Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets

December 2021

GAFILAT is grateful for the technical assistance provided by the German Development Cooperation, implemented by the Deutsche Gesellschaft für Iternationale Zusammenarbeit (GIZ) for the elaboration of this document, with the additional support of Mr. Hernán Blanco. The contents of this publication are the sole responsibility of the Financial Action Task Force of Latin America (GAFILAT).

TABLE OF CONTENTS

I. INTRODUCTION

The development and massive global adoption of the use of the Internet, personal computers, mobile devices, services and platforms associated with them, has had a vast impact on the speed and nature of social interactions, and commercial or financial transactions are not exceptions.[1] One of the expressions of the transition of human activity from the physical to the virtual world has been the emergence of virtual assets (VAs), understood, according to the definition of the Financial Action Task Force (FATF), as a digital representation of value that can be digitally exchanged or transferred, and used as a form of payment or investment instrument.[2] In this scenario, the most important development has undoubtedly been the creation of cryptocurrencies, which since their birth in 2008—with the publication of the famous "White paper" by Satoshi Nakamoto on Bitcoin[3]—have become one of the largest unregulated markets in the world.[4]

The emergence of cryptocurrencies and the underlying "distributed ledger technology" (DLT) (exemplified by the Blockchain) is a phenomenon that may well be set to positively revolutionize many aspects of the financial system. However, like many innovations, it is also susceptible to being exploited to favor illicit activities. The use of bitcoins, or similar cryptocurrencies that emerged later, known generically as "Altcoins," allows anyone—regardless of whether they are engaged in a legal or criminal activity—to transfer value almost instantaneously at little or no cost, with minimal entry barriers and with no paper trail.

Criminals, usually adept at adopting new technologies, quickly realized that the particular characteristics of Bitcoin could be useful to their interests. This resulted in the use of this cryptocurrency to facilitate the emergence of online marketplaces on the "dark web" of the Internet, where (mostly) illegal goods and services are still exchanged in exchange for bitcoins.

The adoption of Bitcoin as the main exchange currency for criminal activity in cyberspace became apparent from the shutdown of Silk Road—the first illicit online marketplace—by US authorities in 2013. Since then, references to the use of cryptocurrencies for illicit purposes have been repeatedly made in documents from various law enforcement agencies or organizations. Thus, Europol's Internet Organized Crime Threat Assessment (IOCTA) reports noted the growing adoption of Bitcoin as a preferred currency among criminal organizations, replacing other VAs.[5] In

[1] Refer to: European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses," Policy Department for Citizen's Rights and Constitutional Affairs," May 2018, p. 21.
[2] This definition excludes digital representations of fiat currencies, securities or other financial assets covered by other sections of the FATF Recommendations.
[3] Refer to: NAKAMOTO, Satoshi: "Bitcoin: A peer-to-peer electronic cash system," 2008.
[4] In relation to that issue, an academic paper published in 2019 highlighted the emergence of more than 170 "cryptofunds" (investment funds dedicated exclusively to cryptocurrencies) with assets more than USD 2.3 billion. Refer to: 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, No. 5, 2019, pp. 1798/1853.
[5] Refer to: European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses," Policy Department for Citizen's Rights and Constitutional Affairs," May 2018, pp. 15/18.

this context, a recent study estimates that 26% of Bitcoin users and 46% of Bitcoin transactions are associated with illegal activities.[6]

Specifically with regard to money laundering and terrorist financing (ML/TF), one of the first mentions of the possibility of using bitcoins for this purpose can be found in an FBI report produced in 2012.[7] Since then, numerous documents from organizations dedicated to crime prevention in general and money laundering in particular have confirmed the consolidation of the use of cryptocurrencies as a method to recycle illicit funds coming not only from criminal activities in cyberspace (online sale of illegal goods and services, ransomware, extortion, VA theft through hacking, etc.), but also from crimes committed in the physical world.

The FATF had already warned about the possibility that the evolution of information and communication technologies (ICTs) could generate new ML/TF vulnerabilities and typologies in its report on new payment methods, published in 2006.[8] The issue was revisited in a 2010 report[9] that highlighted the growth in the number of cases of illicit use of new payment methods reported by member countries, while highlighting the importance of implementing customer due diligence (CDD) measures at access points to these new technologies as a way to mitigate ML risks.

Subsequently, cryptocurrencies became increasingly prevalent among new payment methods until they took a central role as an exchange currency in illicit transactions. The FATF addressed the issue in the report on "virtual currencies" published in 2014,[10] in which it analyzed the ML/TF risks linked to cryptocurrencies, which it considered particularly vulnerable to exploitation for criminal purposes. A year later, in its "Guidance for a risk-based approach: virtual currencies"[11] the FATF set out a series of guidelines for better implementation of the 40 Recommendations in order to minimize potential risks, highlighting, once again, the desirability of focusing AML/CFT measures on the intersection between the cryptocurrency and fiat currency ecosystems.

In these reports, the FATF identified the following as the main features that increase ML/TF risk: (a) the anonymity associated with the design of VAs (which can even be increased through the use of tools such as "mixers" or "tumblers"; (b) the possibility of the same person controlling multiple "virtual wallets"; (c) the decentralized nature of most cryptocurrencies (which implies the lack of a supervisory body covered by AML/CFT regulations); and (d) the global reach of many of them, among others.

---

[6] Refer to: 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, No. 5, 2019, pp. 1798/1853. It is worth noting, however, that since 2016, the proportion of Bitcoin activity linked to illegal trafficking has been steadily declining, largely due to the rapid growth of speculative interest in Bitcoin thanks to the increase in its value.
[7] Refer to: Federal Bureau of Investigations (FBI): "Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity," Criminal Intelligence Section / Cyber Intelligence Section, April 2012.
[8] Refer to: FATF: "Report on new payment methods," October 2006.
[9] Refer to: FATF: "Money laundering using new payment methods," October 2010.
[10] Refer to: FATF: "Virtual currencies. Key definitions and potential AML/CFT risks," June 2014.
[11] Refer to: FATF: "Guidance for a risk-based approach: Virtual currencies," June 2015.

In response to this, in October 2018, the FATF updated Recommendation 15, referring to the fundamental obligations of member countries with respect to the risk-based approach (RBA) towards new technologies, in order to clarify its application to VAs, activities related thereto, and to VA service providers (or VASPs).[12] Then, in 2019, the FATF adopted a new Interpretative Note to Recommendation 15 to further clarify how standards and measures for the regulation and supervision of the activities of VAs and VASPs should be applied.

In the same year, the FATF published a guide with recommendations for an RBA.[13] In that guidance it highlighted the risks arising from the inconsistent application, at the international level, of the body's parameters for the AML/CFT obligations of VASPs, noting that, given the inherently cross-border nature of the Internet, a VASP based in one jurisdiction may offer its products and services to customers located in any other, where it is subject to different duties and supervisory standards, which is a concern when the provider is located in a jurisdiction with weak or non-existent controls. Then, in September 2020, the FATF issued updated guidance on VA risk indicators and red flags.[14]

Vulnerabilities resulting from regulatory divergences are accentuated due to the wide range of providers in the AML/CFT field and their presence in multiple jurisdictions, which make it difficult to determine which entities or persons (natural or legal) involved in these types of transactions are subject to AML/CFT measures and which country or countries are responsible for regulating and supervising compliance. Likewise, in a subsequent report on "so-called stablecoins,"[15] the FATF recognized the existence of identical risks in relation to this type of VA.[16]

At the regional level, the Group of Experts for the Control of Money Laundering of the Organization of American States (OAS) highlighted the ML/TF risks associated with cryptocurrencies. On the European continent, the issue of virtual currencies was first analyzed in a 2012 European Central Bank (ECB) report.[17] The following year, the European Banking Authority (EBA) issued a warning to consumers regarding VAs,[18] stating that the illicit use of such assets could put their funds at risk. To mitigate such risks, it recommended including virtual currencies in the scope of the European Anti-Money Laundering Directive (AMLD). Then, in an opinion issued

[12] Defined by the FATF as a natural or legal person (not covered by any other definition in the Recommendations), who conducts one or more of the following transactions commercially for the benefit of another legal or natural person: (*i*) Exchange between virtual assets and legal currency; *(ii)* Exchange between one or more forms of virtual assets; *(iii)* Transfer of virtual assets (understood as the movement of such assets from one virtual address or account to another); *(iv)* Custody or administration of virtual assets or instruments that allow controlling virtual assets; and *(v)* participation in or provision of financial services linked to the offer and/or sale of virtual assets by users.
[13] Refer to: FATF: "Virtual assets and virtual assets service providers. Guidance for a risk-based approach," June 2019. In October 2021, the organization will publish an update to said guidance.
[14] Refer to: FATF: "Money laundering and terrorist financing red flag indicators associated with virtual assets," September 2020.
[15] This is the name given to cryptocurrencies that have the support of large technology or financial companies, which are claimed to be more stable than other cryptocurrencies.
[16] Refer to: FATF: "FATF report to the G20 Ministers and Central Bank governors on the so-called stablecoins". June 2020.
[17] Refer to: European Central Bank (ECB): "Virtual currency schemes," Frankfurt, October 2012.
[18] Refer to: European Banking Authority (EBA): "Warning to consumers on cryptocurrencies," December 2013.

in 2014,[19] the same entity identified more than 70 risks associated with virtual currencies, while reiterating the need for regulation on the matter. The EBA reiterated this position in a subsequent opinion, published in 2016.[20]

Moreover, the 2019 Internet Organized Crime Threat Assessment (IOCTA) highlighted the use of cryptocurrencies to facilitate online crime, urging law enforcement agencies (LEAs) to develop, share, and propagate knowledge on how to recognize, track, seize, and recover VAs.[21] More recently, a joint paper by Interpol, the on Basel Institute on Governance and Europol also emphasized the importance of member countries or states establishing clear regulatory frameworks and processes to support the AML/CFT registration and supervision of VASPs, in line with FATF recommendations.[22] Similarly, in 2020, both the Financial Stability Institute and the Basel Committee on Banking Supervision published documents highlighting the existence of ML/TF risks arising from the use of cryptoassets and the need for adequate regulation.[23]

Likewise, during the last decade, the concern of international organizations regarding the possible use of cryptocurrencies to facilitate the financing of terrorism, especially as a means to (semi-) anonymously channel donations or contributions to terrorist organizations, has been accentuated. In this regard, the 2012 ECB report on virtual currencies already emphasized, in relation to the emergence of Bitcoin, that the degree of anonymity associated with this asset posed a TF risk. In turn, the EBA explained, in 2014, that the TF risk resulting from the use of virtual currencies derives from the fact that the schemes referred to these assets are not restricted by jurisdictional boundaries, since they are accepted across borders. In this regard, it pointed out that all that was required to operate with VAs was an Internet connection; that the underlying infrastructure was distributed around the globe, making it difficult to intercept transactions; and those transactions tended to be irreversible.[24]

Following the terrorist attacks in France in 2015, the European Commission proposed to analyze vulnerabilities in TF prevention policies on that continent, including those linked to the anonymous acquisition and use of virtual currencies. As a result, in 2016 the European Commission agreed to include measures similar to those recommended by the FATF and the EBA in respect of VAs in the 5th European Anti-Money Laundering Directive (5AMLD), which was adopted by the European Parliament in April 2018 and by the Council of Europe in May of the same year.

[19] Refer to: European Banking Authority (EBA): "EBA opinion on 'virtual currencies,'" EBA-Op-2014-08, July 2014.
[20] Refer to: 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, August 2016.
[21] Refer to: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe. February 2021, p. 2.
[22] Refer to: INTERPOL / Basel Institute on Governance / EUROPOL: "Recommendations 4th Global Conference on Criminal Finances and Cryptocurrencies". November 2020.
[23] Refer to: Basel Committee on Banking Supervision: "Prudential treatment of cryptoasset exposures," Bank for International Settlements (BIS) Consultative Document, June 2021; and Financial Stability Institute (FSI): "Supervising cryptoassets for anti-money laundering," FSI Insights on Policy Implementation, No. 31, BSI, April 2021.
[24] Refer to: European Banking Authority (EBA): "EBA opinion on 'virtual currencies,'" EBA-Op-2014-08, July 2014, p. 33 § 120.

Notwithstanding the above, a 2018 European Parliament report noted, in relation to these risks, that the number of extremists who have turned to cryptocurrencies (attracted by the perception of anonymity and their decentralized structure) is still low. It was explained, in this regard, that, in the short term, the most significant risk comes from the possibility of using VAs to purchase illegal items (such as weapons or explosives) on the Dark Web, or to raise funds through anonymous donations.[25] The report concludes, however, that for the time being VAs do not provide substantial benefits for most terrorist organizations compared to established TF methodologies.[26]

The challenge of maintaining AML/CFT standards in the new scenario posed by the widespread global use of cryptocurrencies as currency (both in the context of licit and illicit transactions) is not limited to updating regulatory frameworks so that registration, information, and reporting obligations also reach the VAs and VASPs that are continually being incorporated into the global financial markets. This is because, given the special characteristics of VAs, their exploitation for illicit purposes may affect the effectiveness of asset investigations and the possibility of seizing or confiscating assets of illicit origin or destination, both aspects that have been considered by the FATF as central elements of the AML/CFT standards and of the national regimes on the matter.[27]

Indeed, the fact that transactions with cryptocurrencies and other similar VAs take place almost entirely in a virtual environment and almost completely detached from the physical world (the so-called "cyberspace"), imposes a paradigm shift in everything related to the strategies, methods, and tools used to investigate, prosecute, and punish ML/TF activities committed through VAs, as well as for the seizure and confiscation of the funds involved in them.

Thus, since the existence of cyberspace means that crime is no longer territorial and borders become irrelevant to the perpetrator, criminals are favored, and law enforcement agencies are harmed. The process of investigation and evidence gathering is dramatically changed, forcing the use of technological tools to carry out tasks with already established procedures. In such a context, there are complexities in the prosecution of crimes, which is hampered by factors such as difficulties in government procurement of technological tools, limited use of ICTs by LEAs, and certain biases in the culture of LEAs regarding the needs and skills required for the use of new technologies.[28]

In order to sustain the effectiveness of asset investigations in the virtual environment, with all the challenges that this entails, the national authorities in charge of investigating, identifying, seizing,

[25] In this regard, a 2018 FATF report highlights a case in which a propaganda website of the terrorist organization ISIS was exploited to solicit donations in Bitcoin (refer to: FATF: "Financing of terrorism for recruitment purposes," October 2018).
[26] Refer to: European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses," Policy Department for Citizen's Rights and Constitutional Affairs," May 2018, p. 27.
[27] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 7 § 1.
[28] Refer to: McQUADE, Samuel: "Cybercrime," in TONRY, Samuel, *The Oxford handbook of crime and public policy*, Oxford University Press, 2011.

and confiscating VAs need to adapt their approach to the new technological reality in which they must operate. This adaptation demands the adoption of new investigation strategies based on the scenario created by the technological evolution of the last two decades, with a multidisciplinary approach and using new investigative tools linked to information technology, in line with FATF Recommendations 30 and 31.

In this scenario, the purpose of this *guide on relevant aspects and appropriate steps for the investigation, identification, seizure, and confiscation of VAs* is to offer ideas, concepts, and good practices that are useful for all operators in GAFILAT member countries to ensure greater efficiency in investigations related to criminal maneuvers involving VAs, their seizure and confiscation. In view of the differences between the various national jurisdictions in which they may be applied, these ideas, concepts and good practices are presented in general terms, leaving it up to the authorities of each country to define how they should be adapted to the normative, regulatory, political, economic, and social reality of their territory.

EXECUTIVE SUMMARY

This "Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets" is the first best practices document prepared by GAFILAT on the subject, with the aim of promoting the development and strengthening of capacities for the identification and localization of this type of assets by GAFILAT's Asset Recovery Network (RRAG) contact points and, through them, specialized units of the Public Prosecutor's Office, law enforcement agencies, and other investigative agencies dedicated to the identification, seizure, and confiscation of assets linked to ML/TF in Latin America. In this regard, the purpose of this guide is to offer ideas, concepts and good practices that are useful for all operators in GAFILAT member countries to ensure greater efficiency in investigations related to criminal maneuvers involving VAs, their seizure and confiscation. In particular, it aims to help reconcile the regulatory structures, tools and strategies currently in use for asset investigation and asset recovery—designed to be used for ML/TF operations carried out in the "physical" or "real" world—with the new scenario represented by the emergence of VAs, the specific scope of which is cyberspace.

Over the last decade, VAs, and especially cryptocurrencies, have come to occupy a central place as a currency of exchange in illicit transactions carried out, above all, in illegal marketplaces operating on the Internet. The FATF has referred to them in different documents published since 2014, in which it identified anonymity associated with the design of VAs, the possibility of the same person controlling multiple "virtual wallets," the decentralized nature of most cryptocurrencies, and the global reach of many of them, among others, as the main features that increase the risk of ML/TF. The evolution of this phenomenon resulted in the agency updating Recommendation 15 and developing its Interpretative Note, referring to the fundamental obligations of member countries with respect to the RBA related to new technologies, in order to clarify its application to VAs, related activities, and VASPs.

In this regard, the guide contains a detailed analysis of the problems inherent to the investigation, seizure, and confiscation of VAs of illicit origin or used for ML/TF, describing both the typologies associated with this type of assets, the technological context in which they are developed, the tools available to criminals to hinder the action of the authorities, and the consequences arising from their use. It also describes the aspects of the new technological ecosystem that favor the action of the LEAs, the new investigation strategies and techniques that can be adopted, and the technological tools available for this purpose.

Taking as a starting point the scenario described above, the guide lists a series of recommendations related to the effective regulation of VA ecosystem's operators (with special emphasis on those that serve as a nexus between fiat and virtual currency); the sources of information available to LEAs to feed asset investigations on ML/TF conducts involving VAs; the identification of "red flags" on the possible configuration of this kind of behaviors; the elements of the technological architecture that supports the use of VAs, which can be exploited for greater effectiveness in

investigations; their combination with traditional investigative measures and those that have emerged in recent decades from the evolution of VA technologies, and communication technologies (ICTs) (in particular, automated or electronic surveillance tools, the undercover computer agent, and the use of spyware); and everything related to the planning and execution of seizure or confiscation of VAs, including their treatment once they are in possession of the authorities. It also includes recommendations on personnel training and international cooperation in the investigation, seizure, or confiscation of VAs, including a list of international agencies or organizations that can be called upon for this purpose.

As a complement, the guide includes an annex with a synthesis of all the recommendations contained in the main document, in order to facilitate their analysis by the LEAs and/or specialized units of the Public Prosecutor's Office, as well as the contact points of the RRAG, to whom this document is addressed. It also includes a second annex with comparative legislation on the regulation concerning the use of advanced computer tools for investigation or surveillance, which may be useful either as a reference for their eventual incorporation into the procedural regulations of the countries of the region or for their analogical application, where possible, in accordance with the legal principles in force.

II. METHODOLOGY

A. Starting Point

1. Within the framework of the conclusions, recommendations, and priorities outlined at the XVII General Meeting of the GAFILAT Asset Recovery Network (RRAG) Contact Points, which took place in November 2020, the possibility was raised of developing good practices or technical documents on topics of interest to contact points and their institutions, including the investigation, identification, seizure, and confiscation of VAs and the implementation of special investigative techniques.

2. In particular, it was noted that the development and strengthening of skills for the identification and tracing of VAs is an inevitable challenge for the RRAG's contact points. In this regard, the members of the Network themselves identified this problem as a central aspect for the development of their tasks and made it a priority.

3. This "Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets" is the result of this recognition. It is addressed to RRAG contact points and, through them, to specialized units of the Public Prosecutor's Office, law enforcement agencies, and other investigative agencies dedicated to the identification, seizure, and confiscation of ML/TF-related assets in Latin America.

4. The purpose of this guide is to help reconcile the regulatory structures, tools, and strategies currently in use for asset investigation and asset recovery—designed to be used for ML/TF operations carried out in the "physical" or "real" world—with the new scenario represented by the emergence of VAs, the specific scope of which is the "virtual" world or cyberspace.

B. Scope

5. In view of the objectives set out for the guide, its scope is limited to the analysis of issues that have a practical impact on the investigation of ML/TF conducts involving VAs. Therefore, the general study of the phenomenon known as "Fintech" (understood as the confluence between technology and the provision of financial products and services) is excluded, within which the emergence of VAs (and especially cryptocurrencies) represents only one of the multiple variants within a much broader universe, comprising a wide range of activities that includes the provision of banking services through digital channels not associated with banking institutions, credit assessment based on alternative data, peer-to-peer (P2P) lending to the unbanked, the use of blockchain technology for smart contracts, digital currencies issued by central banks, initial offerings of virtual currencies, and algorithmic investment strategies, among others.

