AOParaciones o más información, incluido el contenido íntegro de las conversaciones intervenidas.

Artículo 588 ter i. *Acceso de las partes a las grabaciones.*
1. Alzado el secreto y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas. Si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos. La no inclusión de la totalidad de la grabación en la transcripción entregada se hará constar de modo expreso.
2. Una vez examinadas las grabaciones y en el plazo fijado por el juez, en atención al volumen de la información contenida en los soportes, cualquiera de las partes podrá solicitar la inclusión en las copias de aquellas comunicaciones que entienda relevantes y hayan sido excluidas. El juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa.

3. Se notificará por el juez de instrucción a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. Si la persona notificada lo solicita se le entregará copia de la grabación o transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia.

Sección 2.ª Incorporación al proceso de datos electrónicos de tráfico o asociados

Artículo 588 ter j. *Datos obrantes en archivos automatizados de los prestadores de servicios.*
1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial.

2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

Sección 3.ª Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad

Artículo 588 ter k. *Identificación mediante número IP.*
Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

Artículo 588 ter l. *Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes.*
1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de

alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.
2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 ter d. La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior.
El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 bis c.

Artículo 588 ter m. *Identificación de titulares o terminales o dispositivos de conectividad.*
Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia.

CAPÍTULO VI
Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos

Artículo 588 quater a. *Grabación de las comunicaciones orales directas.*
1. Podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados.

Los dispositivos de escucha y grabación podrán ser colocados tanto en el exterior como en el interior del domicilio o lugar cerrado.
2. En el supuesto en que fuera necesaria la entrada en el domicilio o en alguno de los espacios destinados al ejercicio de la privacidad, la resolución habilitante habrá de extender su motivación a la procedencia del acceso a dichos lugares.
3. La escucha y grabación de las conversaciones privadas se podrá complementar con la obtención de imágenes cuando expresamente lo autorice la resolución judicial que la acuerde.

Artículo 588 quater b. *Presupuestos.*
1. La utilización de los dispositivos a que se refiere el artículo anterior ha de estar vinculada a comunicaciones que puedan tener lugar en uno o varios encuentros concretos del investigado con

otras personas y sobre cuya previsibilidad haya indicios puestos de manifiesto por la investigación.
2. Solo podrá autorizarse cuando concurran los requisitos siguientes:
a) Que los hechos que estén siendo investigados sean constitutivos de alguno de los siguientes delitos:
1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.
2.º Delitos cometidos en el seno de un grupo u organización criminal.
3.º Delitos de terrorismo.
b) Que pueda racionalmente preverse que la utilización de los dispositivos aportará datos esenciales y de relevancia probatoria para el esclarecimiento de los hechos y la identificación de su autor.

Artículo 588 quater c. *Contenido de la resolución judicial.*
La resolución judicial que autorice la medida deberá contener, además de las exigencias reguladas en el artículo 588 bis c, una mención concreta al lugar o dependencias, así como a los encuentros del investigado que van a ser sometidos a vigilancia.

Artículo 588 quater d. *Control de la medida.*
En cumplimiento de lo dispuesto en el artículo 588 bis g, la Policía Judicial pondrá a disposición de la autoridad judicial el soporte original o copia electrónica auténtica de las grabaciones e imágenes, que deberá ir acompañado de una transcripción de las conversaciones que considere de interés.
El informe identificará a todos los agentes que hayan participado en la ejecución y seguimiento de la medida.

Artículo 588 quater e. *Cese.*
Cesada la medida por alguna de las causas previstas en el artículo 588 bis j, la grabación de conversaciones que puedan tener lugar en otros encuentros o la captación de imágenes de tales momentos exigirán una nueva autorización judicial.

CAPÍTULO VII
Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización

Artículo 588 quinquies a. *Captación de imágenes en lugares o espacios públicos.*
1. La Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos.

2. La medida podrá ser llevada a cabo aun cuando afecte a personas diferentes del investigado, siempre que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación.

Artículo 588 quinquies b. *Utilización de dispositivos o medios técnicos de seguimiento y localización.*
1. Cuando concurran acreditadas razones de necesidad y la medida resulte proporcionada, el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización.
2. La autorización deberá especificar el medio técnico que va a ser utilizado.
3. Los prestadores, agentes y personas a que se refiere el artículo 588 ter están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos por los que se ordene el seguimiento, bajo apercibimiento de incurrir en delito de desobediencia.
4. Cuando concurran razones de urgencia que hagan razonablemente temer que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización se frustrará la investigación, la Policía Judicial podrá proceder a su colocación, dando cuenta a la mayor brevedad posible, y en todo caso en el plazo máximo de veinticuatro horas, a la autoridad judicial, quien podrá ratificar la medida adoptada o acordar su inmediato cese en el mismo plazo. En este último supuesto, la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso.

Artículo 588 quinquies c. *Duración de la medida.*
1. La medida de utilización de dispositivos técnicos de seguimiento y localización prevista en el artículo anterior tendrá una duración máxima de tres meses a partir de la fecha de su autorización. Excepcionalmente, el juez podrá acordar prórrogas sucesivas por el mismo o inferior plazo hasta un máximo de dieciocho meses, si así estuviera justificado a la vista de los resultados obtenidos con la medida.
2. La Policía Judicial entregará al juez los soportes originales o copias electrónicas auténticas que contengan la información recogida cuando éste se lo solicite y, en todo caso, cuando terminen las investigaciones.
3. La información obtenida a través de los dispositivos técnicos de seguimiento y localización a los que se refieren los artículos anteriores deberá ser debidamente custodiada para evitar su utilización indebida.

CAPÍTULO VIII
Registro de dispositivos de almacenamiento masivo de información

Artículo 588 sexies a. *Necesidad de motivación individualizada.*
1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.

Artículo 588 sexies b. *Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado.*
La exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización.

Artículo 588 sexies c. *Autorización judicial.*
1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial.
2. Salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos.
3. Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación.
4. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El

juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.
5. Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia.
Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.

CAPÍTULO IX
Registros remotos sobre equipos informáticos

Artículo 588 septies a. *Presupuestos.*
1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:
a) Delitos cometidos en el seno de organizaciones criminales.
b) Delitos de terrorismo.
c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.
e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.
2. La resolución judicial que autorice el registro deberá especificar:
a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.
b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.
c) Los agentes autorizados para la ejecución de la medida.
d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.
e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.
3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo,

pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.

Artículo 588 septies b. *Deber de colaboración.*
1. Los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización.
2. Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia.
Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco, y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.
3. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.
4. Los sujetos mencionados en los apartados 1 y 2 de este artículo quedarán sujetos a la responsabilidad regulada en el apartado 3 del artículo 588 ter e.

Artículo 588 septies c. *Duración.*
La medida tendrá una duración máxima de un mes, prorrogable por iguales períodos hasta un máximo de tres meses.

CAPÍTULO X
Medidas de aseguramiento

Artículo 588 octies. *Orden de conservación de datos.*
El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes.
Los datos se conservarán durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días.
El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado·3 del artículo 588 ter e.

De la detención y apertura de la correspondencia escrita y telegráfica

Artículo 579. *De la correspondencia escrita o telegráfica.*

1. El juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa, siempre que la investigación tenga por objeto alguno de los siguientes delitos:
1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.
2.º Delitos cometidos en el seno de un grupo u organización criminal.
3.º Delitos de terrorismo.
2. El juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales o inferiores períodos hasta un máximo de dieciocho meses, la observación de las comunicaciones postales y telegráficas del investigado, así como de las comunicaciones de las que se sirva para la realización de sus fines delictivos.
3. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.
4. No se requerirá autorización judicial en los siguientes casos:
a) Envíos postales que, por sus propias características externas, no sean usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías o en cuyo exterior se haga constar su contenido.
b) Aquellas otras formas de envío de la correspondencia bajo el formato legal de comunicación abierta, en las que resulte obligatoria una declaración externa de contenido o que incorporen la indicación expresa de que se autoriza su inspección.
c) Cuando la inspección se lleve a cabo de acuerdo con la normativa aduanera o proceda con arreglo a las normas postales que regulan una determinada clase de envío.
5. La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.