6. The focus of the analysis is on the problems related to centralized and decentralized VAs, with special emphasis on the use of cryptocurrencies for ML/TF purposes. This also

includes the "so called stable-coins." This is because this type of asset presents many of the same ML/TF risks found in other VAs, stemming from their potential for anonymity, global reach, and their possible use for the layering of illicitly sourced funds. These vulnerabilities increase in the event that these currencies are massively adopted, which, although it has not yet occurred, may happen in the near future with the release of "stable currencies" sponsored by large financial, technology, or telecommunications companies.[29]

7. Likewise, with regard to cryptocurrencies, it is important to bear in mind that, although Bitcoin, Ethereum, and Ripple are the best known, in practice all of them are, to a greater or lesser extent, susceptible to being exploited for ML/TF. However, given the vast amount of this type of VAs in circulation (as of March 2020, there were 5,183 known cryptocurrencies),[30] the main focus is on Bitcoin, which holds a predominant place in the market, as well as on widely used Altcoins, and on the so-called "private currencies," such as Monero and ZCash.

8. This guide has been conceived to be applied in the 17 countries that make up GAFILAT, which represent a geographical, political, and social diversity, which in turn results in a great diversity in terms of the regulatory reality prevailing in each jurisdiction, as well as the integration and operation of the agencies in charge of the investigation, seizure, and confiscation of ML/TF-related assets. Consequently, both the analysis and the recommendations are made on a general basis, so that the addressees of the recommendations can adapt their provisions to the specific context of each country where they are to be applied.

C. Methodology

9. The analysis carried out for the purpose of preparing this guide included the following issues: (a) the functioning of VAs, the ML/TF risks associated with them and the consequent need for effective regulation, at the international level, aimed at mitigating them; (b) the special characteristics of the investigation of crimes committed in the virtual environment (including ML/TF conducts with VAs), the difficulties related to the identification of those responsible, the reconstruction of the transactions, and the confiscation or seizure of the funds involved; and (c) the new technological tools available to LEAs to achieve greater effectiveness in asset investigations related to the matter.

10. In this context, a diagnosis was prepared on the situation in Latin America in relation to the treatment of VAs, the supervision of persons or entities that provide services related to them (VASPs), and the possible implementation of new strategies and technological tools in order to achieve greater effectiveness in asset investigations related to ML/TF conducts involving VAs.

[29] Refer to FATF: "Report to the G20 finance ministers and central bank governors on so-called Stablecoins". June 2020, sections §§ 1 and 4.
[30] Refer to: ALLEN, Franklin / GU, Xian / JAGTIANI, Julapa: "A survey of Fintech research and policy discussion," Federal Reserve Bank of Philadelphia Research Department, Working Papers 20-21, June 2020, p. 18.

11. To this end, a survey of the regulatory and normative reality of the region was carried out by means of a questionnaire addressed to GAFILAT countries, in addition to the RRAG contact points. This survey emphasized two central issues:

a) In the first place, the situation regarding compliance with the standards established in FATF Recommendation 15 and its Interpretive Note (as well as the guidelines and reports of the organization in relation to the matter) in order to regulate the duties of AML/CFT in terms of VAs and VASPs. This is because the degree of adequacy they present not only has an impact on the possible generation of alerts on suspicious ML/TF transactions involving this type of assets, but also on the possibility that the agencies in charge of the investigation, identification, seizure, and confiscation of VAs have a source of accurate and detailed information about the natural or legal persons that operate with this type of assets, which may be of paramount importance for the success of the asset investigations that target them.

b) Second, the identification of the resources available to the LEAs or specialized units of the Public Prosecutor's Offices in Latin America to investigate, identify, seize, and confiscate VAs. In this context, an attempt was made to determine the regulatory situation in the region in terms of the possible adoption of the technological investigation techniques and tools described above, which is essential for an effective identification and prosecution of ML/TF activities related to cryptocurrencies.

12. The result of this survey constituted the fundamental input for the preparation of a diagnosis on the situation of the region in the face of the new scenario of the growing adoption VAs and their potential exploitation for ML/TF. However, to that effect, the information obtained by GAFILAT in the framework of the 4th Round of Mutual Evaluations on compliance with FATF Standards, particularly to Recommendation 4 and 38, was also analyzed, as well as that collected by the OAS Group of Experts for the Control of Money Laundering as a result of a study on cryptocurrencies agreed at the meeting of that group in 2016, in the framework of which a questionnaire was circulated between 2017 and 2018.

13. In addition, other inputs were taken into consideration such as:

- Interviews with officials from the Organization of American States (OAS), CARIN, World Bank, and ICAR.

- Documents published by various international organizations, starting with FATF reports and guidelines and continuing with documents from Interpol, Europol, the Basel Institute on Governance, the Basel Committee on Banking Supervision, the Financial Stability Institute (FSI), CARIN, the Association of Certified Anti-Money Laundering

Specialists (ACAMS), the European Central Bank (ECB), the European Banking Authority (EBA), the European Parliament and the FBI, among others (as well as in numerous academic publications on the subject) reflecting the ML/TF risks associated with VAs and the consequent need for effective regulation, at the international level, aimed at mitigating them.

- Documents from international organizations and academic material referring to the operation of VAs in general and cryptocurrencies in particular, reflecting both the obstacles they pose for a financial investigation, as well as the possibilities that such operation offers for obtaining evidence and/or relevant information for the identification and prosecution of ML/TF conducts with VAs. As well as with regard to the seizure and/or confiscation of this type of assets. In this regard, the guides published on the subject by the FATF, UNODC, the Council of Europe and the Regional Organized Crime Information Center (ROCIC) stand out.

- Documents from international organizations and academic material on the impact of technological advances on the investigation of cybercrime, and the need to adopt new strategies and implement the use of new tools in order to effectively combat this type of crime. For example, documents published by the OAS Working Group on Cybercrime, the Basel Institute on Governance, the European Parliament, Interpol, Europol, the International Association of Chiefs of Police (IACP) and the Police Executive Research Forum (PERF).

- International instruments related to the implementation of innovative tools for the investigation of cybercrime, including the Council of Europe Convention on Cybercrime (Budapest Convention); the ITU/CARICOM/CTU Model Legislative Texts, the Draft African Union Convention, the Commonwealth Model Law, the ECOWAS Draft Directive and the League of Arab States Convention. There are also examples of specific regulation of the use of new surveillance or technological research techniques in Spain, France, England, the Netherlands, and Poland.

D. Elaboration Process

14. The process of preparing the guide was divided into four phases or stages: 1. Preparatory stage; 2. Study stage; 3. Diagnostic stage and preliminary report; and 4. Final stage.

15. The Preparatory stage included the compilation and analysis of reports from specialized agencies and academic material on the issues covered by this guide, as well as the preparation, in coordination with the GAFILAT Executive Secretariat and the German Development Cooperation implemented by GIZ, of the draft questionnaire addressed to GAFILAT countries and RRAG contact points in order to obtain information on: (a) local regulation on cryptocurrencies; (b) local

AML/CFT regulation in relation to VASPs; (c) local regulations on seizure and confiscation; and (d) local procedural regulations on technological and/or IT investigative techniques.

16. During the Study stage, the Work Plan was developed together with GAFILAT's ES, which coordinated the distribution of the questionnaires. Then, the responses received were compiled and systematized, and finally, interviews were held with representatives of the OAS, CARIN, the World Bank, and ICAR.

17. In the Diagnostic phase, based on the information gathered during the previous phases, an assessment was made of the regional situation regarding the regulation, investigation, seizure, and confiscation of VAs, identifying the sources of information and the legal tools provided for in the regulations, as well as the margin for action for the implementation of new technological research measures.

18. In the final stage, and taking this diagnosis as a starting point, a preliminary report was prepared, focusing on the identification of strategies for the effective use of the contact points between the "virtual" and the "physical" universe in asset investigations, as well as investigative methods and tools appropriate to the reality of cyberspace and the current technological context.

19. The last step consisted of drafting the final document and its approval by the GAFILAT Executive Secretariat.

E. Structure

20. This guide is structured as follows: following the introduction (Section I) and this review of the methodology used (Section II), there are definitions of the technical terms used in the guide (Section III); the analysis of the information obtained regarding the problems of asset investigation, seizure, and confiscation of VAs, with special reference to the regional context (Section IV); and, finally, the recommendations and appropriate steps for the investigation, identification, seizure, and confiscation of VAs (Section V).

21. An overview of good practices for the investigation, identification, seizure, and confiscation of VAs linked to proceeds of crime is included as **Annex I**, and an analysis of comparative legislation on the implementation of technological investigative tools is included as **Annex II**.

III. DEFINITIONS

Related to virtual assets

22. **Virtual Asset (VA):** As defined by the FATF, a digital representation of value that can be digitally exchanged or transferred and used as a form of payment or investment instrument. VAs do not include digital representations of fiat currency, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.

23. **Fiat money:** It refers to real (non-virtual) currency or money, or national currency. It differs from virtual currency in that it functions as the currency and paper money of a country, designated as legal tender; it circulates, is used, and accepted as a means of exchange in the country of issuance.

24. **Convertible (or open) virtual asset:** It is one that has an equivalent value in fiat currency and can be converted from or into that type of currency. Examples: Second Life Linden Dollars, or WebMoney.

25. **Non-convertible (or closed) virtual asset:** It is intended to be specific to a particular domain or virtual world, such as those created within the "Massively Multiplayer Online Role-Playing Games" (MMORPG) or Amazon.com, which is why the rules that regulate their use prohibit exchanging them for fiat currency. Examples: Project Entropia Dollars, Q Coins, and World of Warcraft Gold. This does not imply that non-convertible VAs can be traded for fiat currency (or cryptocurrencies) in a secondary market, which may be subject to sanctions by the administrator. All non-convertible virtual assets are centralized.

26. **Centralized virtual assets:** They are those that answer to a single central authority (administrator), which is a third party that controls the system. The administrator issues the VA, sets the rules for its use, maintains a central ledger of payments, and has the authority to redeem the currency (withdraw it from circulation). Examples: Examples: Second Life "Linden dollars," PerfectMoney, WebMoney "WM units," and World of Warcraft gold.

27. **Decentralized virtual assets:** These are distributed, open-source, peer-to-peer virtual assets without a central management, monitoring, and supervisory authority. The main exponents of decentralized VAs are cryptocurrencies.

28. **Cryptocurrencies:** These are open source, convertible and decentralized VAs that operate in a distributed peer-to-peer network that applies mathematical and cryptographic principles to provide security to the system. Transfers between users are carried out "peer-to-peer," without intermediaries, based on a set of public and private cryptographic keys, and require cryptographic signature to be completed. The transparency of the system is ensured by the recording of

transactions in a sort of distributed "ledger" (called Blockchain in most cryptocurrencies), maintained by a network of mutually "untrusted" parties (called "miners" in the Bitcoin and other cryptocurrencies ecosystem) that elaborate the cryptographic blocks of the chain and are rewarded for it with fees paid by the users.

29. **Bitcoin:** Launched in 2009, it was the first decentralized convertible VA, and the first cryptocurrency. Bitcoins are account units composed of unique alphanumeric sequences that constitute units of currency (divisible, in turn, into smaller units, called Satoshis) and have value only because individual users are willing to pay for them. Bitcoins are traded digitally between users in a partially anonymous form (the persons or entities involved in each transaction are identified only by alphanumeric pseudonyms called "Bitcoin addresses") and can be exchanged for fiat currency or other cryptocurrencies. The software required to send, receive, and store bitcoins or to monitor transactions can be downloaded free of charge. Users can also obtain their Bitcoin addresses (which function as accounts) from Bitcoin exchange platforms or online wallet services. Transactions (flows of funds) are recorded in a shared public registry (the "blockchain"), where they are identified by Bitcoin addresses.

30. **Altcoin:** The term refers to any mathematically grounded decentralized convertible virtual currency that is mathematically distinct from the original Bitcoin. There are currently thousands of Altcoins. Among the most important ones, the following are worth mentioning:

a) **Litecoin (LTC)** was launched in 2011. It was one of the first Altcoins after Bitcoin. While it resembles the latter in many respects, block generation is faster, which increases the speed of transaction confirmation.
b) **Ethereum (ETH)**: It is a decentralized software platform that allows the execution and development of "Smart contracts" and distributed applications (DApps) without interference from third parties. Ether is the cryptographic token with which Ethereum-based applications run.
c) **Dash (DASH)**: Originally known as Darkcoin, it is a more private version of Bitcoin. It offers a higher level of anonymity, as it runs on a decentralized network that makes it difficult to trace transactions.

31. **Ripple (XRP):** It is a global payment clearing network that offers the possibility of instant, certain, and low-cost transfers. Its registration does not require mining (which distinguishes it from most cryptocurrencies), which reduces the use of computational capacity and latency (delay) in the network.

32. **Bitcoin Cash (BCH)**: It is a derivation of Bitcoin, whose main difference is that it allows a higher flow of transactions per second, which in turn results in lower fees.

33. **"So-called stablecoins"** are VAs that indicate that they maintain a stable value in relation to one or more reference assets (which may be fiat currencies, other virtual assets, securities, commodities, or real estate assets). The term does not respond to a legal or regulatory classification but is generally used as an advertising term. Depending on the design of the VA in question, it may be classified as a currency or as a "financial asset" (such as securities) in accordance with the standards set by the FATF.

Related to technologies associated to virtual assets

34. **VA or cryptocurrency address (e.g., Bitcoin address):** It is an alphanumeric code that identifies the virtual location associated with a certain amount of VAs, necessary to be able to send or receive cryptocurrencies. It works like a bank account in the traditional financial system to receive or send transfers. For example, Bitcoin addresses are between 26 and 32 characters long. They start with the number 1 for standard addresses and number 3 for multi-signature addresses. Other cryptocurrencies have their own systems for representing their addresses. VA addresses can also be represented by means of QR codes.

35. **QR codes:** They are a graphical representation created by a graphical hash algorithm, meaning that it always provides the same graph if the same information is entered. When used in connection with cryptocurrencies, it allows the Bitcoin address to be shared more easily, since the code can be scanned using a smartphone camera.

36. **Blockchain:** It is a form of registry or "ledger" used by Bitcoin and most cryptocurrencies and works by chaining together blocks of data. Each of these blocks contains information about the transaction being carried out. The initial and final elements of the block are related, respectively, to the previous and next block. Thus, modification of the block would corrupt the entire chain, although it is practically impossible to alter it. In addition, blockchain-based technology works in a distributed fashion, with multiple computers operating simultaneously with the chain, which makes it extremely difficult to compromise it through a computer attack. Each cryptocurrency has its own Blockchain.

37. **Distributed ledger technology (DLT):** It is a data structure that is geographically distributed, so that the information in the database is processed simultaneously by multiple servers, without the existence of a main administrator. It is essentially a database managed by a group of participants, each of whom has a copy of the registry, so that any variations are easy to detect, since updates to the database can only be made by consensus of all the participants.

38. **Public/private key set:** The main cryptocurrencies, such as Bitcoin, are built on the basis of asymmetric cryptography technology, which uses a public/private key set. The former can be known by anyone, the latter is confidential. In the Bitcoin ecosystem, the public key is derived

from the private key through a one-way cryptographic function known as "Elliptic curve multiplication."

39. **Private key:** It is a random number that functions as a secret key, generated through an asymmetric cryptographic process, and is used to safeguard the ownership and management of cryptocurrencies. During the process of creating a VA wallet, first the private key is generated and then, from it, the public key, which is mathematically related to the former. The process, however, is impossible to realize in reverse (deducting the private key from the public one), providing a high level of security. The private key is the one that assigns to the holder the control of the funds associated with a given VA address.

40. **Public key:** It is an identifier that can be shared to enable the transfer of VAs to third parties. It is one of the two parts of the set of keys created by asymmetric cryptography to share secrets securely.

41. **Cryptocurrency wallets:** They are software applications that allow interacting with the VA Blockchain in order to generate and/or store cryptocurrency addresses and their corresponding public/private key sets. It is an interface that allows users to manage, transfer or receive VAs. There are several types of VA wallets.

42. **Hosted / Custodial wallets:** These are virtual wallets that are hosted on an external server (i.e., in "the cloud"), and are offered through VA wallet service providers. The name refers to the fact that the private keys are not held by VA holders, but "in custody" of the service provider.

43. **Hybrid wallets:** These are hosted wallets, but not "in custody," since, although they are hosted on the servers of a service provider, the user retains control over the private key(s).

44. **Self-custody/ Self-hosted wallets:** These are the wallets that cryptocurrency users themselves keep in their possession, for their own use of the VAs associated with the addresses stored in them. These wallets may be virtual or hardware wallets.

45. **Software wallets:** These are downloadable desktop or mobile applications that can be kept on a desktop computer or on a mobile device (smartphone) to enable secure storage of keys on the device.

46. **Hardware wallets:** They are wallet applications hosted on physical devices such as pen drives or USB, which allow the user to store his/her keys offline, on portable physical devices such as pen drives.

47. **Paper wallets:** These are sheets of paper or other material on which the cryptocurrency addresses, and the set of public/private keys used to manage the exchange of

cryptocurrencies are printed, either in plaintext format or in the form of a QR code, by means of a VA wallet program. They are used for the storage and safekeeping of funds that will not be used or moved for a long time, since they offer a higher level of security, as they are not susceptible to cyber theft.

48. **Cold storage:** It refers to wallets that are not connected to the Internet, such as hardware or paper wallets. The purpose of **"cold storage"** variants is to provide protection against hacking or theft of cryptocurrencies.

49. **Hot storage:** In contrast to the previous one, this refers to VA wallets that operate online, i.e., with an Internet connection. As a result, this form of storage is more vulnerable to hacking/theft than cold storage.

50. **Multi-signature wallets:** These are applications that provide an additional level of security by requiring the use of multiple private keys to authorize a transaction, thereby reducing the risk of cryptocurrency theft if a single private key is compromised.

51. **State-controlled wallets:** This is a wallet (of any kind) that is under the control of a government authority (it can be a state agency specialized in handling seized assets, a law enforcement agency, a prosecutor's office, a jurisdictional body or even a private company collaborating with the state), to which VAs that are seized or confiscated are transferred.

52. **"Seed words" or "Seed phrase":** They are used by many VA wallet applications to generate private keys from a single "seed," which takes the form of a mnemonic consisting of a sequence of between 12 and 24 words in different languages (English, Japanese, Korean, Spanish, Chinese, French, and Italian), which function as a backup for the wallet, allowing that in case of loss of control over the wallet (for example, due to theft, loss or technical malfunction of the device in which it is stored), it is possible to recreate it by entering the words in the order originally provided in the corresponding application.

53. A **Mnemonic** is, in computer science, a word or phrase that substitutes an operation code (machine language), thus making programming easier.

54. **Massively multiplayer online role-playing games (MMORPGs):** They are video games that allow thousands of players to enter simultaneously into a virtual world through the Internet and interact with each other.

Related to players in the virtual asset ecosystem

55. **User:** It is the person or entity that obtains a VA and uses it to purchase physical or virtual goods or services, or to transfer them to another person, or to hold it as an investment. VAs can

be obtained in several ways. Namely: (1) by acquiring them in exchange for fiat currency (either on a VA exchange platform or, in the case of centralized assets, directly from the administrator or issuer); (2) by carrying out tasks that are rewarded through payments in VAs; and/or (3) in the case of decentralized VAs—such as Bitcoin—by self-generating units of the cryptocurrency through participation in the "mining" process.

56. **Miner:** A person or entity that intervenes in the decentralized network of a cryptocurrency using special software to solve complex algorithms within the "proof-of-work" system used by the system to validate transactions.

57. **Administrator:** The person or entity commercially engaged in the issuance (putting into circulation) of centralized VAs, who is also responsible for setting the rules of use and maintaining the central payment registry, as well as holding the authority to withdraw the assets in question from circulation.

58. **Virtual Asset Service Providers (VASPs):** As defined by the FATF, comprises any natural or legal person not covered elsewhere under the Recommendations who, as a business, carries out one or more of the following activities or transactions for/on behalf of another natural or legal person:

i. Exchange between virtual assets and fiat currency.
ii. Exchange between one or more forms of VAs.
iii. Transfer of VAs.
iv. Custody or administration of VAs or instruments that allow controlling VAs; and
v. Participation in, and provision of financial services in connection with an issuer's offering or sale of a VA.

59. **VA/cryptocurrency exchange platforms (cryptocurrency exchanges):** These are those operated by persons or entities commercially engaged in the exchange of cryptocurrencies for fiat currency, funds, precious metals, or other cryptocurrencies (or vice versa), in exchange for a fee (commission). They generally accept a wide variety of payment methods (cash, wire transfers, credit cards or other cryptocurrencies) and are used to deposit or withdraw funds from VA accounts.

60. **Cryptocurrency wallet service providers:** Also covered by the FATF definition of VASPs, these are persons or entities that offer as a service the provision of wallets (either hosted "in custody" or hybrid). When "custodial" wallets are offered, this type of provider facilitates participation in the VA ecosystem by simplifying the performance of transactions for users. They are responsible for maintaining the customers' balance and usually also offer security with respect to cryptocurrency storage and transactions. In that direction, they can provide services such as

encryption, back up or "cold storage" of the wallets, protection through multiple signatures or mixers.

61. **Mixers:** These are platforms that offer cryptocurrency users the possibility of obscuring the transaction chain in the Blockchain through the use of anonymity software tools that link multiple transactions to a single VA address and send them together in a way that makes them appear to come from a different address. The mixer or tumbler intervenes when it receives an instruction from the customer to send funds to a certain address. In order to conceal the origin and destination of the transaction, the mixer combines it with a complex and semi-random series of fictitious transactions, so as to prevent the transfer to the final destination from being associated with the address of origin. Examples of mixers are Bitmixer.io, SharedCoin, Blockchain.info, Bitcoin Laundry, Bitlaunder, Easycoin.

62. **Trading platforms:** They function as marketplaces, connecting buyers and sellers by offering them a platform where they can make and receive offers for their cryptocurrencies. Transactions between users of these platforms are carried out on a "peer-to-peer" basis, i.e., without intermediation by the platform. They are not included in the FATF definition of VASP.

63. **Peer-to-peer systems** (P2P) are communication or file exchange systems (including cryptocurrencies) in which all or some aspects operate without customers or fixed servers as intermediaries, but through a series of nodes that behave as equals ("peers") among themselves.

64. **Local Exchange Trading System (LETS):** It is a locally implemented economic organization that allows members to exchange goods and services with others in the group. LETS use a locally created currency to denominate units of value that can be traded or exchanged for goods or services. Theoretically, bitcoins could be adopted as a local currency used within a LETS. Examples: Ithica Dollars or Mazacoin.

Related to anonymity or anti-forensic tools

65. **Anonymizers or anonymity programs/tools:** These are software tools and/or services, such as darknets or mixers, which have been designed to hide the origin of a VA transaction and/or to facilitate the anonymity of Internet users.

66. **Anti-forensic tools:** These are computer tools that have been designed or may be exploited to prevent or hinder the execution of investigative measures by law enforcement agencies or state authorities.

67. **Dark wallets:** These are virtual wallets that function as browser extensions (available in Chrome and potentially Firefox) for the purpose of ensuring the anonymity of cryptocurrency transactions by incorporating the following functions: self-anonymizer (mixer), decentralized

trading, "crowdfunding" platforms, securities platforms, and information and access to online markets on the "dark web."

68. **Chain hopping:** A method used to hinder the traceability of VA transactions, which consists of "hopping" from one cryptocurrency to another (and, consequently, from one Blockchain to another) using different VA exchange platforms.

69. **Atomic swaps:** These are a variant of "chain hopping" through digital smart contracts, which make it possible to exchange one cryptocurrency for another without resorting to centralized intermediaries, such as VA exchange platforms. They are carried out between currencies operating with different blockchains, and can be concluded "off-chain," i.e.: outside the Blockchain of each cryptocurrency. The contract requires both parties to confirm reception of the funds within a predetermined period of time by means of a cryptographic hash function. If within the established period one of the parties does not confirm the transaction, the transaction is voided, and the funds are not exchanged.

70. **CoinJoin or Coin Mixing:** It is an anonymization technique that takes the form of a digital smart contract where the parties agree to commit their VAs in a new transaction, where each one ends up with the same amount of cryptocurrencies it entered with, but in which the addresses used are intermingled to make traceability difficult.

71. **Ring signature:** It is a method of anonymization that consists in the use of a group digital signature modality, according to which each member of the group has its own key, but when using it, it is impossible to know which of all of them was used to confirm a certain VA transaction.

72. **TOR (The Onion Router):** It is a distributed network of computers on the Internet that is used to conceal the true IP addresses (and therefore the true identity) of users by routing communications through multiple nodes (randomly chosen for each communication) around the world and shielding the data packets indicating the origin and destination of the communication in several layers of encryption.

73. **IP (Internet Protocol) address:** It is a unique code that identifies a given computer connected to the Internet to the rest of the computers with which it is connected. IP addresses are assigned by the user's Internet Service Provider (ISP), which assigns users certain blocks of addresses corresponding to the geographical region where they are located. No two computers connected to the Internet can have the same IP address at the same time.

74. **Dark web (Dark net):** The area of the Internet occupied by online content that can only be accessed using specialized anonymization software such as TOR.

75. **Hidden services:** These are web pages located on the "dark web," which can only be accessed through the use of anonymous communication systems such as TOR. This prevents their true location (IP address) from being identified, since they are masked by the "layered" routing provided by TOR. Communication between these sites and their users takes place through a "rendezvous point" that provides an additional layer of protection against traffic analysis.

76. **Virtual private network (VPN)** is a computer network technology that allows a secure extension of the local area network (LAN) over a public or uncontrolled network such as the Internet. It allows the computer on the network to send and receive data over shared or public networks as if it were a private network with all the functionality, security, and management policies of a private network. This is accomplished by establishing a virtual end-to-end connection through the use of dedicated connections, data encryption or a combination of both methods. Like the TOR system, VPNs hide users' real IP addresses, assigning them random IP addresses to connect to their destination sites.

77. **Encryption:** It is a data encryption method that consists of encoding the contents using a mathematical formula or algorithm that disorganizes them, so that if the corresponding key (called a "cryptographic key") is not available, they look like a set of alphanumeric characters with no meaning or reading logic.

78. **"Strong" encryption** is that which uses cryptographic keys sufficiently complex to make it mathematically impossible for them to be deciphered by a "brute force" attack. This is achieved, in computer terms, by adding bits to the cryptographic keys to make them more complex, which exponentially increases the difficulty of decryption by testing each of the possibilities. Thus, adding a single bit to the cryptographic key minimally increases the work required to encrypt the data, but doubles the computational effort needed to attack the algorithm. As an example, a 128-bit key contains 2^{128} (340,282,366,920,938,463,463,374,607,431,768,211,456) possible keys, while a 256-bit key contains 2^{256}, i.e., a number with twice as many digits as the previous one. Therefore, a successful computer attack on cryptographic keys of 128 or more bits is unfeasible.

79. **"Brute force" attack:** An attack in which great computational power is used to crack a password by trying all possible combinations.

80. **End-to-end encryption** is an encryption mechanism in which the message with its contents is encrypted on the sender's device by means of its own key, randomly generated for that communication. This key accompanies the message in transit and reaches the recipient's device, being decrypted at that moment only for the persons involved in that conversation.

81. **"Perfect forward secrecy":** It is a cryptographic key management protocol that ensures that session keys cannot be compromised even if the server's private key is compromised. This is done by generating a unique key for each session initiated by the user (as opposed to

older encryption systems, in which all sessions were encrypted with a single key that, if compromised, granted full access). It is the system used to protect communications in the main Internet messaging services, such as WhatsApp or Telegram.

82. **PGP (Pretty Good Privacy):** It is an encryption software based on the Open PGP protocol designed to provide privacy, security, and authentication for online communication systems. Originally created to protect e-mail messages, its use has been extended to also include digital signatures, full disk encryption, and network protection. PGP works with a public key (password) and a private key (password). The public key or session key is used to encrypt the plaintext information to be protected, and the private key is used to decrypt it. To this end, the receiver of the message provides a public key (randomly generated for each PGP communication session) to the sender, who uses it to encrypt the data. Then, once both the message text and the session key have been transmitted in encrypted form, the receiver uses its private key to decrypt the session key, which is then used to return the text to plaintext format.

83. **Voice over IP/VoIP:** It brings together different applications to transmit audio information in real time over the Internet like the human voice, emulating traditional telephone service. However, unlike the traditional Public Switched Telephone Network system, communications using VoIP systems are "peer-to-peer," without intermediaries, which prevents the interception of communications through the systems usually used. In addition, the data packets containing the communications are generally protected by encryption while they are "in transit" over the Internet.

84. **Public Telephone Switched Network (PTSN):** A network in which all telephone calls are established through a central switch that directs the outgoing call to its intended destination (the telephone of the receiver of the call, identified by its line number).

85. **Full-Disk Encryption (FDE)** is the process by which the entire hard disk of a computer (including the operating system) is encrypted, allowing access to the data contained therein only after successful authentication (by entering the corresponding password) in the FDE product. This implies that no person without the password (including the companies that manufacture the FDE product) can access the information contained in the device. There are FDE products for personal computers, laptops, and storage devices (TrueCrypt, BitLocker and PGP, among others). In addition, smartphones from the world's leading technology companies (Apple and Google) are protected by FDE, making it impossible to access without a numeric or biometric password to open the phone.

Related to new technological research tools

86. **Blockchain analysis:** It is the process of inspection, identification, segmentation, and modeling for the visual representation of the public data contained in the Blockchain, in order to obtain useful information about those who carry out transactions with cryptocurrencies. This

analysis is usually carried out by private companies that use proprietary algorithms to map the transactions carried out by cryptocurrency users and link them to each other.

87. **Dusting attack:** It consists of sending traces of cryptocurrencies (called "dust") to thousands (sometimes hundreds of thousands) of addresses, in order to monitor their activity and deanonymize their true holders. Cryptocurrency traces can be found on most public blockchains, including Bitcoin, Litecoin, Bitcoin Cash, and Dogecoin, among others.

88. **Open-Source Intelligence (OSINT):** A term that refers to the systematic collection, processing, and analysis of open access information. That is: information available to the general public without restrictions (on social networks, websites, search engines, news portals, public records, etc.).

89. **APIs (Application programming interfaces):** A set of requirements that govern the way applications communicate with each other, for which a part of the internal functions of a given program is "exposed" in a limited way. This allows applications to share data with each other and perform actions for each other's benefit without having to share the entire software code. APIs achieve this by limiting external access to only a specific set of functions, usually those related to requests for different types of information.

90. **Spyware:** It is a type of malware (malicious program) designed to operate surreptitiously within a computer system and secretly record information. It can monitor and copy what is typed ("keylogger"), what enters or leaves the system, capture stored information, or even activate the computer's microphones or cameras.

91. **Vulnerability:** A flaw or weakness in the code of a computer system that can be manipulated by an attacker to expose all or part of the system.

92. **Exploit:** It is the method (computer code) used to gain unauthorized access to a vulnerable system. Exploits can be programs, or simply a set of commands or actions designed to "exploit" a system vulnerability.

93. **Spear phishing:** A method of gaining surreptitious access to a computer system based on the deception of legitimate users of the system through "social engineering" techniques, such as the creation of an email or SMS message that appears to come from a source trusted by the target, containing a "call to action" (a required act, which may consist of connecting to a link or opening an attachment).

94. **Social engineering:** The term refers to the practice of obtaining confidential information or the performance of a certain action through the manipulation of legitimate users. It consists of the use of deception to obtain the delivery of relevant information, access or privileges in

information systems, enabling the attacker to carry out an act that harms or exposes the targeted person or organization.

95. **Watering hole attack:** An attack in which the attacker takes control of a server or a web page and manipulates it in such a way as to download spyware into the system of the users who access it or carry out some kind of action while they are connected.

96. **Supply chain attack:** An attack in which weak points in an organization's supply chain are exploited, increasing the chances of success by taking advantage of the trust of the organization's members in the products originating in that chain. An example of this attack consists of introducing spyware in software updates, so that they are installed and executed by the organization's customers on the basis of a relationship of trust with the issuing entity.

97. **Packet sniffers:** These are programs for network monitoring purposes, specifically designed to identify, within the Internet traffic flowing through an interception point, data packets that comply with different parameters set by the user.

Related to electronic or digital evidence

98. **Electronic (or digital) evidence:** Information generated, stored, or transmitted by means of electronic devices that may be used as evidence in court.

99. **Content evidence:** Evidence concerning the substance of a communication, i.e., the part that represents what the sender wishes to communicate to the receiver of the communication.

100. **Wrapper, data-related or "non-content" evidence:** It comprises all the information related to the communication, except for the content. For example, the date and time of the communication, its duration, the telephone numbers or IP addresses of the persons involved, the cellular telephone cells involved in the communication, etc.

101. **Evidence in transit:** This is digital evidence that is captured in real time while it is moving through the network. It may be content evidence, wrapper evidence, or both.

102. **Stored evidence:** Evidence that, at the time of collection, is not in motion but stored on a server (internal or external). Like the previous one, it can be content evidence, wrapper evidence, or both.

103. **Location evidence:** It refers to the location of a given communication device at a given time and, consequently, also of the person who was using it at that time. It is not content evidence.

104. **Metadata:** This is "data about data." It is not information created by the user ("active data") but information about the information: date of creation of the documents, author, changes made, data about the system or equipment they were created with transmission data, etc., which can generally be accessed only by operating digitally (i.e., it does not appear by default on the screens).

105. **Cloud storage (or cloud computing):** It is the service offered by certain companies that allows the user to store digital information on external servers owned by the service provider. It comprises three broad categories of services: *(i)* "infrastructure as a service" (IaaS), *(ii)* "software as a service" (SaaS) and *(iii)* "platform as a service" (PaaS). The first refers to the provision of "machines" (servers) over the Internet, the second to the provision of software applications via the Internet, and the third to the provision of a complete network (including servers, operating systems, and storage space).

106. **Cryptographic hash:** It is a mathematical algorithm that creates, from an input, an alphanumeric output of normally fixed length that represents a summary of all the information given to it and that can only be recreated with the same data. This ensures that the file has not been modified, since any change in the information, however small, completely alters the "hash," making it impossible to find other information resulting in the same alphanumeric value.

107. **Forensic image:** This is a bitstream copy of the contents of a file, hard disk, or server to enable computer forensic analysis without altering the original. This copy or "image" differs from traditional copies, such as those made when transferring computer files from one folder to another or from one computer to another, in that it duplicates every bit of the original, making it an exact clone of the original. If a forensic disk image is made, the duplication includes all the files, the empty spaces, the "master file table," and the metadata in exactly the same order as in the original.

IV. RELEVANT ASPECTS RELATED TO THE INVESTIGATION, SEIZURE, AND CONFISCATION OF VIRTUAL ASSETS

A. Money laundering and terrorist financing through virtual assets

108. The use of virtual assets for money laundering (crypto-laundering) is a natural consequence of the emergence of online markets for illegal goods and services (drugs, weapons, computer viruses, hacking services, etc.) in the so-called "Dark Web" or "Darknet." That is: the sector of the Internet that can only be accessed with technological tools that allow anonymous surfing, such as the TOR system. This criminal phenomenon, in turn, is a consequence of the emergence of Bitcoin in 2009, which made it possible for these "dark markets" to operate by offering a means of payment that is, in principle, also anonymous.

109. The emergence of the first of these markets (Silk Road) in early 2011 marked the beginning of a new era in the trade of illicit goods and services. Despite being shut down fairly quickly by the authorities, it was immediately replaced by other similar markets. Since then, "dark markets" have proliferated on the Web, and today they are the source of a high percentage of the illicit funds recycled through VAs and the services associated with them. In this regard, a study that analyzed Bitcoin transactions between 2013 and 2016[31] concluded that almost all of the bitcoins of illicit origin laundered through cryptocurrency exchange platforms came from dark web marketplaces.

110. However, VAs are also used to legitimize funds originating from both cybercrime per se (Ransomware, computer fraud, scams such as the recent "Plus Token" pyramid scheme in China,[32] etc.) and from illicit acts committed in the physical world, such as bribery. Most of the criminal schemes involving VAs are not necessarily novel, but variants of traditional schemes carried out by taking advantage of technological advances.[33]

111. The "crypto-laundering" process involves the same three stages as traditional money laundering (placement, layering, and integration). However, the maneuvers associated with each of these stages have their own characteristics, as a result of the nature of the VA involved. Thus, for example, the need for a placement stage depends on whether the illicit funds are obtained in fiat currency or directly in cryptocurrencies. This is so, since in the first case it is necessary to carry out a conversion from one currency to another, while in the second case it is not.

112. In the event that the placement stage is required, it is usually necessary to resort to a VASP—usually a cryptocurrency exchange platform—to convert the fiat currency into bitcoins or other similar VA. This circumstance can be exploited by the authorities in charge of AML/CFT or by State investigative agencies to obtain information on persons attempting to carry out a ML/TF scheme with VAs. Hence, especially since the update of the FATF 40 Recommendations in 2019, many countries have adjusted their domestic regulations to the new FATF Recommendation 15, and now require VASPs to carry out CDD on their customers and report suspicious transactions.

113. To circumvent this obstacle, launderers may resort to methods used to achieve the same purposes with respect to traditional financial institutions, such as structuring of funds or the use of front men. Another approach is to arrange the placement through a VASP located in a jurisdiction where they are not subject to AML/CFT duties or are not in compliance with the obligations in force. Taking advantage of the transnational nature of the Internet, some VASPs

[31] Refer to: FANUSIE, Yaya J. / ROBINSON, Tom: "Bitcoin laundering: An analysis of illicit flows into digital currency services," Elliptic Center on Sanctions & Illicit Finance, January 2018.
[32] This fraud yielded over 3 billion dollars in illicit profits, most of which was successfully recycled through cryptocurrency conversion services. It is estimated that the subsequent transformation of these funds into fiat currency is what caused the sharp decline in the value of Bitcoin in August 2019 (refer to: DUPUIS, Daniel / GLEASON, Kimberley: "Money laundering with cryptocurrency: Open doors and the regulatory dialectic," Journal of Financial Crime, August 2020).
[33] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 12 § 22.

have explored ways to provide services to customers in certain jurisdictions without registering in those jurisdictions, in order to avoid compliance with AML/CFT obligations, as illustrated in the following case:[34]

Case 1: BitMex. VA exchange platform in violation of AML/CFT regulations:
In October 2020, the U.S. State Department prosecuted four executives of VA exchange platform BitMex for violations of U.S. anti-money laundering regulations.
Despite serving at least 85,000 customers in the U.S. and running most of its financial infrastructure from the U.S., BitMex never registered with U.S. authorities. BitMex's primary parent was the firm HDR Global Trading Ltd., incorporated in a tax haven (the Seychelles), where it never operated or had any employees. The platform was owned by a series of shell companies (HDR Global Trading Ltd., 100x Holdings, ABS Global Trading, Shine Effort and HDR Services) controlled by the same individuals. The CEO himself claimed legal domicile in the Seychelles, but owned part of BitMex shares through a Delaware-registered LLC, which held bank accounts in financial institutions in the US.
BitMex was accused of being an unregistered financial entity, providing services to customers in the U.S. despite declaring that its system is designed to exclude them, as well as of violations of AML/CFT regulations, including the deletion of critical information about its customers.

114. However, the conversion of large volumes of illicit funds into VAs can be problematic. The cryptocurrency market is still relatively small, so a massive purchase may cause suspicion. As was evident in the case of the illicit proceeds of the Plus Token scam, a massive sale or purchase of cryptocurrencies tends to generate sudden price changes in such assets, which may attract the attention of the authorities. In any case, and due to the preponderance of this cryptocurrency, it is likely that a high volume of transactions will go unnoticed in the Bitcoin Blockchain, while transfers for high amounts will surely be conspicuous in those of less used currencies.

115. Once the placement phase has been completed, there are multiple ways to carry out the layering of funds. On the one hand, it can take the form of a series of transactions between VA wallets controlled by different persons or even by a single person, since cryptocurrencies allow users to maintain an indefinite number of addresses. This circumstance, together with the simplicity of creating new addresses, the dissociation between these and real-world identities, the speed with which transfers are completed (faster than those carried out in the correspondent banking network) and the ease with which they cross national and regulatory borders, makes it possible to create extremely complex layering patterns.

116. These characteristics of VAs are not only useful for crypto-laundering but can also be exploited for terrorist financing. Thus, the ease with which fiat currency can be converted into cryptocurrencies and then transferred across borders quickly and with a relatively high level of anonymity has resulted in some terrorist organizations resorting to these methods to obtain funds

[34] Source: CipherTrace: "Cryptocurrency crime and anti-money laundering report," February 2021.