Artículo 579 bis. *Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales.*
1. El resultado de la detención y apertura de la correspondencia escrita y telegráfica podrá ser utilizado como medio de investigación o prueba en otro proceso penal.
2. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen.

3. La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, éste comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo, se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada.

BIBLIOGRAFÍA

ABELSON, Harold / ANDERSON, Ross / BELLOVIN, Steven M. / BENALOH, Josh / BLAZE, Matt / DIFFIE, Whitfield / GILMORE, John / GREEN, Matthew / LANDAU, Susan / NEUMANN, Peter G. / RIVEST, Ronald L. / SCHILLER, Jeffrey I. / SCHNEIER, Bruce / SPECTER, Michael / WEITZNER, Daniel J.: "Keys under doormats: Mandating insecurity by requiring government access to all data and communications", Massachusetts Institute of Technology Science and Artificial Intelligence Laboratory, julio 2017.

ACAMS: "Combating the proliferation of mobile and internet payment systems as money laundering vehicles", 2015.

ALSALAMI, Nasser / ZHANG, Bingsheng: "SoK: A systematic study of anonymity in cryptocurrencies", IEEE Conference on Dependable and Secure Computing (DSC), noviembre 2019.

ALLEN, Franklin / GU, Xian / JAGTIANI, Julapa: "A survey of Fintech research and policy discussion", Federal Reserve Bank of Philadelphia Research Department, Worgking Papers 20-21, junio 2020.

ANDROULAKI, Elli / KARAME, Ghassam / ROESCHLIN, Mark / SCHERER, Tobias / CAPKUN, Sdrjan: "Evaluating user privacy in bitcoin", *Financial cryptography and data security. Volume 7859 of Lecture Notes in Computer Science*, Springer, Berlin, 2013, págs. 34/51.

AUCOIN, Kaleigh E.: "The spider's parlour: Government malware on the dark web", Hastings Law Journal, Vol 69, N° 5, 2018, págs. 1433/1469.

Basel Committee on Banking Supervision: "Prudential treatment of cryptoassets exposures", Bank for International Settlements, junio 2021.

BAZZELL, Michael, *Open source intelligence techniques. Resources for searching an analyzing online information* (5ª ed.), IntelTechniques, 2016.

BELLIA, Patricia L.: "Spyware and the limits of surveillance law", University of Notre Dame Law School, Legal Studies Research Paper N° 05-15, 2005.

BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan: "Going bright: Wiretapping without weakening communications infrastructure", IEEE Security & Privacy, Vol 11, N° 1, 2013, págs. 62/72.

BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan: "Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet", Northwestern Journal of Technology and Intellectual Property, Vol. 12, N° 1, 2014, págs. 1/64.

BIRYUKOV, Alex / KHOVRATOVICH, Dimitry / PUSTOGAROV, Ivan: "Deanonymisation of clients in Bitcoin P2P network", AAVV, *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Scottdale, 2014, págs. 15/29.

BIRYUKOV, Alex / FEHER, Daniel: "Deanonimization of hidden transactions in Zcash", University of Luxembourg, 2018.

BLANCO, Hernán, *Tecnología informática e investigación criminal*, La Ley, Buenos Aires, 2020.

BLANCO, Hernán: "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre", InDret, N° 1/2020, enero de 2020.

BOJARSKI, Kamil: "Dealer, hacker, lawyer, spy. Modern techniques and legal boundaries of counter-cybercrime operations", The European Review of Organized Crime, Vol. 2, N° 2, 2015, págs. 25/50.

BRILL, Alan / KEENE, Lonnie: "Cryptocurrencies: The next generation of terrorist financing", Defence Against Terrorism Review, Vol. 6, N° 1, 2014, págs. 7/30.

BRYANS, Danton: "Bitcoin and money laundering: Mining for an effective solution", Indiana Law Journal, Vol. 89, 2014, págs. 441/472.