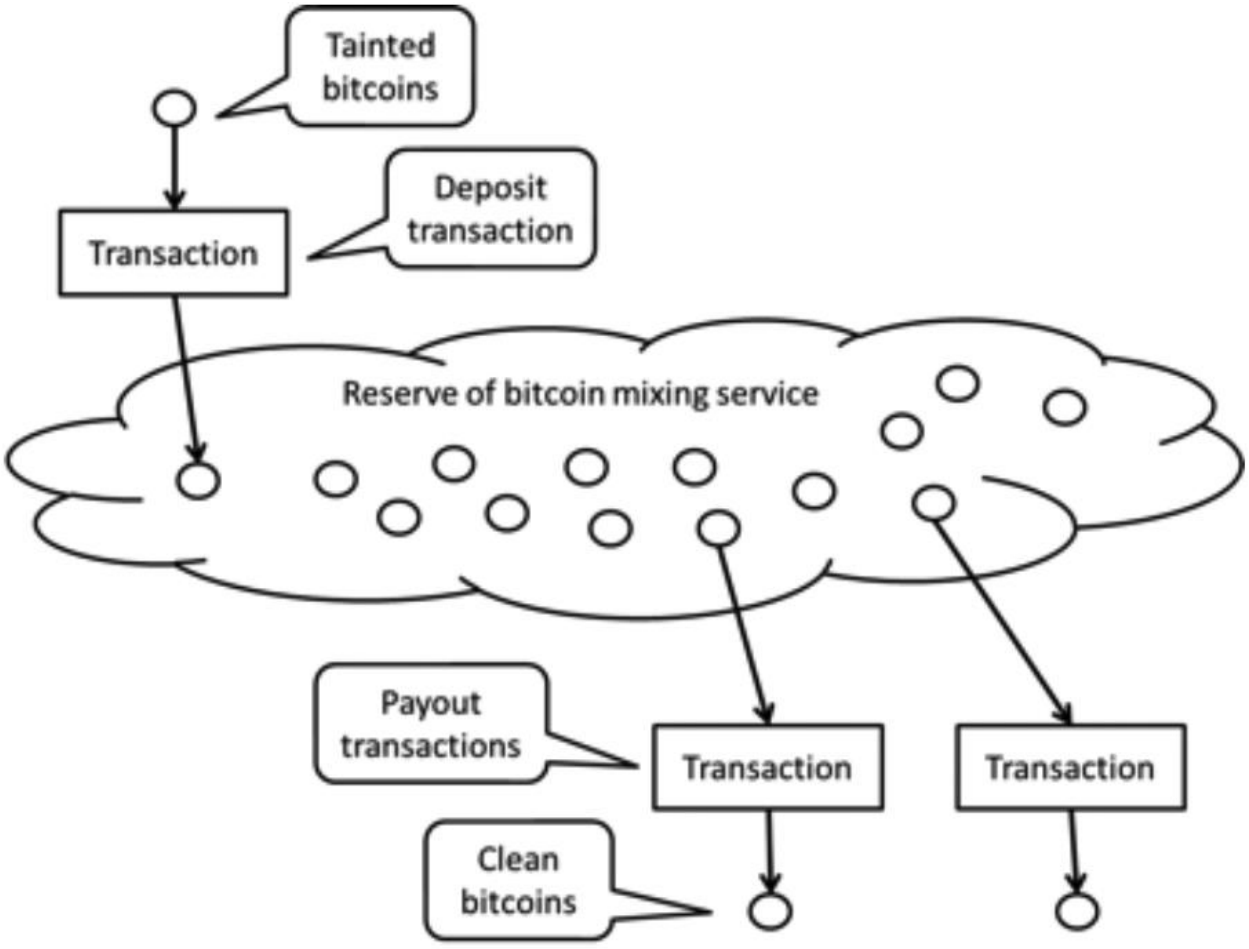
by receiving anonymous "donations" in VAs. Likewise, this kind of assets can also be used to acquire weapons or other items in the virtual marketplaces of the Dark Web.

117. VASPs play an essential role in crypto-laundering schemes, either in the placement phase (for the conversion of fiat currency into VA), during the layering phase (e.g., allowing the exchange of one cryptocurrency for another or providing "mixing" services) or in the final stage, where the beneficiaries of the scheme convert the funds back to fiat currency.[35] This has led to the emergence of VAs exchange platforms specifically created and structured to facilitate crypto-laundering.[36] In this context, a recent report concludes that one third of the volume of cross-border Bitcoin traffic is being diverted to VASPs with deficient AML/CFT policies.[37]

118. Among the main services that VASPs can offer to assist launderers of illicit funds are cryptocurrency "mixing" services. So-called "mixers" or "tumblers" function as independent money laundering services, combining the inflows and outflows of funds from different users to make them indistinguishable from each other. In such a context, passing through a "mixer" replaces the transfer of VAs between two addresses (e.g. Bitcoin), so that the illicit funds that one person intends to transfer to another are intermingled with those coming from many other VA addresses before finally being sent to the recipient's, hindering the identification of the address of origin and the accounts associated with the illicit funds.[38] This is illustrated in the graph below:[39]

[35] Refer to: FATF: "Guidance for a risk-based approach: Virtual currencies," June 2015.
[36] Refer to: FATF: "Professional money laundering," July 2018, pp. 45/46.
[37] Refer to: CipherTrace: "Cryptocurrency crime and anti-money laundering report," February 2021, p. 6. While the report itself reports a sharp drop in the overall percentage of bitcoins channeled to high-risk VASPs, this is primarily due to the rapid increase of interest in bitcoins as an investment vehicle, which has led to an estimated 57% decline in the proportion of bitcoins of illicit origin between 2019 and 2020. This is largely due to the huge increase in the value of bitcoins, which at the time of their launch were valued at less than a penny on the dollar each, while in February 2021 they reached a global value of $200 billion (refer to: FANUSIE, Yaya J. / ROBINSON, Tom: "Bitcoin laundering: An analysis of illicit flows into digital currency services," Elliptic Center on Sanctions & Illicit Finance, January, 2018, p. 1).
[38] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 34 § 109.
[39] Source: 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, No. 2, 2018, pp. 419/432.

Graph 1: Operation of a Mixer:



119. The basic concept of mixers resembles that of investment funds, in which multiple individuals accumulate their funds to obtain a collective benefit. The difference is that, in the case of mixers, the pooled fund is used to effect multiple cryptocurrency transactions, and the benefit is to achieve a greater degree of anonymity by preventing the linking of transfers to specific VA addresses.

120. ML/TF mixers generally charge a fee for their services, do not keep records of their users, and can obscure their infrastructure by operating as "hidden services" of the TOR system. From the LEAs' point of view, the use of mixing services by persons under investigation makes it very difficult to reconstruct the chain of transactions (unless that person concentrates a significant amount of the funds processed through the mixer or random or semi-random methods are not used to combine users' VAs).[40]

[40] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 35 § 110.

121. Mixers occupy an important place in the market of illicitly sourced VAs, to such an extent that some hidden markets of the dark web have an integrated mixer to facilitate the laundering of funds from the purchase and sale of illegal goods and services. Hence, despite representing only a small percentage of Bitcoin traffic to and from VASPs, mixers are much more likely to be used for crypto-laundering.[41] Some of the most widely used mixers overtly advertised the possibility of using these services to "clean" "dirty coins," as illustrated below:[42]

Graph 2: Explanation of the operation of the "Helix" mixer:

122. Use of VASPs also facilitates the realization of other VA layering methodologies, such as "chainhopping," which consists of exchanging different cryptocurrencies with each other, in order to cut the chain of transactions in the respective blockchains, a maneuver that—according to some studies—has become one of the preferred methods for crypto-laundering.[43]

B. The importance of imposing AML/CFT duties on VASPs for the prevention and investigation of ML/TF maneuvers involving VAs

123. In view of the above, the imposition of information and reporting duties to VASPs is a central element of any AML/CFT strategy related to VAs that aims to be effective. At the same time, it constitutes a fundamental tool for the development of asset investigations on ML/TF conducts involving cryptocurrencies, to the extent that it takes advantage of the essential role

[41] Thus, for example, between 2013 and 2015, more than 20% of the transactions concluded by "mixers" came directly from illicit sources (refer to: FANUSIE, Yaya J. / ROBINSON, Tom: "Bitcoin laundering: An analysis of illicit flows into digital currency services", Elliptic Center on Sanctions & Illicit Finance, January 2018, p. 7).
[42] Source: Website of the now defunct Mixer "Helix," whose administrator, Larry Dean Harmon, was arrested in February 2020 for money laundering.
[43] Refer to: FATF: "FATF report to G20 Finance Ministers and Central Bank Governors," July 2018, § 35 and 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.

played by VASPs as intermediaries between the physical and virtual world, i.e., between the VAs and fiat currencies.

124. In this regard, the new FATF Recommendation 15 provides that member countries should adapt their domestic regulations to extend the AML/CFT, registration, and reporting rules applicable to financial or non-financial service providers to VASPs, understood as natural or legal persons who commercially carry out one or more of the following operations for the benefit of another legal or natural person: (i) exchange between VAs and fiat currencies; (ii) exchange between one or more classes of VAs; (iii) transfer of VAs (understood as the movement of such assets from one virtual address or account to another); (iv) custody and/or administration of VAs or instruments that allow the control thereof; and (v) participation in or provision of financial services linked to the offer and/or sale of VAs by users.

125. Therefore, the main players in the VA ecosystem, such as cryptocurrency exchange platforms and VA transfer services; some VA wallet providers (such as those that host wallets or maintain custody or control over the VAs of another natural or legal person, their wallets and/or their private keys); and providers of financial services linked to the issuance, offer or sale of VAs; among other possible business models, are included within the definition.[44]

126. The importance of these actors lies in the fact that they serve as the main entry point into the global financial system for criminals seeking to convert funds obtained or held in the form of VAs into fiat currency. In this regard, it is important to keep in mind that while it is true that some businesses in many countries support payment with cryptocurrencies for the purchase of goods and services, most goods are still paid for with fiat currency. Therefore, it is most likely that profits earned or recycled in cyberspace (through VAs) will eventually be transferred to the real world and converted into fiat currency, so that the holder can enjoy them or reinvest them in their illegal business (e.g., acquiring items that can only be paid for with physical currency).

127. In this scenario, the links between the physical and virtual worlds constitute the main focal point of asset investigations related to transactions with VAs, since it is there where transactions perpetrated in cyberspace—in a context of (pseudo) anonymity—can be connected with one or more real persons. The same is true in the opposite direction, if criminals intend to resort to the use of cryptocurrencies for the placement or layering of funds obtained in fiat currency, in which case VASPs will be the entry point into the VA ecosystem.

128. It is clear that if VASPs are obliged to require the full range of information aimed at identifying their customers and establishing the origin of the funds they operate with, the recourse to VAs will lose some of its attractiveness compared to fiat currency. In turn, AML/CFT regulation

[44] Refer to: FATF: "Virtual assets and virtual assets service providers. Guidance for a risk-based approach," June 2019, p. 14 § 35.

provides supervisory agencies and LEAs with an important starting point for the identification and prosecution of money launderers and other criminals.[45]

129. The most important entrance or exit point to and from the VA ecosystem are the cryptocurrency exchange platforms ("exchanges"), which present different forms and business models. Their primary function is to allow their customers to buy or sell VAs in exchange for fiat currency, other VAs, or other tradable goods or securities, in exchange for a fee, commission, or other form of remuneration. They generally accept a wide variety of payment methods, including cash, bank transfers, credit or debit card payments, or even other VAs.[46]

130. There are two main types of cryptocurrency exchange platforms: centralized or decentralized. In the first case, VAs are transferred "through" the platform, which acts as an intermediary. That is, it is part of the transaction, buying VAs from the seller and selling them to the buyer. On some of these centralized platforms, users first deposit fiat currency or cryptocurrencies into custodial accounts, which are then used to fund the transactions. Decentralized platforms, on the other hand, only provide a venue for buyers and sellers to meet to conduct exchanges, which are done exclusively in a P2P format.[47] Although most platforms are centralized, this makes them vulnerable to hacking, which is why there is a trend in the VA community to replace them with the decentralized variant.[48]

131. Unlike centralized platforms, which are included in the FATF definition of VASP (which indicates that they must be subject to the CDD and reporting obligations established in the AML/CFT regulations, according to the new Recommendation 15 of said organization), P2P platforms, in principle, are not.[49] This, since it is understood that, for the time being, the use of the latter type of platforms has not been generalized to the point of constituting a relevant ML/TF risk.

132. Another channel for the exchange between VA and fiat currency is using the so-called VA ATMs or "kiosks." These are machines similar to ATMs, located in many cities around the world, which provide a physical point where people can buy or sell cryptocurrencies. In the absence of effective regulation and oversight, VA ATMs can become a vulnerability in the AML/CFT system; and, in fact, there are already reports indicating that operators of this class of ATMs tend to be

[45] Refer to: MBIYANGA, Stefan "Cryptolaundering: Anti-money laundering regulation of virtual currency exchanges," Journal of Anti-Corruption Law, Vol. 3, No. 1, 2019, p. 1.
[46] Refer to: FATF: "Virtual assets and virtual assets service providers. Guidance for a risk-based approach," June 2019, pp. 14/15, § 37.
[47] Refer to: MBIYANGA, Stefan "Cryptolaundering: Anti-money laundering regulation of virtual currency exchanges," Journal of Anti-Corruption Law, Vol. 3, No. 1, 2019, p. 4.
[48] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 67, §§ 238/239.
[49] Refer to: FATF: "12-month review of the revised FATF standards on virtual assets and virtual asset service providers," June 2020, p. 7 § 20. However, the Financial Stability Institute (FSI) points out that the use of P2P platforms constitutes a potential source of risk, precisely because it does not involve any entity that is covered by AML/CFT obligations. This risk could increase if cryptocurrencies are massively adopted, and the volume traded without any control through these platforms increases proportionally (refer to: Financial Stability Institute: "Supervising cryptoassets for anti-money laundering," FSI insights on policy implementation, No. 31, April 2021, p. 18. Data from the company CipherTrace is cited indicating that 40% of Bitcoin payments in 2020 went to private wallets).

less compliant than other VASPs with the CDD and reporting obligations set out in the regulations. In turn, VA ATMs have been linked to illicit activities, having been used by drug traffickers, credit card fraud or prostitution networks and unregistered P2P exchange platforms.[50] This was the route used in the case detailed below:[51]

Case 2: Operation Glutons. Use of Bitcoin ATMs for ML.
Spain's Guardia Civil reported through Europol the frequent use of Bitcoin ATMs operated by a company under investigation by a criminal organization with a background in drug trafficking to convert illicit proceeds into VAs. In order to circumvent AML/CFT controls, the persons in charge of making the deposits applied "smurfing" (structuring) techniques, dividing the funds into batches of less than EUR 1,000. In a single day, they made multiple deposits in different VA ATMs in different locations, for total amounts of approximately EUR 200,000 per month.
The suspicion of the Spanish authorities was that there was complicity with the illegal operation on the part of the company managing the VA ATMs, since no CDD tasks were carried out and no STRs were filed regarding the aforementioned scheme.

C. Diagnosis of the regional situation regarding the regulation of VAs and VASPs

133. As noted above, for the development of an effective AML/CFT strategy with respect to the potential illegal use of VAs, it is essential that there is consistent regulation, at the global level, with respect to both such assets and VASPs. Conversely, the absence of consistent regulation is one of the main reasons why VAs are vulnerable to exploitation for illicit purposes. For this reason, the FATF has noted that the effectiveness of the 2019 revised standards to prevent ML/TF with VAs depends on their effective implementation by all jurisdictions, as well as on compliance with the obligations imposed on private sector entities by these standards.[52]

134. In this context, after the update of the 40 Recommendations, the above-mentioned organization carried out an annual global review of the implementation of the revised standards by the different jurisdictions and the private sector. As a result, the FATF concluded that, in general, both the public and private sectors have made progress in implementing the revised standards. It noted that 35 of the 54 jurisdictions assessed reported having implemented the standards, with 32 of them regulating VASPs' activity and the remaining 3 prohibiting it.[53]

135. With specific regard to Latin America, prior to the update of the 40 FATF Recommendations and the subsequent evaluation by the FATF, the OAS Group of Experts for the Control of Money Laundering carried out, between 2017 and 2018, a survey of the situation in

[50] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 40 § 131.
[51] Source: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 40 § 132.
[52] Refer to: FATF: "12-month review of the revised FATF standards on virtual assets and virtual asset service providers," June 2020, p. 2 § 3.
[53] Refer to: FATF: "12-month review of the revised FATF standards on virtual assets and virtual asset service providers," June 2020, p. 2 § 2.

terms of VAs at the regional level.[54] In such context, it was possible to establish that the situation at that time presented the following characteristics:

- Lack of regulation regarding the operation of VAs.
- Lack of convictions for illegal acts perpetrated with/involving VAs.
- Incipient research strategies, only at FIU level.
- Identification of virtual currency supply portals in almost all the countries consulted, with most of them indicating the circulation of more than one cryptocurrency.
- Existence of a considerable sector of the economy accepting virtual currencies (especially Bitcoin) as a means of payment.
- Absence of minimum user standards and AML/CFT regulation referring VAs and VASPs.

136. With regard to convictions or investigations, the OAS noted that there had been only one investigation into the illicit use of VAs in the region (the "Liberty Reserve" case in Costa Rica). Furthermore, with regard to the seizure or confiscation of this type of asset, the survey found no experience in this area, nor any type of regulation for the seizure, confiscation, or administration of VAs.[55]

137. In addition, it is important to note that as regards the evaluation of Recommendation 15 based on the FATF amendments, as of the date of this report, no GAFILAT country has been evaluated in this regard, so that the results can be seen either in countries not yet evaluated in the 4th Round of Mutual Evaluations, or in future follow-up reports and other rounds of evaluation.

138. Moreover, for the purposes of preparing this guide, a questionnaire was sent to the RRAG focal points requesting information—among other questions—on whether the ML/TF risks associated with VAs were recognized at the local level, whether there was local legislation regulating their use, and whether AML/CFT standards had been introduced in relation to VASPs, in compliance with the new FATF Recommendation 15.

139. In this context, 15 of the 17 countries in the region (88%) considered the use of VAs as a potential source of ML/TF risk.

140. However, the identification of the possible illicit use of VAs as a vulnerability in terms of ML/TF has not resulted, so far, in the general adoption of local rules regulating the market for VAs The responses to the questionnaire show that only 4 of the 17 GAFILAT countries have legislated on this issue (24%).

[54] Refer to: Organization of American States (OAS): "Study on new typologies in money laundering, specifically in the use of virtual currency," conclusions of the XLV Meeting of the Expert Group for the Control of Money Laundering – FIU/OIC Sub-Working Group 2016-2018, OAS/Ser.L/XV. 4.45 DDOT/LAVEX/doc. 16/18, October 2018.
[55] Refer to: Organization of American States (OAS): "*Estudio sobre nuevas tipologías en el lavado de dinero, específicamente en el uso de moneda virtual*" [Study on new typologies in money laundering, specifically in the use of virtual currency], conclusions of the XLV Meeting of the Expert Group for the Control of Money Laundering – FIU/OIC Sub-Working Group 2016-2018, OAS/Ser.L/XV. 4.45 DDOT/LAVEX/doc. 16/18, October 2018.

141. Finally, with regard to the introduction of regulations aimed at addressing the actions of VASPs—in line with the new FATF Recommendation 15—, it is noted that, of the 11 countries that responded to this question, 6 have addressed VASPs (55%), while the remaining 5 have not yet done so.

142. In this regard, there has been progress in the recognition of the use of VAs as a potential source of ML/TF risks, which—while not leading to a generic regulation of the cryptocurrency market in most countries—did result in most of them updating their local regulations on AML/CFT to include VASPs.

143. Given the importance of adequate regulation of the performance of VASPs—both for the purposes of preventing AML/CFT and as a source of information for law enforcement agencies in the framework of ML/TF investigations of assets involving VAs—it is essential that the process of implementation of the new FATF standards continues to progress in Latin America, in order to achieve a homogeneous regulatory framework throughout the region.

D. Challenges inherent to the investigation of ML/TF with VAs

144. The emergence of VAs as an element to develop new ML/TF typologies implies the transfer of a significant portion of the investigations related to such maneuvers—as well as the measures aimed at the seizure and confiscation of funds—to cyberspace, a completely different scenario from the setting in which they have traditionally been carried out. This forces the national authorities in charge of ML/TF prosecution in general, and of investigation, identification, seizure, and confiscation of VAs in particular, to face new obstacles and challenges and, in turn, to resort to new strategies and methodologies in order to remain effective.

145. In terms of obstacles and challenges, the following stand out: the "extra-territorial" nature attributed to cyberspace by many experts; the freedom and speed of exchange of computer data (including those that may be relevant as evidence or to identify VAs susceptible to seizure or confiscation) through the Internet; the phenomenon of "loss of knowledge of the location" of such data[56] and the consequent difficulty in establishing the procedural law that should govern their collection. In addition, there is the emergence of new technologies that prevent—or at least hinder to a great extent—the exercise by police agencies of the surveillance powers conferred upon them by local laws, among which we should mention—in addition to those related to the operation of VAs—the new methods of communication that replace the Public Switched Telephone Network

[56] This lies in the impossibility of establishing with certainty the geographic location of digital data as a result of the use of "cloud computing" services for storage and technological factors associated with such services, such as data fragmentation, the automatic displacement of data (due to storage space issues) or the generation of multiple backup copies.

(PSTN),[57] the anonymous navigation systems on the Internet, and the encryption of communications and stored contents, among others.

146. The problem related to the determination of the regulations applicable to the implementation of investigative measures restricting rights or tending to seize VAs in view of the transnational nature of such assets is particularly relevant with regard to decentralized VAs. This is due to the fact that in the case of centralized VAs (for example, virtual currencies issued in the field of "Massively Multiplayer Online Role Playing Games" or MMORPGs), since there is a central administrative authority that controls the management of the assets, unless expressly provided otherwise, the regulations applicable in the jurisdiction in which such authority is based shall apply.

147. In the case of decentralized assets such as cryptocurrencies, on the other hand, there is—by design—no central authority controlling the flow of VAs. The currencies themselves are nothing more than digital information (specifically, the record of transfers between users of the cryptocurrency in question). Their location for the purposes of the applicable jurisdiction for an eventual seizure or confiscation is the one corresponding to the place where the wallet in which such information is stored is located. However, this location may be fixed (in the case of a fixed wallet) or it may not be fixed, as in the case of an online wallet, especially if it is "in the cloud," in which case the information is usually stored in servers located in data centers located in strategic points of the globe. In addition, electronic data may be in a single location or distributed (in sections) across multiple servers (even in different countries), and automatically rearranged depending on the availability and demand for cloud storage space at any given time. They may also be stored redundantly, in multiple copies, so that they can be recovered even if one server (or data center) fails.

148. Consequently, in some cases it may not be possible for the company providing the cloud storage service itself—and, therefore, for national authorities seeking to seize or confiscate VAs—to establish precisely where a specific set of digital data, for example, a Bitcoin wallet, is located at any given time. As a consequence, it is also impossible to establish which country has jurisdiction to order the seizure or confiscation of cryptocurrencies.

149. This problem is addressed by the concept of "loss of location" coined in a Council of Europe document,[58] which in turn occurs within the framework of a more general phenomenon, namely delocalization as an essential feature of the Internet or, more specifically, of cyberspace. This, insofar as it is a field that is not located in a specific place, but, in a functional sense, is in all of them at the same time, but in a physical sense, in none. These characteristics clash with the

[57] In Spanish "Red Telefónica Pública Conmutada (RTPC)," translated from the English "Public Telephone Switched Network (PTSN)." That is, a network in which all telephone calls are established through a central switch that directs the outgoing call to its intended destination (the telephone of the receiver of the call, identified by its line number).
[58] Refer to: SPOENLE, Jan: "Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal," Council of Europe Discussion Paper No. 31, 2010.

upholding of the principle of territoriality as the focal point of the exercise of sovereignty by countries through the application of procedural rules within the scope of their jurisdiction, insofar as they question the possibility of establishing where the objects which the rules refer to are located. This is because the speed and unpredictability of electronic information flows make it difficult (or impossible) to locate the data at any given time.[59]

150. Technological evolution also entails another series of consequences arising from the emergence of technological developments that can be exploited by cybercriminals (whether, for the purposes of this guide, ML or TF) to evade the action of the authorities or hinder their efforts. In turn, the parallel emergence of sophisticated surveillance or forensic tools has turned the pursuit of cybercrime into a veritable arms race between criminals and investigative agencies, each seeking to exploit technological advances to prevail.

151. In this context, one of the main areas of conflict is around "anonymity by design" technologies, which are one of the most important features of decentralized virtual currencies such as Bitcoin, which have been created with the specific aim of guaranteeing their users at least some degree of anonymity. In this sense, the first feature tending to achieve this goal is precisely the decentralized structure, lacking a central authority that can be subject to state supervision and know the true identities of the users. To this end, cryptocurrencies are organized as P2P exchange systems, in which interactions are carried out directly between two users, without intermediaries.

152. Notwithstanding the above, the different cryptocurrencies also implement a series of additional technological developments aimed at increasing the anonymity of the users. Thus, based on how they are structured, these VAs can offer four different levels of anonymity, namely: 1) pseudo-anonymity: derived from the use of pseudonyms (alphanumeric addresses) to obscure the user's identity; 2) partial anonymity ("Set anonymity"), where the identity of the real user can be one among several possible ones, which is achieved through the use of "ring signatures"; 3) total anonymity of the user, which is obtained when the real user can be any of the nodes in the system; and 4) confidential transactions, in which the amounts transferred are also guaranteed to remain concealed.

153. Both Bitcoin and most altcoins operate at the first level, in which the addresses involved in the transactions (and the amounts transferred) are public, but the identity of the users involved is protected using pseudonyms (the alphanumeric keys that identify the addresses). Consequently, while it is not difficult to follow value flows within the system, understanding how this reflects the actual value transfers between individuals is more complicated. However, the emergence of technological tools that facilitate the latter, weakening the anonymity offered by Bitcoin and other traditional cryptocurrencies, has led to the creation of alternative currencies—called "privacy

[59] Refer to: DASKAL, Jennifer; "The un-territoriality of data," The Yale Law Journal, Vol. 125, No. 2, 2015, p. 329.

coins"—that include features aimed at ensuring a higher level of anonymity for users. The most important of these currencies are Dash, Zcash, and Monero.

154. The most important characteristic of private coins is that, like Bitcoin, although they operate from an open-source public Blockchain, they do not make the same data visible. Namely:

- Dash (DASH), launched in 2014, uses a type of "Coinjoin" mixer known as "PrivateSend" to reduce the traceability of coins on its Blockchain.
- Zcash (ZEC), created in 2016, is based on the use of a novel variety of cryptography known as "zero-knowledge proof," which allows users to reach a consensus on the validity of the information (necessary to avoid the emergence of apocryphal transactions) while keeping the data encrypted. This ensures the legitimacy of the Zcash network transfers and at the same time safeguards the true identity of the participants.
- Monero (XBR) also launched in 2014, does not publish information about the sender, receiver, or value of transactions on its Blockchain. Instead, it uses "stealth addresses," created specifically for one-time use to ensure that only the user(s) involved in the transaction have access to the transaction data. It also employs a form of cryptography known as "ring signature;" which allows transactions to be confirmed within a group of users in such a way that an observer is not able to identify the specific person who confirmed a particular transfer.[60]

155. One of the main differences between Monero, Dash, and Zcash is that, in the latter, applications aimed at increasing anonymity are optional, while in the former it is enabled by default. Consequently, the use of the advanced anonymity variant of Dash or Zcash is reduced to a minority.[61] Moreover, being derivations of the Bitcoin Blockchain, both Zcash and Dash retain some vulnerabilities (in terms of anonymity protection) similar to those of the former.

156. In comparison, cryptocurrencies using the Cryptonote protocol (such as Monero) offer a higher level of privacy. By using this protocol, the traceability of transactions is obfuscated by avoiding the identification of the true balance resulting from a transfer (known as "unspent transaction output" or TXO), replacing it with a set of possible TXOs that includes the real one together with other "fillers," known as "mixins."

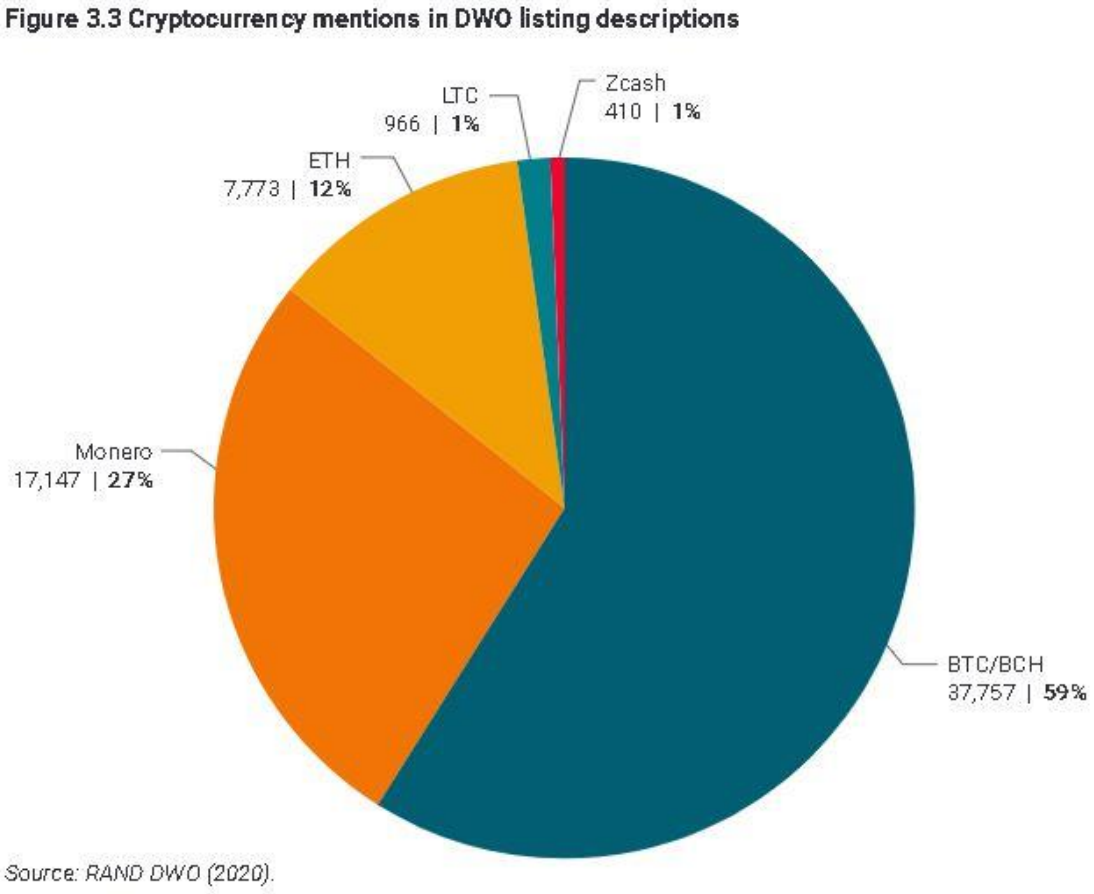
157. Partly due to this, Monero has been positioning itself, since its launch in 2014, as the main alternative to Bitcoin from the point of view of transaction (un)traceability. In that regard, it received a big boost when it was accepted as a payment currency by the (now defunct) AlphaBay Dark Web marketplace in August 2016, when the number of transactions registered on the

[60] European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses," Policy Department for Citizen's Rights and Constitutional Affairs," May 2018, p. 32.
[61] According to data updated as of January, only 15.5 % of Zcash transactions had been made with the anonymous variant (refer to: 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, p. 12).

Monero Blockchain increased by 80%.[62] Currently, one of the most important hidden markets of the Dark Web (White House Market) only accepts this currency to pay for products and services traded there.

158. At present, however, the presence of "private currencies" in ML/TF investigations is minimal, although their growing acceptance by the main VASPs and in markets of the Dark Web seem to indicate that their use is set to increase in the future.[63] In any case, Bitcoin continues to be the most widely accepted currency in most virtual markets, as reflected in information from the Dark Web Observatory (DWO) on the use of cryptocurrencies in the main virtual markets of the Dark Web.[64]

Graph 3: Incidence of cryptocurrencies in the Dark Web markets:



[62] Refer to: 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," Proceedings on Privacy Enhancing Technologies, Vol. 3, 2018, p. 153.
[63] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 35 § 113.
[64] According to the DWO survey, the most widely used cryptocurrencies are Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (ETH), Litecoin (LTC), Monero (XBR or BitMonero), and Zcash (ZEC). Refer to: 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, p. 17.

159. According to the data collected by the DWO, Bitcoin, Monero, and Ethereum monopolize exchanges on the Dark Web marketplaces (98%). Although Monero has a significant presence (27%), displacing Ethereum (12%), the predominance of Bitcoin in transactions is clearly maintained (59%). In contrast, the use of other "private currencies" is minimal, with Zcash registering just 1%.

160. The persistence of Bitcoin as the dominant cryptocurrency in this area would seem to contradict the idea that criminal activity is turning en masse to "private currencies" in order to exploit their advantages in terms of obscuring transaction-related information. This could be due to the fact that Bitcoin has reached a "critical mass" in the licit and illicit cryptocurrency markets, which increases the likelihood that Bitcoin transactions will go unnoticed in the overall volume of transactions.

161. Another factor in favor of the continued dominance of Bitcoin is the greater ease of access to them on cryptocurrency exchange platforms (including those located in jurisdictions with few AML/CFT controls). In contrast, private currencies remain relatively difficult to obtain and have less liquidity, which may force them to be sought on platforms with higher transaction volumes, where—in turn—it is more likely that AML/CFT measures have been implemented. Therefore, at least for the time being, private currencies do not seem to be suitable for the laundering of illicit funds on a large scale but are rather restricted to the use of a minority portion of the criminal element, as a currency of exchange for small-scale drug trafficking or other crimes.[65] They may be considered suitable for terrorist financing involving small volumes of funds.

162. Moreover, the anonymity that is not obtained through the use of private currencies can be achieved through other methods or tools, such as the use of mixers, decentralized exchange platforms or applications, cryptocurrency exchanges through "chain-hopping" or "atomic swaps," or through "dusting" (which consists of transferring traces of cryptocurrencies to multiple random addresses, in order to hinder the traceability of the transaction chain).[66]

163. Mixers operate with the main cryptocurrencies (Bitcoin, Ethereum, Litecoin) and can be accessed both on the Surface Network and on the Dark web, through the TOR system. While there are no limits on the amounts of cryptocurrency transactions, there are limits when transforming these VAs into fiat currency, an aspect that can reduce the effectiveness of mixers for recycling significant volumes of funds of illicit origin. To circumvent these limits and avoid drawing attention to themselves, launderers may choose to space out outgoing payments over time and make them in varying amounts.

[65] Refer to: MBIYANGA, Stefan "Cryptolaundering: Anti-money laundering regulation of virtual currency exchanges," Journal of Anti-Corruption Law, Vol. 3, No. 1, 2019, p. 7.
[66] Refer to: FATF: "12-month review of the revised FATF standards on virtual assets and virtual asset service providers," June 2020, p. 7.

164. Decentralized exchange platforms (DEXs) enable direct P2P exchanges between cryptocurrency users. These are applications that exploit technological innovations such as multi-signature custodial accounts to allow users to exchange VAs without the need for a third-party custodian of funds. These include IDEX, Bitsquare, OpenLedger, CryptoBridge, and Bitshares.

165. The possible uses for technological developments based on encryption, to provide a higher degree of anonymity, are not limited to the design of cryptocurrencies or in the implementation of mechanisms to further hinder to the traceability of the transactions carried out with them. On the contrary, encryption is, at present, the main element for the protection of digital data throughout the global IT ecosystem, both with respect to data that are "in transit" through the Internet and those that are stored, including data that are generated by communications or necessary for those communications to take place.

166. In this context, the very environment of the "dark web," where online markets operate and much of the illicit activity with cryptocurrencies takes place, is the result of the emergence of these anonymity tools based on encryption. In particular, the TOR system ("The Onion Router"). It is a distributed network of computers on the Internet, where all machines running the TOR software (which can be downloaded for free) serve as nodes, allowing all users of the system to surf anonymously, masking their real IP address (and thus their identity) by routing communications through random circuits between nodes around the world. In addition, the system covers the computer data packets that make up the communication (including those indicating origin and destination) with multiple layers of encryption, which prevents their traceability. Other methods, such as virtual private networks (VPNs) or the I2P network, operate with similar mechanics.

167. The TOR system makes it possible to host web pages on the "dark web" whose true IP address cannot be identified—called "Hidden services"—making it difficult to determine the geographical jurisdiction they are operating from. For the same purposes, other cryptocurrency exchange platforms operating on the superficial Web choose to use intermediaries to register their Internet domains or use DNS records that suppress or conceal the identity of the real domain holders.[67] Most illicitly sourced VAs are recycled through exchange platforms or mixers located in unknown jurisdictions.[68]

168. In addition, in the last ten years, the use of "strong" encryption (i.e., with cryptographic keys of 128 bits or higher) to protect the content of Internet communications has been consolidated. The massive adoption of these technologies by the main global technology companies has created new opportunities for online criminals and, in turn, new challenges for police and investigative agencies.

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

169. Thus, administrators and sellers in the first illicit online marketplaces protected their communications with "Pretty Good Privacy" (PGP) encryption software, which was later also adopted by more technically sophisticated criminals or criminal organizations. The TOR system also makes it possible to encrypt e-mails. Criminals have also begun to use means of communication that make interception more difficult, such as Voice over Internet Protocol (VoIP) systems, like Skype. Subsequently, some companies have developed encrypted telephone communication systems specifically designed to avoid state monitoring, which were quickly adopted by criminal organizations around the world. In 2020 and 2021, two of these systems (EncroChat and Sky ECC) were the subject of highly sophisticated undercover operations by law enforcement agencies in Europe. The same happened in 2021 with another similar system (An0M), in this case by the FBI in the USA.

170. In many of its variants, encryption is used in such a way that access to the content of communications is not only beyond the technical reach of the authorities (regardless of whether they have judicial authorization to obtain it), but also of the companies that implemented the technology. Such is the case of the most globally widespread messaging systems (WhatsApp, Facebook Messenger, Telegram, Signal), in which communications in transit are protected by an "end-to-end" encryption system that automatically generates by default a unique random key for each communication, which only the sender and the receiver possess. This prevents any third party outside the communication (including the company that developed the application) from being able to decrypt it in order to access its contents.

171. In addition, applications that use encryption to protect digital information stored on computer equipment (whether desktop computers, laptops, external servers, or storage units such as pen drives or removable hard disks) have also emerged. These applications allow both specific files and the entire disk to be encrypted with virtually invulnerable "strong encryption" protocols. Given the growing trend to replace paper documents with digital documents (including, of course, those that may be useful as evidence in ML/TF proceedings), the emergence of technologies that make it impossible for legally authorized authorities to access these documents poses a considerable challenge.

172. The availability of cheap or even free strong encryption tools (such as TrueKrypt, BitLocker or PGP) offers criminals with minimal computer skills the possibility of protecting their confidential information behind an insurmountable barrier. The problem this creates for investigative agencies has been getting worse from 2014 onwards, since the implementation by two of the major technology companies (Apple and Google) of full-disk encryption of computers containing operating systems developed by these firms, using private keys generated from the password

generated by each user of the device (which means that the company does not have this key and therefore cannot decrypt the contents of the disk).[69]

E. Technological developments that favor the investigation of ML/TF activities with virtual assets

173. Crimes that, as is the case with ML/TF with VAs, are committed to a large extent in cyberspace (i.e., so-called cybercrimes), therefore have special characteristics that distinguish them from crimes committed in the physical world. This, in turn, means that the investigation of such unlawful conduct requires the use of strategies, methods, techniques, and tools that are suited to the environment in which the investigation takes place (cyberspace) and to the type of evidence that must be obtained to prove the commission of the crime and the responsibility of the accused (electronic or digital evidence).

174. In this regard, it has been pointed out that the existence of procedural instruments that support the use of investigative techniques and tools suitable for the investigation of crimes committed in cyberspace is an essential requirement for the LEA to be effective in the fight against cybercrime. Consequently, countries without adequate legislation run the risk that their authorities will not be able to provide answers to citizens affected by cybercrime.[70] In this regard, organizations such as Interpol and Europol emphasize that the adoption of new technologies in the field of VA investigations is crucial to assist in the effectiveness of such investigations and increase the confiscation of funds of illicit origin. Therefore, they recommend the research and development of technological tools that facilitate the prevention and investigation of ML/TF conducts involving VAs.[71] In Latin America, the OAS has urged those states that have not yet done so to adopt or update, as soon as possible, the legislation and procedural measures necessary to ensure the collection and safekeeping of all forms of electronic evidence and its admissibility in criminal proceedings and trials.[72]

175. In this scenario, since the dawn of the new millennium, international instruments dedicated to the problem of cybercrime have begun to appear, starting with the Council of Europe Convention on Cybercrime (Budapest Convention), which, since its entry into force in 2001, has become the most relevant multilateral instrument on the subject at the global level. Subsequently, at the regional level, other documents have appeared on this issue, including the Caribbean Community Model Legislative Texts (ITU/CARICOM/CTU Model Legislative Texts), the Draft African Union Convention, the Commonwealth Model Law, the Draft Directive of the Economic

[69] Refer to: 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, p. 15.
[70] Caribbean Community Model Legislative Texts (ITU/CARICOM/CTU Model Legislative Texts), p. 8.
[71] Refer to: INTERPOL / Basel Institute on Governance / EUROPOL: "Recommendations. 4th Global Conference on Criminal Finances and Cryptocurrencies," November 2020, p. 3.
[72] Refer to: Organization of American States (OAS): *"Recomendaciones de la 9ª reunión del Grupo de Trabajo en Delito Cibernético,"* [Recommendations of the 9th Meeting of the Working Group on Cybercrime], Meetings of Ministers of Justice or Other Ministers, Attorneys or Attorneys General of the Americas (REMJA), December 12-13, 2016.