Camdem Asset Recovery Inter-Agency Network (CARIN): "CARIN Manual" (5a Edición), Guernesey Law Offices, 2015.

CARRELL, Nathan E.: "Spying on the mob: United States v. Scarfo – A constitutional analysis", Journal of Law, Technology & Policy", Vol. 2002, N° 1, 2002, págs. 193/214.

CipherTrace: "Cryptocurrency crime and anti-money laundering report", febrero 2021.

Convención de la Liga de Estados Árabes (League of Arab States Convention).

Convenio del Consejo de Europa sobre Cibercriminalidad (Convención de Budapest).

Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, febrero 2021.

DASKAL, Jennifer; "The un-territoriality of data", The Yale Law Journal, Vol. 125, N° 2, 2015, págs. 326/398.

DE HERT, Paul / BOULET, Gertjan: "Cloud computing and trans-border law enforcement access to private sector data. Challenges to sovereignty, privacy and data protection", *Big data and privacy. Making ends meet*, Future of Privacy Forum & Stanford Center for Internet & Society, 2013, págs. 23/26.

DE ZAN, Tomasso: "E-evidence and cross border data requests in Italy", *EUnited against crime: Improving criminal justice in European Union cyberspace*, Instituti Affari Internazionali, 2016, págs. 42/59.

DUPUIS, Daniel / GLEASON, Kimberley: "Money laundering with cryptocurrency: Open doors and the regulatory dialectic", Journal of Financial Crime, Agosto 2020.

European Banking Authority (EBA): "Warning to consumers on cryptocurrencies", diciembre 2013.

European Banking Authority (EBA): "EBA opinion on 'virtual currencies'", EBA-Op-2014-08, julio 2014.

European Banking Authority (EBA): "Opinion of the European Banking Authority on the EU Commision's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (AAMLD)", EBA-OP-2016-07, Agosto 2016.

European Central Bank (ECB): "Virtual currency schemes", Frankfurt, octubre 2012.

European Central Bank (ECB) "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", ECB Crypto-Assets Task Force, Occasional Paper Series, N° 223, mayo 2019.

European Parliament: "Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices", Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, 2017.

European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses", Policy Department for Citizen's Rights and Constitutional Affairs, mayo 2018.

European Union Agency for Cibersecurity (ENISA) y Europol: "On lawful criminal investigation that respects 21st century data protection. Europol and ENISA joint statement", declaración del 20 de mayo de 2016.

European Union Agency for Cibersecurity (ENISA): "Crypto assets. An introduction to digital currencies and distributed ledger technologies", Febrero 2021.

Europol: "Dismantling of an encryted network sends shockwaves through organized crime groups across Europe", julio 2020.

FALIERO, Johanna C., *Criptomonedas: La nueva frontera regulatoria del Derecho informático*, Ad-Hoc, Buenos Aires, 2017.

FANUSIE, Yaya J. / ROBINSON, Tom: "Bitcoin laundering: An analysis of illicit flows into digital currency services", Elliptic Center on Sanctions & Illicit Finance, enero 2018.

Federal Bureau of Investigations (FBI): "Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity", Criminal Intelligence Section / Cyber Intelligence Section, abril 2012.

Financial Stability Institute: "Supervising cryptoassets for anti-money laundering", FSI insights on policy implementation, N° 31, abril 2021.

FOLEY, Sean / KARLSEN, Jonathan R. / PUTNINS, Talis J. "Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?", The Review of Financial Studies, Vol. 32, N° 5, 2019, págs. 1798/1853.

FORGANG, George: "Money laundering through cryptocurrencies", Economic Crime Forensics Capstones, La Salle University, Vol. 40, 2019.

GAFI: "Report on new payment methods", octubre 2006.

GAFI: "Money laundering using new payment methods", octubre 2010.

GAFI: "Virtual currencies. Key definitions and potential AML/CFT risks", junio 2014.

GAFI: "Guidance for a risk-based approach: Virtual currencies", junio 2015.

GAFI: "Emerging terrorist finance risks", octubre 2015.

GAFI: "FATF report to G20 Finance Ministers and Central Bank Governors", julio 2018.

GAFI: "Professional money laundering", julio 2018.

GAFI: "Financing of terrorism for recruitment purposes", octubre 2018.

GAFI: "Virtual assets and virtual assets service providers. Guidance for a risk-based approach", junio 2019.

GAFI: "Guidance on financial investigations involving virtual assets", junio 2019.

GAFI: "FATF report to the G20 Ministers and Central Bank governors on the so-called stablecoins", junio 2020.

GAFI: "Money laundering and terrorist financing red flag indicators associated with virtual assets", septiembre 2020.

GAFI: "Estándares internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva", diciembre 2020.

GAFI: "12-month review of the revised FATF standards on virtual assets and virtual asset service providers", junio 2020.

GAFILAT: "Plan estratégico GAFILAT 2020-2025".

GAFILAT: "10 años de la Red de Recuperación de Activos del Grupo de Acción Financiera de Latinoamérica – RRAG", septiembre 2020.

GAFILAT: "Inventario de redes existentes a nivel global para la identificación y recuperación de activos producto del delito", junio 2021.

GAFILAT /RRAG: "Listado de fuentes abiertas de los países miembros de la RRAG", junio 2021.

GHAPPOUR, Ahmed: "Searching places unknown: Law enforcement jurisdiction on the dark web", Stanford Law Review, Vol. 69, N° 4, 2017, págs. 1075/1136.

GASSER, Urs / GERTNER, Nancy / GOLDSMITH, Jack / LANDAU, Susan / NYE, Joseph / O'BRIEN, David R. / OLSEN, Matthew G. / RENAN, Daphna / SÁNCHEZ, Julian / SCHNEIER, Bruce / SCHWARTZOL, Larry / ZITTRAIN, Jonathan: "Don't panic. Making progress in the 'going dark' debate", Berkman Center for Internet & Society, Harvard University, febrero 2016.

HENNESSEY, Susan: "The elephant in the room: Addressing child exploitation and going dark", Hoover Institution, Stanford University, Aegis Paper Series, N° 1701, 2017.

HERRERA-JOANCOMARTÍ, Jordi: "Research and challenges on Bitcoin anonymity", *Data privacy management, autonomous spontaneous security, and security assurance*, Revised

Selected Papers from 9th International Workshop, DPM 2014, 7th International Workshop, SETOP 2014, and 3rd International Workshop, QASA 2014, Wroclaw, 2014, págs. 3/16.

HOSCHEIDT, Matheus M. / FELBER EICHNER, Elisa: "Legal and political measures to address cybercrime", World Summit on the Information Society Forum, UFGRS Model United Nations, Vol. 2, 2014, págs. 445/477.

International Association of Chiefs of Police (IACP): "Data, privacy and public safety. A law enforcement perspective on the challenges of gathering electronic evidence", IACP Summit Report, 2015.

INTERPOL / Basel Institute on Governance / EUROPOL: "Recommendations 4th Global Conference on Criminal Finances and Cryptocurrencies", noviembre 2020.

JOHNSON, David R. / POST, David: "Law and borders – The rise of law in cyberspace", Stanford Law Review, Vol. 48, N° 5, 1996, págs. 1367/1402.

JONES, Phil: "Habilidades fundamentales para rastrear activos", Basel Insitute of Governance, Quick Guide Series, N° 14, noviembre 2020.

KAPPOS, George / HAAROON YOUSAF, Mary Maller / MEIKLEJOHN, Sarah: "An empirical analysis of anonymity in Zcash", Proceedings of the 27th USENIX Security Symposium, Baltimore, 2018.

KERR, Orin S. / MURPHY, Sean D.: "Government hacking to light the dark web. What risks to international relations and international law?", Stanford Law Review Online, Vol. 70, 2017, págs. 58/69.

KERR, Orin S. / SCHNEIER, Bruce: "Encryption workarounds", Georgetown Law Journal, Vol. 106, N° 4, 2018, págs. 989/1019.