Community of Eastern Africa (ECOWAS Draft Directive), and the League of Arab States Convention.

176. Although there are some nuances among them, all these multilateral instruments coincide in pointing out that, in order to combat cybercrime more effectively, not only do countries need to criminalize the main cybercrimes, but it is also necessary to incorporate into the procedural regulations of the signatory countries provisions that legitimize the use of techniques and methods of investigation and evidence gathering appropriate to the problem of cybercrime. Among these, the following are worth mentioning:

- **Production orders:** These are orders issued by a judge or competent authority to require Internet service providers or other ICT-related companies to hand over relevant computer evidence in their possession or to which they have access in accordance with the law in force.

- **Preservation orders:** Orders issued by a competent authority, for the purpose of requiring Internet service providers or other ICT-related companies to preserve, for a certain period of time, information or digital evidence that is at risk of being altered or destroyed, in order to allow the legal steps necessary for its collection to be complied with.

- **Mandatory cooperation of Internet service providers or other ICT-related companies:** It refers to cases where it is necessary to provide technical assistance to the competent state authorities for the collection of computer evidence. This cooperation may include the obligation to keep the measures carried out in such context secret.

- **Search of computer systems or equipment:** This consists of the possibility for a magistrate to order the search of a system or device that may contain important digital evidence or information, in order to extract or copy it.

- **Extended access:** This consists of the possibility of remotely recording evidence or electronic information contained in another computer system or equipment accessible from and through the computer system being searched *'in situ'*, in order to extract or copy it. Generally, it is required for extended access to be considered legitimate that the state authority knows (or has reason to believe) that the second system or equipment is located within the same country in which the first search is carried out.

- **Obtaining electronic communications traffic data:** This consists of the possibility that a judge or competent authority may order the monitoring of electronic communications by law enforcement agencies (either with the cooperation of telecommunications companies or by their own technical means), in order to obtain "wrapper" data (i.e., data that does not include the content of the communications).

- **Interception of electronic communications content data:** This consists of the possibility that a judge may order the interception of electronic communications, either with the cooperation of the telecommunications companies or by its own technical means.

- **International cooperation:** The need to establish provisions that would allow countries to collaborate with each other to obtain digital evidence through production or preservation orders is mentioned. It also highlights the importance of implementing mechanisms to expedite the exchange of information, adapting it to the characteristics of digital evidence.

177. In this scenario, it is important to bear in mind that technological evolution not only favors criminals who seek to exploit its developments to facilitate the commission of crimes or hinder their investigation but may also offer advantages and innovative tools to the LEAs, which have the possibility of resorting to investigative techniques linked to new technologies to pursue (for example) possible ML/TF activities with VAs.

178. Thus, as far as the subject matter of this guide is concerned, it has been pointed out that the use of cryptocurrencies not only facilitates illicit exchange on the Internet, but also its detection, due to the public nature of the respective blockchains. Indeed, although Bitcoin and other similar currencies are commonly used to perpetrate crimes, some authors understand that, in fact, their use favors the investigation of illicit flows of funds.[73]

179. Both Bitcoin and most Altcoins do not offer true anonymity, but "pseudo-anonymity." This is because, although the identity of the users is protected under a pseudonym in the form of the alphanumeric sequence that constitutes their address, the data referring to the transactions they carry out (dates, amounts, balance and addresses of the counterparties) are recorded in a public registry (the corresponding Blockchain). This is inherent to the "distributed ledger technology" (DLT) on which the operation of cryptocurrencies is based,[74] by virtue of which the legitimacy of transactions—in the absence of a central authority to validate them—is given by their cryptographic record in blocks that make up a chain (the "Blockchain"). This, in turn, forms an unalterable sequential record of all transactions made with the cryptocurrency in question.

180. In this scenario, the public nature of the Blockchain allows the information contained therein to be mined for years in search of clues to determine the identity of the users. This has given rise to the so-called "Chain analysis" (in reference to the Blockchain), a term that encompasses a series of techniques based on the use of computer tools to reverse the anonymity of cryptocurrency users. The origin of these techniques—developed by private companies dedicated to assisting research agencies and other private entities in the identification of actors in the Blockchain—dates back to academic studies conducted since 2011, which demonstrated the limits of the pseudo-anonymity offered by Bitcoin and other cryptocurrencies.[75]

[73] In this sense, refer to 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, No. 5, 2019, pp. 1798/1853.
[74] For a detailed explanation on this technology, refer to: European Union Agency for Cybersecurity (ENISA): "Crypto assets. An introduction to digital currencies and distributed ledger technologies," February 2021.
[75] Refer to: ALSALAMI, Nasser / ZHANG, Bingsheng: "SoK: A systematic study of anonymity in cryptocurrencies," IEEE Conference on Dependable and Secure Computing (DSC), November 2019; BIRYUKOV, Alex / KHOVRATOVICH, Dimitry / PUSTOGAROV, Ivan: "Deanonymization of clients in Bitcoin P2P network," AAVV, *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Scottdale, 2014, pp. 15/29; Biryukov, Alex / Feher, Daniel: "Deanonymization of hidden transactions in

181. One of the main methods of deanonymization consists of determining the identity of the holders of certain addresses through the use of statistical tools that, based on the analysis of information contained in the Blockchain, link them to known addresses (for example, cryptocurrency exchange platforms, online marketplaces or persons already identified) or to pseudonyms published online. That is: data generated by exchange networks between users with proven links to illicit activities is exploited to reconstruct the complete chain of transfers between them and their customers or contacts. In order to identify relevant VAs addresses within the cryptocurrency ecosystem, investigators can also make payments with their own VAs to different services (exchange platforms, gambling sites, online wallets, etc.), or search the Internet for published VA addresses.

182. Chain analysis tools also take advantage of vulnerabilities intrinsic to the Blockchain network (such as the filtering of IP addresses and time stamps associated with each published transaction) to deanonymize users. And this is regardless of the specific Blockchain application they are using, and even when they resort to anonymity tools such as TOR. In this direction, academic works point out that it is possible to take advantage of a countermeasure built into the Bitcoin system to repel DDoS attacks, so as to prevent users from hiding through the use of TOR.[76] The method known as "dusting attack" can also be used, which consists of sending traces of cryptocurrencies (known as "dust") to thousands (or hundreds of thousands) of wallets and then analyzing their subsequent movements in search of clues as to the identity of their holders.

183. When large VAs transactions take place, tracing the movements of those involved through chain analysis methods is easier, which is important because the Bitcoin ecosystem and the main cryptocurrencies do not offer a high degree of anonymity for major money laundering transactions. The traceability of transactions is even greater if there is access to a central service, such as a VASP.

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, p. 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, pp. 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, pp. 127/140; and 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," Proceedings on Privacy Enhancing Technologies, Vol. 3, 2018, pp. 143-163.

[76] Refer to: BIRYUKOV, Alex / KHOVRATOVICH, Dimitry / PUSTOGAROV, Ivan, "Deanonymization 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, pp. 15/29.

184. The increasing transparency of the Bitcoin Blockchain and the main Altcoins has led to the emergence of so-called "private currencies," such as Monero or Zcash. However, academic studies have shown that also users of private currencies can be de-anonymized with a higher degree of accuracy than expected,[77] exploiting specific features of the functioning of such VAs.

185. In the case of Monero, advantage is taken of the way in which "filler coins" (called "Mixins") are created and used to obfuscate the identification of those that are actually exchanged. As far as Zcash is concerned, an analysis of the operation of this cryptocurrency found that only 3.5% of the operations carried out with it involve the increased anonymity variant offered by the system, and of those, up to 31.5% of the movements can be reconstructed using advanced analytical tools. This means that, in practice, 98% of Zcash transactions are subject to traceability.[78]

186. The availability of software tools designed to exploit the characteristics of cryptocurrencies to enable the deanonymization of their users is not, however, the only product of the technological evolution of the last two decades that favors state surveillance. On the contrary, the shift of modern societies towards the massive, widespread and constant use of ICTs for the realization of virtually all human activities (whether institutional, commercial, informational, educational, academic, recreational, and, of course, also criminal), whose main consequence is the generation of a huge amount of data linked to these activities, which can be "mined" by LEAs for investigative purposes, can also be exploited for this purpose. The exploitation of this accumulation of data is favored by the fact that such data, being digital, is generated, cross-referenced and stored much more easily. Especially since the emergence of the tools that make up the phenomenon known as "Big data," specifically designed to allow the analysis of huge volumes of information.

187. Another fundamental feature of the new technological reality that can be exploited for the purposes of state "computer surveillance" is that the prevailing business model of the main technology companies—especially around the Internet—is based on the exploitation of user-generated data. Consequently, in practice, the companies themselves have generated, for commercial reasons, a veritable "surveillance superstructure" of unprecedented proportions, the results of which can be accessed by state agencies by requesting the cooperation of private parties, as recommended by the international instruments mentioned above.

188. In such a context, LEAs are in a position to access three main categories of information on citizens. Namely:

a. Information on communications and movements collected by telecommunications companies (including both those generated constantly, as a result of communication

[77] Refer to: European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses," Policy Department for Citizen's Rights and Constitutional Affairs," May 2018, pp. 34/35.
[78] Refer to: DUPUIS, Daniel / GLEASON, Kimberley: "Money laundering with cryptocurrency: Open doors and the regulatory dialectic," Journal of Financial Crime, August 2020.

between smartphones and cell phone towers, and those generated by GPS devices inserted in most of these devices and collected by applications that are enabled to "know the location" of users).

b. Data stored and processed by Internet companies (including that derived from search histories in Internet search engines, data, and metadata generated by interaction in social networks, data on purchases or browsing in online marketplaces, and information on Web browsing collected by cookies on Web pages); and

c. The information generated by the devices comprising the so-called "Internet of Things" (IoT).

189. In addition, the advent of the digital era has resulted in a significant increase in the capacity of traditional state surveillance techniques, as a result of the availability of technological tools such as digital cameras (including those installed in closed circuit systems on public roads, infrared cameras or those placed in unmanned aircraft—"drones,"—GPS devices, digital spy microphones, cell phone cell simulator equipment, and technologies for interception and analysis of Internet traffic, among others).

190. The main consequence of these technological advances is that the effectiveness of surveillance carried out by the State is no longer limited by its magnitude or duration, since the decrease in technology and data storage costs has eliminated many of the financial or practical drawbacks traditionally involved. Consequently, states have, as never before, the potential to conduct simultaneous, invasive, targeted, and large-scale surveillance activities.[79]

191. Finally, two other tools have emerged that are specifically designed to respond to the anti-forensic defenses employed by modern cybercriminals (including crypto-launderers) by taking advantage of the very features of the Internet and the computer systems they exploit to carry out their illicit activity. Thus, the possibility of surfing the Net anonymously allows "digital undercover agents" to operate, while the existence of vulnerabilities in computer programs opens the door to state hacking.

192. The use of digital undercover agents basically consists of taking advantage of anonymity tools such as TOR and the widespread use of pseudonyms on the Internet (and especially on the dark web) so that investigative agency personnel (designated and authorized in accordance with the legislation of each State) can interact online with potential criminals, penetrate organizations and obtain evidence that can be used to obtain a conviction.

193. State hacking involves adapting the "Trojan" or spyware programs used by cybercriminals so that they can be used to obtain information or computer evidence remotely (i.e., without making

[79] Refer to: United Nations Organisation (UN): "The Right to Privacy in the Digital Age," Statement A/HRC/27/37, Report of the Office of the United Nations High Commissioner for Human Rights, June 2014, p. 3 § 2.

physical contact with the device that stores or generates the data). This has two major advantages for investigators: (a) that, unlike physical searches, the remote collection of evidence can be carried out surreptitiously, without notifying the person under investigation of the existence of the investigation; and (b) that it can be carried out even if the location of the person under investigation and/or the location of the device into which the spyware is being introduced is unknown.

194. Furthermore, the use of state spyware has multiple uses. It can be used not only to remotely access stored data, but also to obtain access keys to encrypted documents or those stored on external servers, to monitor communications over the Internet, to carry out acoustic or audiovisual surveillance, to locate and individualize people who contact certain pages (or individuals) over the network, or to track subjects under investigation in real time.

195. The first records of spyware use by state investigation agencies date back to more than two decades ago.[80] This tool began to be used in the USA and was later adopted also in other countries, such as Italy, France, Germany, the United Kingdom, Australia, and Israel.[81] In some countries (Spain, France, England, the Netherlands, Poland), the use of spyware is expressly regulated in local procedural law, while in others (USA, Australia, Germany, Italy) its use is governed by the analogical application of procedural rules relating to traditional investigative measures.[82]

196. In turn, two of the international instruments on cybercrime mentioned above refer directly or indirectly to the possibility of resorting to the use of spyware to obtain data on the content of communications. Thus, the Commonwealth Model Law (art. 18.b) mentions the possibility of law enforcement agencies obtaining content data through "the application of technical means;" while the Model Legislative Texts of the Caribbean Community (art. 27.1.) refer to the possible use of "forensic software" for investigative purposes.

197. Since the use of spyware by the State has become widespread, the fact that it can be used in a more invasive way than traditional measures—to the extent that it is possible to obtain, by this means, all the information contained in a smartphone (beyond the fact that, according to the legislation in force in each country, it is generally the applicable judicial authority who decides the extent to which this tool will be used)—has led international organizations such as the United Nations to express their concern about the possible impact on the right to privacy derived from

[80] Refer to: CARRELL, Nathan E.: "Spying on the mob: United States v. Scarfo – A constitutional analysis," Journal of Law, Technology & Policy," Vol. 2002, No. 1, 2002, pp. 193/214.
[81] Refer to: United against crime: Improving criminal justice in European Union cyberspace, Instituti Affari Internazionali, 2016 and 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] Refer to: 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.

practices that take advantage of the vulnerability of digital communication technologies for electronic surveillance.[83]

198. However, the UN itself has also recognized that since digital communication technologies can be, and have been, used by private individuals for criminal purposes (such as recruitment for and financing of terrorist attacks), lawful and targeted surveillance of digital communications can be a necessary and effective measure for law enforcement agencies when carried out in compliance with international and national law.[84] In the same sense, ENISA and Europol have also expressed their views at the European level.[85]

199. In this context, it is generally considered preferable that the use of new forms of electronic surveillance such as state spyware be expressly regulated, since it is understood that the analogical application of existing rules may not be able to compensate for the invasive nature of such an investigative tool.[86] However, in the absence of express regulation, where the legislation in force authorizes analogical application, it is possible to reduce the risks with respect to the right to privacy and ensure proportionality between the restriction to that right and the state purposes by adopting, at the time of ordering a measure of this type, the prior and subsequent requirements established in the rules of the countries that have legislated on the matter.

200. Such requirements include the need for judicial authorization, the restriction of the use of state hacking to the investigation of serious crimes, the setting of limits on the mode of use, the requirement of separate authorizations for each function of the state spyware, the control over the operation of the computer tools used, and the destruction of irrelevant information. It is also advisable to establish the obligation to remove the software after its use, to notify the interested parties, and to implement mechanisms to supervise the use of spyware, among others.

[83] Refer to: United Nations Organisation (UN): "The Right to Privacy in the Digital Age," Statement A/HRC/27/37, Report of the Office of the United Nations High Commissioner for Human Rights, June 2014, p. 3 § 3. The UN issued statements linked to the "right to privacy in the digital age" in 2013, 2014 and 2016. Refer to: UN: "The Right to Privacy in the Digital Age," Statement 68/167, December 18, 2013; "The Right to Privacy in the Digital Age," Statement 69/166, December 18, 2014; and "The Right to Privacy in the Digital Age," Statement A/C.3/71/L.39/Rev.1, December 19, 2016.
[84] Refer to: United Nations Organisation (UN): "The Right to Privacy in the Digital Age," Statement A/HRC/27/37, Report of the Office of the United Nations High Commissioner for Human Rights, June 2014, p. 9 § 24.
[85] Refer to: European Union Agency for Cybersecurity (ENISA) and Europol: "On lawful criminal investigation that respects 21st century data protection. Europol and ENISA joint statement," statement of May 20, 2016.
[86] Refer to: 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, pp. 12/13. In the same sense: UN: "The Right to Privacy in the Digital Age," Statement A/HRC/27/37, Report of the Office of the United Nations High Commissioner for Human Rights, June 2014, pp. 10/11, § 28; and ENISA/EUROPOL: "On lawful criminal investigation that respects 21st century data protection. Europol and ENISA joint statement," statement of May 20, 2016, p. 1.

F. Regional situation with respect to the incorporation of new technological investigation methods

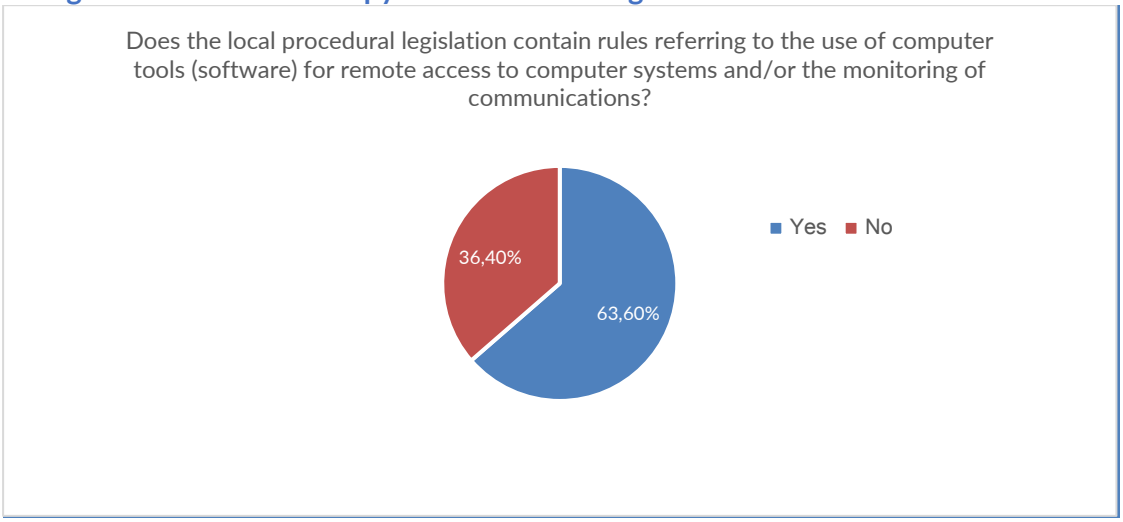
201. The relationship between new technologies and the investigation of cybercrime was the subject of a global survey conducted by the UNODC in 2013,[87] which highlighted the problems and challenges generated by the emergence of technological tools with anti-forensic capabilities. These same issues were later pointed out by other organizations linked to police agencies, such as the International Association of Chiefs of Police (IACP).[88] In contrast, the European Parliament carried out another survey, in this case on the use of spyware by the state as a means of counteracting the above-mentioned problems,[89] which revealed the growing adoption of this tool by the USA, several European countries, Israel, and Australia.

202. In the questionnaire sent out for the purposes of this guide, the RRAG contact points were asked whether the procedural legislation in their respective countries contained rules on the use of software tools for remote access to computer systems and/or monitoring of communications, as well as on investigation using open-source intelligence techniques (OSINT). Also, whether, if not, the existing procedural rules can be used analogically to cover the use of investigative techniques not expressly regulated.

203. As to whether the procedural legislation covers the use of spyware, a large majority of the countries that responded (7 out of 11, 63.6%) did so in the affirmative. It can be seen, however, that the answers do not show that the rules cited expressly refer to the use of computer tools (as is the case, for example, with the legislation of Spain, France, England or the Netherlands), but rather that such use is interpreted as falling within the scope of the rules governing, in a generic way, the interception of electronic communications and other measures in which spyware can be used, either by establishing that such a measure can be carried out by "any technical means" or without saying anything about it. In other words, they leave it up to the authority in charge of carrying out the measure to choose the technical resources to be used for this purpose.

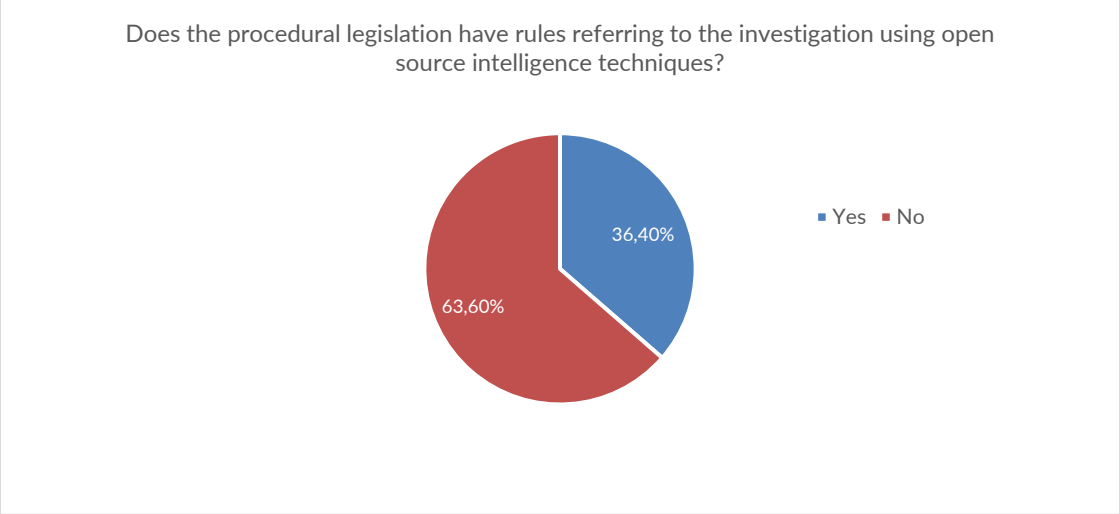
[87] Refer to: United Nations Office on Drugs and Crime (UNODC), *Comprehensive study on cybercrime*, 2013.
[88] Refer to: International Association of Chiefs of Police (IACP): "Data, privacy and public safety. A law enforcement perspective on the challenges of gathering electronic evidence," IACP Summit Report, 2015.
[89] Refer to: 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.

Graph 4: Regulation of the use of spyware as an investigative tool:



204. The situation is different with regard to OSINT techniques, since in this case most of the countries that responded (7 out of 11, 63.6%) answered that the use of such techniques is not regulated.

Graph 5: Regulation of the use of OSINT techniques:



205. In any case, the fact that the information obtained through OSINT techniques is—as its name indicates— "open source," determines that the lack of express regulation does not constitute an obstacle for the use of this investigative method.

206. Moreover, the responses to the questionnaire show that a large majority of the countries that replied (7 out of 11, 63.6%) indicated that the local procedural system allows for the analogous application of both investigative techniques (spyware and OSINT). Of the remaining 4, one did not

rule out that such analogical use is feasible but stated that it could not provide a definition on the matter because it was left to judicial interpretation. In two of the other three cases, the negative response was due to the fact that the analogical application was not necessary in view of the existence of procedural rules that, in the opinion of the reporting authority, support the use of the investigative measures in question.

207. When evaluated as a whole, the responses to the questionnaire suggest that there is a favorable scenario in the region, in principle, for the implementation of new computer investigation techniques in the framework of asset investigations related to cybercrimes in general, and ML/TF activities with VAs in particular.

G. Treatment of digital evidence

208. A common element in the investigation of ML/TF activities with VAs and the technological tools that can be used to carry out such investigations (and even to seek the confiscation of such assets), is that in both cases, there is digital information generated by ICTs.

209. ICTs are, in fact, the central element that makes the use of VAs possible, since they operate in the virtual environment and all operations related to them involve, at some point or another, the use of computer systems and data. The only "paper" traces, if any, could be found in the records generated by VASPs when VAs are exchanged for fiat currency or vice versa. Therefore, most of the evidence that will eventually be incorporated into legal proceedings to prove illicit transactions with VAs—and certainly the most important—will be almost exclusively in electronic or digital format.[90]

210. In this regard, the UNODC points out a series of relevant features of electronic or digital evidence, which should be taken into account for the purposes of searching, obtaining, maintaining, and analyzing it, and which are of great importance in the context of VA ML/TF investigations.[91] Namely:

- **Difficult traceability:** It results from the circumstance that it is found in places where it can only be detected by specialists, and through the use of specific tools, which allow not only to identify the truly relevant information—separating it from that which is not—but to infer it from the interweaving of apparently innocuous data.

- **The need for the intervention of specialists,** since, without their participation, the information located in the computer systems cannot be extracted in such a way as to

[90] Refer to: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014, p. 60.
[91] Refer to: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014, pp. 61/62.

guarantee that it is reliable and has not been manipulated or altered in any way. The intervention of specialists is also necessary to identify and process related information that may be relevant to the investigation. If the investigation is also related to ML/TF schemes, the specialization of the experts involved should also include knowledge of finance, money laundering methodologies and other such matters.

- **High volatility,** since the computer systems that create, process, and store digital evidence destroy, as part of their routine operation, some of the existing data whenever certain events occur, such as automated updates that overwrite old information in order to free up space for new information.

- **Susceptibility to alteration.** Computer systems or equipment constantly modify the state of their memories, either at the user's request (when saving, copying or updating operations) or automatically (allocation of memory space, temporary storage, scheduled updates, etc.). This feature is relevant to understand the inherent temporal limitations of computer evidence and to be able to manipulate such evidence appropriately from the very moment it is identified as relevant to an investigation.

- **Ability to copy unlimitedly.** Digital information can be copied indefinitely without losing reliability. That is: so that each copy is identical to the original. While this may be problematic for the differentiation between the original and the copy, once it is established that the copies are, in fact, identical to the original, it becomes an advantage, insofar as it allows the distribution of exact copies of the relevant evidence to be analyzed simultaneously by different experts.

211. It follows that the treatment of digital evidence requires greater resources (in terms of technology and specialized human resources) than physical evidence, since the intervention of untrained agents in operations where this type of evidence may be found may not only result in relevant evidence being overlooked, but also in it being accidentally altered or destroyed. Likewise, for it to be truly effective in a judicial process, it must be obtained, safeguarded and analyzed in such a way as to guarantee its authenticity, completeness, reliability, and verisimilitude.

212. The ability to ensure that these standards are met is an essential requirement in relation to the computer tools used to obtain electronic evidence, such as state spyware. This is so, since—in view of the novel nature of these methods—the question of the reliability of the information retrieved becomes crucial for the operators of the judicial system to be convinced that they constitute a legitimate means of incorporating evidence into a criminal proceeding. Therefore, the technological tools used must ensure that it is possible to capture the evidence sought in compliance with the aforementioned guidelines.

213. Moreover, the predominant role that electronic evidence—and potentially also the use of new technological tools—is acquiring in cybercrime investigations in general and ML/TF schemes involving cryptocurrencies in particular, requires the development of new knowledge for all those involved. This includes both the members of the police agencies or departments of the Public Prosecutor's Office who led the investigations, as well as the magistrates who must authorize the adoption of measures or the use of techniques involving ICTs (from the analysis of the Blockchain to the use of spyware, including the use of modern surveillance techniques) or weigh the resulting evidence. The reality shows, however, that there is a significant deficit in terms of the training of relevant actors in all matters concerning the link between ICTs and criminal investigations, which poses a concrete risk to the effectiveness in the prosecution of ML/TF schemes involving cryptocurrencies and the seizure and confiscation of VAs.

214. In view of this, and for the purpose of providing competent authorities in general and police agencies in particular with useful tools to effectively fulfill their functions with regard to the collection, custody, processing, and analysis of electronic evidence, a series of protocols containing standards or good practices on the subject, developed by bodies or agencies specialized in law enforcement or in the use of new technologies, have been emerging around the world.

215. These include the following: "First Responders Guide Template" of the IOCE; RFC 3227 of the Internet Engineering Task Force – Internet Society (IETF-ISOC); "Electronic Crime Scene Investigation, a Guide for First Responders" of the 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" and "Investigation Involving the Internet and Computer Networks," all from the National Institute of Justice (NIJ) of the U.S. Department of Justice (DOJ); "APCO Good Practice Guide for Digital Evidence" of the Association of Chief Police Officers (APCO); "Identification and Handling of Electronic Evidence" of the European Union Agency for Cybersecurity (ENISA); and ISO/IEC 27037:2012 "Information Technology -Security Techniques- Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence."

216. In this context, in the questionnaire addressed to the RRAG contact points for the purpose of preparing this guide, the countries were first consulted on the application of protocols that regulate the treatment of computer evidence. Of the countries that responded to the questionnaire, a large majority (13 out of 16, 81%) responded that they have their own protocols regulating the actions of the security forces in the collection of computer evidence and/or the seizure of computer devices.

217. It is worth mentioning, however, that of the three countries that responded negatively, one (Colombia) reported that despite not having protocols that regulate the activity of security forces

in the collection of digital evidence, local regulations do contain protocols on the matter, although addressed to the Attorney General's Office.

218. From the above it is clear that there is, in general, a high degree of awareness in the region of the need for protocols regulating the collection of evidence. Even in those cases in which no good practice guides have been developed on the matter at the internal level, the above mentioned can be taken as a reference, where appropriate.

219. Moreover, with regard to the existence of specialized cybercrime investigation or cybersecurity units, there is also a substantial majority of positive responses, although not as large as in the case of protocols (11 out of 16, 69%).

220. Likewise, of the seven countries that responded affirmatively, four reported having specialized units of the Public Prosecutor's Office, with a fifth reporting that the creation of such a prosecutorial unit is currently being planned.

H. Problem of VAs seizure

221. Due to the particular characteristics of VAs, their seizure or confiscation may be considerably more difficult than that of tangible assets such as fiat currency. However, the experience gathered since the emergence of Bitcoin to date shows that this can be achieved. This was demonstrated by the closure of Silk Road, the first illicit online marketplace to operate with VAs as a means of payment, when an extensive FBI asset investigation culminated in the arrest of the marketplace's creator and the seizure of bitcoins valued (at the time) at between 3.5 and 4 million dollars.

222. In the following years, there were other confiscations of cryptocurrencies (mostly bitcoins, but not exclusively) valued at millions of dollars in Europe, Australia, Japan, and China. The most recent were the seizure of VAs subtracted by a hacker from Silk Road accounts and the confiscation of cryptocurrencies originating from the "PlusToken" pyramid scheme by Chinese authorities, totaling approximately $4 billion. There were also seizures linked to terrorist financing, such as the capture of around 2 million VAs belonging to terrorist groups (including Al-Qaeda, ISIS and Hamas) in August 2020.[92] Even "private currencies" were confiscated. In one case, approximately 3,691 Zcash were seized that were in the hands of the administrator of the now defunct illicit online marketplace AlphaBay (one of the successors of Silk Road), who had been arrested in 2017.[93]

223. Also, from the responses received to the questionnaire sent during the development of this guide, it appears that European countries that are observers in the RRAG reported cases in which

[92] Refer to: CipherTrace: "Cryptocurrency crime and anti-money laundering report," February 2021.
[93] Refer to: 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.

they managed to "block" VAs of a suspect on a cryptocurrency exchange platform (Spain), seize VA wallets (Andorra), and transfer VAs belonging to suspects to wallets controlled by state authorities (France).

224. Similarly, at the regional level, a favorable scenario is noticed, from the regulatory point of view, for the implementation of seizure and confiscation measures. In this regard, it should be noted that from the results of the 4th Round of Mutual Evaluations on compliance with FATF standards, 12 of the 17 GAFILAT countries that have been evaluated, have a degree of compliance between mostly compliant and compliant with Recommendations 4 and 38. Under these Recommendations, countries are required to establish mechanisms to enable their competent authorities to effectively manage and, when necessary, dispose of frozen, seized or confiscated assets. These mechanisms should be applicable both in the context of domestic proceedings and pursuant to requests from foreign countries.[94] This is illustrated below[95]:

Table 1: Compliance with FATF Recommendations 4 and 38:

Rec	Cuba	Costa Rica	Honduras	Guatemala	Nicaragua	Mexico	Panama	Peru	Colombia	Dominican Republic	Uruguay	Chile
R.4	LC	LC	C	LC	LC	LC	C	C	C	C	LC	LC
R.38	LC	LC	LC	LC	LC	PC	LC	C	C	LC	LC	C

225. It should be noted, however, that none of the regulations outlined in the responses received expressly refers to the seizure and/or confiscation of VAs. However, following the reform of FATF Recommendation 15 (in order to incorporate the aforementioned assets in AML/CFT systems), these Recommendations, particularly those relating to international cooperation (R.38), should also apply to VAs.[96]

226. Even so, the FATF itself recognizes that many LEAs or prosecutors' offices lack the knowledge and/or resources required to investigate illicit conduct related to VAs. It points out that most investigators have not yet encountered such assets in their investigations and face a steep learning curve when they do.[97]

227. In this context, the countries of the region are beginning to take the first steps in this direction. In fact, from the responses received, 8 of the 16 (50%) countries consulted reported having registered ML/TF investigations with VAs.

[94] It is important to note that in this 4th Round, the countries that were already evaluated were not considered to include VAs or VASPs given the recent changes in the FATF Standards. Special mention is made of these Recommendations given the obligations of the competent authorities to freeze and confiscate property or assets.
[95] Source: GAFILAT: "2020–2025 GAFILAT Strategic Plan," pp. 26/27. The ratings of the recommendations (R) are adjusted according to the Re-rating reports presented by the GTEM and approved by the Plenary of Representatives.
[96] Refer to: FATF: "Virtual assets and virtual assets service providers. Guidance for a risk-based approach," June 2019, p. 33 § 137.
[97] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 36 § 119.

228. With regard to seizure or confiscation of VAs, three countries (Argentina, Brazil and Chile) reported the adoption of measures to achieve this goal, while another, which also had cases, did not provide information on whether or not measures were adopted on the VAs involved. Thus, with regard to Argentina, a case was reported in which, after identifying a virtual wallet located on a VA exchange platform on behalf of a company involved in the laundering of drug trafficking proceeds, the funds were seized for the purpose of confiscation. For this purpose, the VAs contained in the wallet (approx. USD 295,000) were transferred to a wallet controlled by the intervening court. In other pending cases, the specialized ML/TF prosecutor's office suggested the adoption of similar measures in relation to funds in custody of exchange platforms, but so far, the seizure of the VAs has not been achieved.

229. Brazil reported four cases in which the authorities adopted precautionary measures related to this type of assets. These are the operations "Faroeste," "Rekt," "Faraó," and "Egipto." In the first case mentioned, the use of cryptocurrencies (especially Bitcoin) as one of the means of payment in an alleged scheme for the sale of judgments in a local court was investigated. In the remaining three, a considerable amount of VAs was successfully blocked by court orders directed against "custodial" wallets held by VASPs. Thus, under "Operation Rekt," the injunction targeted VAs valued at BRL 110 million, allegedly originating from drug sales. In "Operation Faraó," bitcoins worth BRL 6.4 million were frozen, linked to a pyramid scheme. While "Operation Egypt" involved the freezing of USD 24 million in cryptoassets that were in the custody of a cryptocurrency exchange platform registered in the USA, also in connection with an investigation into an alleged pyramid scheme.

230. Finally, Chile reported that in a case investigating drug trafficking and ML offenses, a significant amount of cryptocurrencies was seized in a virtual wallet belonging to one of the suspects, which were transferred to an account controlled by the Public Prosecutor's Office for safekeeping.

V. RECOMMENDATIONS, STEPS TO BE TAKEN, AND CONCLUSIONS

A. Introduction

231. The main objective of an asset investigation is to identify and document the movement of funds originating from—or linked to—criminal activity. To this end, the links between (i) the origin of the funds; (ii) their beneficiaries; and (iii) the times at which the funds are received and the places where they are stored, deposited or transferred are valuable sources of information for investigations into the underlying criminal activity.[98]

[98] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 7 § 1.

232. With regard to ML/TF criminal operations with VAs, it is important to bear in mind that beyond the special characteristics of these assets, which make them more vulnerable to exploitation for criminal purposes and represent an additional difficulty for investigators, the fact is that the way in which such criminal operations are detected and investigated is not different from that used in traditional cases of ML/TF or illicit behavior of a patrimonial nature.

233. The patrimonial investigation related to the use of cryptocurrencies can go in two directions. On the one hand, it can start from the finding of the existence of criminal activity and attempt to trace VAs to its beneficiaries (as occurred in the "Welcome to video" case reviewed below, Case § 4). In such a context, ML behaviors with VAs are often identified as the result of an investigation concerning criminal activities that involve the intensive use of cash, are carried out online or are likely to generate significant amounts of illicit proceeds.[99] Among the criminal activities that may derive from the use of cryptocurrencies, there may be traditional criminal behavior brought to the online world (such as drug trafficking in the Dark Web markets); or cybercrime as such, such as ransomware, extortion based on the theft of confidential information, or various forms of computer fraud.

234. On the other hand, the investigation may find as a starting point certain transactions with VAs considered suspicious, either because they were carried out or are connected with persons known to be involved in illicit activities, or because they have been identified as suspicious by a Financial Information Unit (FIU) or other similar body (e.g., because they resemble those carried out by "money mules" or because they are carried out by VASPs known to be involved in the provision of ML/TF services, such as "mixers").

235. In order to make asset investigations more effective, the authorities responsible for conducting them should have at their disposal the widest possible range of information, whether from their own sources, from exchanges with other national authorities, or from cooperation with third parties (e.g., in the private sphere). The FATF highlights different categories of information relevant to asset investigations.[100] Namely:

- **Criminal records and intelligence information:** This refers to information stored by LEAs regarding persons under investigation with potential links to criminal activity. In the context of VAs, it may include data on suspected illicit activity by such persons on the Dark Web; identification of their pseudonyms or aliases; addresses of known cryptocurrencies or accomplices (and their pseudonyms or aliases); prior arrests or convictions; physical or electronic addresses, telephone numbers or email addresses that they may have used in connection with criminal activities. This information may come from proprietary databases

[99] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, pp. 12/13, § 24.
[100] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 16/16, §§ 42/49 (refer, in turn, to FATF: "Operational issues – Financial investigations guidance," June 2012).

or be obtained by querying databases maintained by law enforcement organizations such as Interpol or Europol.

- **Information from AML/CFT controls:** Suspicious transaction reports (STRs) originating from FIUs generally contain a wealth of information regarding the asset profile and activities of the persons under investigation. In investigations linked to the use of VAs, STRs originating from VASPs capable of linking their customers with the transactions carried out are of special importance.

- **Patrimonial information:** This includes all information that may be obtained from compliance with the CDD duties of the reporting institutions under the AML/CFT regulations. That is: bank accounts, financial or commercial records, etc. Regarding the use of VAs, it may include records of transactions carried out through VASPs, or of VASPs with traditional financial entities, or any other asset activity that may generate suspicions of the possible use of VAs to recycle funds of illicit origin.

- **Information from regulators:** That is, all information held by supervisory bodies such as central banks, tax authorities, stock market, or insurance regulators, etc.

- **Open-source information:** It includes all information that can be obtained through open sources of unrestricted use, such as the Internet, social media, print or electronic media or publicly available records. In the context of ML/TF investigation with VAs, it may comprise data such as the price of different cryptocurrencies, contact information or VASPs data, or links between the persons under investigation and potential identifying information (cryptocurrency addresses, wallets, links to criminal activity or criminals, etc.). At the regional level, the RRAG has published a list of open sources from member countries.[101]

236. Likewise, taking into account the close relationship that in many cases ML operations with VAs have with cybercrime, valuable information can also be found in the possession of national units specialized in cybersecurity, in countries where such units exist. This may include: (a) reports on incidents involving the financial sector; (b) information on malware aimed at identity theft or unauthorized collection of confidential and/or financial information (including data or programs used for VA management); and (c) intelligence on the hacker community or on cybersecurity threats.[102]

B. Importance of links between VAs and fiat currency

237. Given that a large part of VA transactions take place in cyberspace, an essential focal point of asset investigations into illicit conduct involving this type of assets lies in the identification of

[101] Refer to: GAFILAT /RRAG: "List of open sources of RRAG member countries," June 2021.
[102] Refer to: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014, pp. 87/88.

the links between the physical and virtual worlds, where the exchange between VAs and fiat currency takes place. These links function both as a "gateway"—when criminals intend to carry out crypto-laundering maneuvers for the placement and/or layering of illicit funds obtained in fiat currency (converting them into cryptocurrencies)—and as an "exit ramp," in cases where the beneficiary of a crime attempts to withdraw the illicit gain and convert it into traditional money, either to spend it or to reinvest it more easily.

238. This "exit ramp" or "gateway," from or to the VA ecosystem, is, in practice, the vulnerable point of any ML/TF scheme involving these values, especially when significant amounts are handled, given that the (relatively) small nature of cryptocurrency markets make them more sensitive to massive inflows or outflows of funds, which usually cause sharp rises or falls in the value of the VAs, which in turn invite scrutiny of the transactions that caused them.