KOOPS, Bert-Jaap: "Police investigations in open sources: Procedural-law issues", Computer Law & Security Review, Vol. 29, N° 6, 2013, págs. 654/665.

KOOPS, Bert-Jaap / GOODWIN, Morag: "Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law", Tilburg Law School Legal Studies Research Paper Series N° 5/2016, 2014.

KOSHY, Phillip / KOSHY, Diana / MCDANIEL, Patrick: "An analysis of anonymity in Bitcoin using P2P network traffic", 18th International Conference on Financial Cryptography and Data Security, 2014.

LEE, Seunghyeon / YOON, Changhoon / KANG, Heedo / KIM, Yeonkeun / KIM, Yongdae / HAN, Dongsu / SON, Sooel / SHIN, Seungwon "Cybercriminal minds: An investigative study of cryptocurrency abuses in the Dark Web", Network and Distributed Systems Security (NDSS) Symposium, 2019.

Ley Modelo del Commonwealth (Commonwealth Model Law).

MAURER, Felix Konstantin: "A survey on approaches to anonymity in Bitcoin and other cryptocurrencies", *Informatik 2016. Lecture notes in informatics*. Bonn, 2016, págs. 2145/2150.

MAYER, Jonathan, "Constitutional malware", en Social Sciences Research Network (SSRN), noviembre 2016.

MBIYANGA, Stefan "Cryptolaundering: Anti-money laundering regulation of virtual currency exchanges", Journal of Anti-Corruption Law, Vol. 3, N° 1, 2019, págs. 1/15.

MCQUADE, Samuel: "Cybercrime", en TONRY, Samuel, *The Oxford handbook of crime and public policy*, Oxford University Press, 2011.

MEDINA, Manuel: "Inteligencia de fuente abierta", Basel Insitute of Governance, Quick Guide Series, N° 17, junio 2020.

MEIKLEJOHN, Sarah / POMAROLE, Marjori / JORDAN, Grant / LEVCHENKO, Kirill / MCCOY, Damon / VOELKER, Geoffrey M. / SAVAGE, Stefan: "A fistful of Bitcoins: Characterizing payments among men with no names", Proceedings of the 2013 Conference on Internet Measurement Conference, ACM, 2013, págs. 127/140.

MOISENKO, Anton / IZENMAN, Karla: "From intention to action: Next steps in preventing criminal abuse of cryptocurrency", Royal United Services Institute (RUSI) Occasional Paper, Londres, 2019.

MÖSER, Malte / SOSKA, Kile / HEILMAN, Ethan / LEE, Kevin / HEFFAN, Henry / SRIVASTAVA, Shashvat / HOGAN, Kile / HENNESEY, Jason / MILLER, Andrew / NARAYANAN, Arvind / CHRISTIN, Nicolas: "An empirical analysis of traceability in the Monero Blockchain", Proceedigs on Privacy Enhancing Technologies, Vol. 3, 2018, págs. 143-163.

NAKAMOTO, Satoshi: "Bitcoin: A peer-to-peer electronic cash system", 2008.

Organización de los Estados Americanos (OEA): "Recomendaciones de la 9ª reunión del Grupo de Trabajo en Delito Cibernético", Reuniones de Ministros de Justicia u Otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), 12 y 13 de diciembre de 2016.

Organización de los Estados Americanos (OEA): "Recomendaciones de la 11ª Reunión de Ministros de Justicia u Otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA XI), OEA/ser.K/XXXIV.11 REMJA-XI/DOC.2/21 rev. 1, mayo de 2021.

Organización de los Estados Americanos (OEA): "Estudio sobre nuevas tipologías en el lavado de dinero, específicamente en el uso de moneda virtual", conclusiones de la XLV Reunión del Grupo de Expertos para el Control del Lavado de Activos – Subgrupo de Trabajo de UIF/OIC 2016-2018, OEA/Ser.L/XV. 4.45 DDOT/LAVEX/doc. 16/18, octubre de 2018.

Organización de las Naciones Unidas (ONU): "El derecho a la privacidad en la era digital", Declaración 68/167, 18 de diciembre de 2013.

Organización de las Naciones Unidas (ONU): "El derecho a la privacidad en la era digital", Declaración A/HRC/27/37, informe de la Oficina del Alto Comisionado por los Derechos Humanos de las Naciones Unidas, junio 2014.

Organización de las Naciones Unidas (ONU): "El derecho a la privacidad en la era digital", Declaración 69/166, 18 de diciembre de 2014.

ORTIZ PRADILLO, Juan Carlos: "Fighting cybercrime in Europe: The admissibility of remote searches in Spain", European Journal of Crime, Criminal Law and Criminal Justice, Vol. 19, N° 4, 9/5/2011.

ORTIZ PRADILLO, Juan Carlos: "'Hacking' legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática", *Delincuencia informática. Tiempos de cautela y amparo*, Thompson Reuters-Aranzadi, Navarra, 2012, págs. 177/220.

ORTIZ PRADILLO, Juan Carlos: "Fraude y anonimato en la red: Cuestiones constitucionales y procesales de la desanonimización de la red TOR", *Fraude electrónico. Su gestión penal y civil*, Tirant lo Blanch, Valencia, 2015, págs. 55/99.

Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations", 2018.

Proyecto de Directiva de la Comunidad Económica de los Países de África Occidental (ECOWAS Draft Directive).

Proyecto de Convención de la Unión Africana (Draft African Union Convention).

Regional Organized Crime Information Center (ROCIC): "Penetrating de Darknet. Silk Road, bitcoins, and The Onion Router", 2013.

Regional Organized Crime Information Center (ROCIC): "Bitcoin and cryptocurrencies. Law enforcement investigative guide", Special Research Report, 2018.

REID, Fergal / HARRIGAN, Martin: "An analysis of anonymity in the Bitcoin system", Security and Privacy in Social Networks, Springer, 2013, págs. 197/223.

RICHET, Jean-Loup "Laundering money online: A review of cybercriminals methods", Tools and Resources for Anti-Corruption Knowledge, UNODC, junio 2013.

RON, Dorit / SHAMIR, Adi: "Quantitative analysis of the full Bitcoin transaction graph", International Conference on Financial Cryptography and Data Security", Springer, 2013, págs. 6/24.

SALT, Marcos, *Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos*, Ad-Hoc, Buenos Aires, 2017.

SEITZ, Nicolai: "Transborder search: A new perspective in law enforcement?", Yale Journal of Law and Technology, Vol. 7, N° 1, 2005, págs. 23/50.

SILVA RAMALHO, David: "The use of malware as a means of obtaining evidence in Portuguese criminal proceedings", Digital Evidence and Electronic Signature Law Review, Vol. 11, 2014, págs. 55/75.

SILFVERSTEN, Erik / FAVARO, Marina / SLAPAKOVA, Linda / ISHIKAWA, Sascha / LIU, James / SALAS, Adrian: "Exploring the use of Zcash cryptocurrency for illicit criminal purposes", RAND Europe, 2020.

SPOENLE, Jan: "Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal", Council of Europe Discussion Paper N° 31, 2010.

Textos Legislativos Modelo de la Comunidad del Caribe (ITU/CARICOM/CTU Model Legislative Texts).

SWIRE, Peter / AHMAD, Kenesa: "'Going dark' versus a 'golden age for surveillance'", CDT Fellows Focus Series, publicado el 28/11/2011.

VON WEGBERG, Rolf / OERLEMANS, Jan-Jaap / VAN DEVENTER, Oscar: "Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using Bitcoin", Journal of Financial Crime, Vol. 25, N° 2, 2018, págs. 419/432.

United Nations Office on Drugs and Crime (UNODC), *Comprehensive study on cybercrime*, 2013.

United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies", junio 2014.

VACIAGO, Giuseppe / SILVA RAMALHO, David: "Online searches and online surveillance: The use of trojans and other tipes of malware as means of obtaining evidence in criminal proceedings", Digital Evidence and Electronic Signature Law Review, Vol. 13, 2016, págs. 88/86.