239. It is also important to bear in mind that VA exchange networks are populated by centralized intermediaries, such as exchange platforms and custodial wallet services. Even though cryptocurrencies were created to operate with a decentralized structure, and the exchange between users within the network is quite simple, converting fiat currency into VAs or vice versa can be difficult without the assistance of a third party, especially if you are dealing with cryptocurrencies for the first time. Exchange platforms emerged to fulfill this role and have become so prevalent that they now account for up to 99% of cryptocurrency transactions.[103] A large part of this volume is handled by major international platforms such as Binance, Bitstamp, Bitfinex, Coinbase, and Kraken.[104]

240. There are also numerous platforms dedicated to VA exchange in Latin America, most of which provide services in more than one country in the region: 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, and CritoWay, among others.

241. This means that, in practice, almost all VA transaction chains are bound to pass, at one time or another, through one of these intermediaries. Thus, the insertion of this centralized element in a naturally decentralized ecosystem generates bottlenecks that can be exploited for greater efficiency, both in supervision and in the investigation of criminal conduct involving VAs. Hence, the new FATF Recommendation 15 requires that local regulations impose on VASPs the obligation to collect, maintain, and share with competent authorities' information obtained through CDD,

[103] Refer to: 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 (quotes data from: MOISENKO, Anton / IZENMAN, Karla: "From intention to action: Next steps in preventing criminal abuse of cryptocurrency," Royal United Services Institute (RUSI) Occasional Paper, London, 2019).
[104] Refer to: European Parliament: "Virtual currencies and terrorist financing: Assessing the risks and evaluating responses," Policy Department for Citizen's Rights and Constitutional Affairs, May 2018, p. 40.

which can be extremely useful for investigative agencies to identify persons operating with AML/CFT, in addition to being a potentially useful source of evidence on ML/TF schemes.

242. Given that VASPs constitute the first line of alert regarding ML/TF with VAs—insofar as they are in a privileged position to detect possible suspicious transactions and report them to the respective FIUs—STRs derived from transactions considered suspicious by them constitute one of the main sources of information for asset investigations concerning illicit maneuvers with decentralized VAs (in particular, cryptocurrencies).[105]

243. In this regard, the list elaborated by the FATF on the main "red flags" of suspicious activity with VAs in its June 2020 report should be considered as the main reference on the issue.[106] In turn, in a previous report, the FATF highlighted the following as the most relevant red flags:[107]

- Structuring VA transactions to circumvent registration or reporting thresholds (similar to the structuring of cash transactions).
- Transfer of VAs operating on a public and transparent Blockchain (such as Bitcoin) to a centralized exchange platform, for immediate conversion into "private currencies" (such as Monero, Zcash, or Dash).
- Depositing VAs on an exchange platform and subsequent (often immediate) withdrawal, without additional exchange activity, which is an unnecessary step that generates the payment of transfer fees.
- Transactions with VA addresses linked to known fraudulent schemes or with markets on the Dark Web.
- Creation of separate accounts under different names to circumvent restrictions on operating or withdrawal limits imposed by VASPs.
- Using money transfer services advertised on P2P platform sites.
- Making a large initial deposit to initiate a new relationship with a VASP.
- Transfer of VAs from/to wallets whose previous activity indicates the use of mixing services.
- Transactions with VAs originating from or directed to online gambling services.

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

- Use of multiple credit or debit cards associated with a VA wallet to withdraw significant amounts of fiat currency ("cryptocurrencies to plastic"); and

- Use of "cold" storage wallets to transport VAs across borders.

244. The information generated by FIUs from data obtained by VASPs (or by traditional financial entities, which operate with VASPs) in compliance with their AML/CFT obligations is of great potential value for asset investigations. Similarly, it can be seen that the STRs submitted by these entities upon detection of any of the "red flags" mentioned above contain both information on transactions (issuing customer, beneficiary, addresses of the customer's wallets, balance in the wallets, date and time of the transactions, type of VA transferred, location of the transfer, canceled transactions, bank accounts registered or verified, and type of devices used); as well as customer information (name, user identification, IP address, physical billing address, e-mail address, date of birth, nationality, citizenship, economic profile and commercial activity).[108]

245. The role assigned to the VASPs as the first warning line in the prevention of ML/TF with cryptocurrencies and their effectiveness in the global AML/CFT structure depend on their activity being regulated in a homogeneous manner at a global level. In such a context and given the ease with which VAs can be transferred and services linked to such assets can be offered across borders on the Internet, the existence of jurisdictions with weak or non-existent controls with respect to VASPs poses a vulnerability to the entire system.

246. Although many VA payment platforms or processors seek to operate within the framework of legality, there are also others that do not. The latter are favored by the very nature of cryptocurrencies, which facilitates the existence of VASPs that operate beyond state regulation, taking advantage of anonymity tools on the Internet that allow them to hide their true location and offer their services to customers around the world. As previously mentioned, these VASPs process a significant percentage of illicitly sourced VAs.

247. In this context, investigative agencies should place special emphasis on the activities of "mixers" or "tumblers" and online gambling sites, which concentrate a high volume of criminal proceeds. Investigations related to the use of VAs should aim not only to identify and prosecute persons who exploit the use of cryptocurrencies to carry out criminal activities, but also to prosecute and eventually stop the activity of VASPs or other service providers when such activity is aimed at favoring or facilitating criminal operations.[109]

248. A favorable aspect for the actions of the authorities against VASPs that act illegally is that, in general, there is usually a certain concentration in terms of the actors that provide services to

[108] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 19 § 55.
[109] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 44 § 147.

criminals. Thus, a recent study on the activity of mixers and online gambling sites that receive funds of illicit origin found that three of these services accounted for 97% of the bitcoins originating from recognized criminal activity.[110]

249. Therefore, identifying those responsible for these services should be a priority for the LEAs. Even if they do not publicize their location or the identity of their owners, there are software tools for the analysis of Internet domains that can be used to determine who are the likely owners or administrators of the pages on which these platforms are hosted. If these VASPs are based on the dark web, it is possible to exploit, for the purpose of identifying the owners, the fact that their success is based on reputation, which means that there is an enormous amount of potentially valuable information about them in specialized forums and pages.

250. Notwithstanding the above, it should also be borne in mind that the standards established by the FATF on the subject do not require the exchange of VAs to be channeled through VASPs. "Peer-to-peer" transactions, without intermediaries, between holders of wallets that are not in custody are not covered by the AML/CFT regulations recommended by said organization.

251. Several P2P platforms can be found on the Internet, such as LocalBitcoins, LocalCryptos, Local.Bitcoin.com, and Ccoins.io, among others, whose service is limited to connecting buyers and sellers with each other for the exchange of cryptocurrencies—either among themselves or with fiat currency—, without establishing payment mechanisms within the page or storing fiat money of its users. Some of these platforms only allow the exchange between VAs, but not their conversion to fiat money, such as Binance, Poloniex, Bittrex, Crypto Exchange, KuCoin, Changelly, ShapeShift, and PrimeXBT, among others. Some of these offer the possibility of carrying out CoinJoin or "Chain Hopping" maneuvers.

252. Although the use of these sites could be used to carry out transactions with VAs while avoiding AML/CFT controls (where they have been implemented), their use has not yet become widespread. At present, VASPs continue to offer an easier and safer service to people wishing to trade cryptocurrencies, regardless of their origin (legal or illegal). The relative difficulty in carrying out P2P transactions functions, for the time being, as a limiting factor to their volume. However, if carrying out this type of operation without intermediaries were to become simpler and safer, this could lead to an increase in the number and value of transactions not subject to AML/CFT controls and represent a vulnerability that must be addressed.[111]

253. Another point of exchange between VAs and fiat currency are the cryptocurrency kiosks or "Bitcoin ATMs" that have begun to appear in cities in many parts of the world, including Latin

[110] Refer to: FANUSIE, Yaya J. / ROBINSON, Tom: "Bitcoin laundering: An analysis of illicit flows into digital currency services", Elliptic Center on Sanctions & Illicit Finance, January 2018, p. 8.
[111] Refer to: FATF: "FATF report to the G20 Ministers and Central Bank governors on the so-called stablecoins," June 2020, p. 8 § 32.

America. In these ATMs, it is possible to exchange, buy or sell cryptocurrencies (especially, but not exclusively, Bitcoins), although for a commission that is generally higher than in online exchange platforms. Although the companies operating these ATMs fall under the FATF definition of VASPs, the fact is that, even in countries where their activity is regulated, most of these ATMs require only a limited amount of identifying information from their customers to carry out transactions, and in many cases the operators cannot guarantee that the documentation they receive is authentic or that the user is not acting on behalf of a third party.[112]

254. Notwithstanding the above, the regular use of VA ATMs by persons under investigation may offer advantages for the investigation, since it constitutes a starting point for possible surveillance or follow-up tasks. In this regard, if it is known that these persons operate in certain places and use VA ATMs to carry out their illicit activity, it is possible to identify the ATMs located in the area through pages such as CoinATMradar[113] and establish surveillance points in order to determine the dates and times when they are used by the suspects. This can be used to request or obtain the information corresponding to the transactions carried out on that date and time (addresses used, type of VA involved, transaction amounts, etc.), or to track their subsequent movements in order to identify their potential partners or accomplices.

C. Investigative techniques based on Blockchain analysis

281. In addition to the information that can be obtained from VASPs, it is also possible to extract data of great relevance for asset investigations from the very structure underlying the operation of VAs. As explained above, the transactions of Bitcoin and most cryptocurrencies are based on the existence of a public registry—called Blockchain—in which they are confirmed and recorded (in chronological order) in order to guarantee the integrity of the system.

282. The operation of the transfer and registration process is similar with respect to most known VAs, with the exception of some "private currencies." Transactions are initiated when the seller transfers a certain amount of cryptocurrencies from his/her wallet to the buyer's VA address, which represents the buyer's wallet. When the transaction is validated by entering the seller's private key, the network acknowledges the sending of information and the network's "miners" process the transaction and add the value of the transaction to the end of a computer data chain representing previous transactions. The "miners" then add a block containing the latest transactions transmitted to the network following the last completed block, at a rate of approximately one block every ten minutes.[114] The resulting succession of blocks makes up the "blockchain."

[112] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 40 § 133.
[113] https://coinatmradar.com/.
[114] Refer to: BRYANS, Danton: "Bitcoin money laundering: Mining for an effective solution," Indiana Law Journal, Vol. 89, 2014, p. 446.

283. The Blockchain records all transactions carried out by the holder of a given VA wallet, in chronological order. For each transaction, the transaction ID (hash value), the date and time of the transaction, the source and destination address (there may be one or more source addresses and one or more destination addresses for each transaction), the amount transferred, the cost of the transaction (i.e., the commission charged by the miners who processed it) and the remaining balance (i.e., how many bitcoins are left for the sender and how many for the receiver at the end of the transaction) are recorded.

284. The following image[115] illustrates how a transaction is reflected in the Bitcoin Blockchain. It shows the hash (the transaction ID), the date and time of the transaction, the sender's address, the amount of bitcoins transferred, the receiver's address and the resulting balance. The "fee" section represents the commission assigned to the "miners" for processing the transaction, which, as can be seen, has not yet been confirmed.

285. All this information is public, and can be consulted on many different websites, such as (with respect to Bitcoin) https://explorer.bitcoin.com/btc. On the Blockchain it is also possible to consult the balance of each VA address, in which the complete history of transactions, the total sent and received, and the resulting balance are recorded.

286. From the data recorded in the Blockchain, investigative agencies can learn the complete transaction history of a given VA address, including the addresses of all the users with whom it carried out transactions and the date, time, and exact amount transferred (which can be useful as a search criterion when analyzing many transactions simultaneously); as well as the complete chain of transactions made by each VA since its creation and the IP addresses associated with each VA address (unless the user connects to the network through an anonymity tool such as a VPN or TOR system). The analysis of this dataset, and its cross-checking with information obtained from other sources (especially if carried out by means of "Big data" IT tools) can be crucial to detect criminal activity with VAs, identify its perpetrators and obtain incriminating evidence.

287. For this reason, the analysis and tracing of transactions with VAs aimed at linking suspected persons with specific VA addresses or wallets should become a routine task in the framework of investigations on ML/TF schemes with VAs.[116] To this end, Blockchain analysis constitutes an

[115] Source: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 13.
[116] Refer to: INTERPOL / Basel Institute on Governance / EUROPOL: "Recommendations. 4th Global Conference on Criminal Finances and Cryptocurrencies," November 2020, p. 3.

essential investigative tool, both to obtain evidence that serves to connect the persons under investigation with criminal activities or illicit proceeds,[117] and to seek the seizure and confiscation of such proceeds. A recent case illustrates the importance of this tool:[118]

Case 3: Confiscation of Bitcoins stolen from Silk Road from Blockchain analysis:
In November 2020, the U.S. government filed a motion to confiscate approximately 69,370 Bitcoins (BTC), Bitcoin Gold (BTG), Bitcoin SV (BSV) and Bitcoin Cash (BCH) valued at USD 1 billion.
These VAs had previously been seized as part of an investigation that traced the destination of bitcoins once belonging to the defunct Silk Road virtual marketplace that had been appropriated by an individual who managed to hack into the marketplace's website, obtain the passwords, and transfer the cryptocurrency to an account of his own whose address was 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbh (hereinafter, 1HQ3).
In 2020, with the assistance of a company specializing in Blockchain analysis, 54 transfers made in early 2013 from Silk Road accounts to two Bitcoin addresses were detected: 1BADznNF3W1gi47R65MQs754KB7zTaGuYZ and 1BBqjKsYuLEUE9Y5WzdbzCtYzCiQgHqtPN totaling 70,411.46 BTC (valued at approximately USD 354,000 at the time of transfer). The assets had been transferred in round amounts and in a short space of time. Thus, 10 of the transactions had taken place at 3:59, all for exactly 2,500 BTC, a pattern that is unusual for Bitcoin users. These transactions had not been recorded in the Silk Road database as withdrawals by sellers or employees, so it was inferred that they were assets stolen from the site.
On April 9, 2013, from the two addresses that had received a total of 70,411.46 BTC, just over 69,471 BTC (valued at that time at USD 14 million) were transferred to the address 1HQ3. Then, on April 23, from the latter address 101 BTC (approximately USD 23,000) were wired to BTC-e, an unregistered VA exchange platform. Between April 2015 and November 2020, the remaining just over 69,370 BTC remained at 1HQ3. During that time frame, a portion of the VAs were converted to BCH, BTG, and BSV. An analysis of the Blockchains of each of the variants determined that the funds remained in 1HQ3.
In November 2020, U.S. authorities identified the individual responsible for the theft of the Silk Road bitcoins, and he entered into an agreement whereby he consented to the seizure of the VAs by the U.S. government.

288. The asset investigation is facilitated in cases where it is possible to trace the movements of VAs from and to a known VASP, especially if it is one that, because it is located in a jurisdiction where its operation is regulated, is subject to AML/CFT obligations. To this end, when—by any method—it is possible to identify the VA address(es) used by the person under investigation, the information recorded in the Blockchain can be used to determine whether he/she has operated with any VASP, and then require those responsible for the latter to provide the data associated with the address(es) obtained through CDD tasks. Another recent case illustrates the usefulness of this investigative strategy:[119]

[117] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 25 § 78.
[118] Source: Department of Justice (DOJ) of the USA.
[119] Source: Department of Justice (DOJ) of the USA.

Case 4: Welcome to video. Tracking of Bitcoin transactions to identify customers of a page dedicated to the exchange of child sexual exploitation images:
A joint operation between authorities in South Korea, the U.S. and eleven other countries led to the identification and arrest of 337 users of the "Welcome to video" (WTV) site, which operated on the Dark Web and was dedicated to the exchange of child sexual exploitation images.
After identifying and arresting the site's administrator in South Korea in early 2018, investigators sent small amounts of bitcoins to the Bitcoin wallets that the site assigned to users. From there, VA movements from each of those wallets were tracked through Blockchain analysis, which allowed them to be connected to the addresses of US-based VA exchange platforms (subject to AML/CFT obligations). With the data provided by those responsible for such platforms in compliance with court orders, it was possible to identify and arrest the users who had resorted to those services for the exchange of VAs linked to WTV's operations.

289. The identification of the VA addresses of key players within the exchange networks of these assets is, therefore, a fundamental element for the "deanonymization" of specific users and the reconstruction of their contact networks. In view of this, it is important that the VA addresses of cryptocurrency exchange platforms, mixers, online gambling houses, illicit markets in the dark web, or of persons already identified as likely suspects of engaging in some illicit activity generating funds, or ML/TF, among others, that are identified in the course of investigations, are registered, ordered and cataloged to allow their subsequent use, both in the framework of the same investigation in which the identification was achieved and in other subsequent investigations. LEAs should have as broad a base as possible of VA addresses with identified holders, as this facilitates the use of the Blockchain to allow the identification of other users who have contact with them.[120]

290. VA users involved in illicit activities can also be identified through an analysis of the Blockchain focused on the patterns that emerge from their transaction history. This is so, since their activity generally differs from that of those engaged in licit activity. Thus, illegal users tend to carry out a greater number of transactions, but for smaller amounts. They are also more likely to carry out transactions with the same interlocutors. The reason for these differences in transactional behavior is that illicit users of VAs tend to use cryptocurrencies (almost) exclusively to facilitate the trafficking of illegal goods and services (or to recycle funds originating from such trafficking or from other crimes), while for licit users VAs are generally treated as an investment. Consequently, illicit users tend to hold on to VAs for less time, which is consistent with the intention of preventing their seizure by the authorities.[121]

[120] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 52 § 180.
[121] Refer to: 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, No. 5, 2019, pp. 1798/1853.

291. Similarly, a VA user is more likely to be involved in illicit activities if he/she uses "mixers" in his/her transactions or carries out the type of operations (such as CoinJoin or "chain hopping") aimed at preventing the reconstruction of the transfer chain. On a more general level, the web of transactions between illicit users tends to be considerably denser than those among licit users, with the different actors much more closely connected to each other through cross-transactions. This is consistent with the tendency of such users to use VAs primarily for trafficking in illicit goods and services and other criminal activities.

292. Based on this, within the framework of Blockchain analysis, different methods coexist to seek the deanonymization of VA users, always based on the data known and the exploitation of the inherent characteristics of the cryptocurrency ecosystem that facilitate the identification of those who operate in that area. These include:

- The tracking of transactions originating from the "hot wallets" (online) of the main illicit markets of the Dark Web, collecting the addresses of all customers and mining the resulting information.

- The segmentation ("Clustering") of users based on the differences—already outlined—between those who usually operate with funds of illicit origin and those who resort to VAs for licit purposes.

- Exploring the topology of the VA network to identify "communities" of users based on the transactions among them.

- The use of information contained in forums and other areas of the dark web on users of VAs involved in illegal operations, including addresses of VAs, pseudonyms or nicknames, references to their activity that may provide clues as to their location, etc.

293. The use of Blockchain analysis (or "Chain analysis") as an investigative technique requires the use of the appropriate technological tools, in addition to the necessary technical knowledge to use them. In terms of tools, at the primary level, a Blockchain explorer is used, which is a network application that operates as a sort of search engine in the VA ecosystem, making it possible to find addresses, transactions, and other data linked to them. Open-source versions of these applications are available for free download on the Internet.[122]

294. There are also more sophisticated computer resources, specifically designed for the needs of investigative agencies, in the hands of private companies specialized in Blockchain analysis such as Chainalysis, Elliptic, Ciphertrace, or Blockchain Intelligence Group, among others. The methods used by these companies allow mapping transactions made with bitcoins with up to 90%

[122] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 25 § 77.

effectiveness;[123] and tools have been developed for the analysis of the main Altcoins, such as Litecoin and Ethereum, which have similar characteristics to Bitcoin.[124] Moreover, the technological capabilities in the hands of these private companies may prove to be the only way to trace the destination of cryptocurrencies in cases of "chainhopping."

295. Although the use of Blockchain analysis techniques may seem to be a resource outside the scope of traditional investigative agencies, it constitutes a key element of any investigation linked to VAs.[125] For this purpose, if it is decided not to develop the necessary technological tools internally, public-private cooperation with companies specialized in Chain analysis (which, moreover, have extensive databases of VA addresses with already deanonymized holders) can be a good alternative, also recommended by agencies such as CARIN.

296. In the latter case, it is necessary that the LEAs or units of the Public Prosecutor's Office involved have agents or officials prepared to explain the findings of these companies in the framework of the judicial proceedings that take place in connection with the criminal behavior with VAs under investigation. In this regard, it is recommended that a good working relationship be maintained with the personnel of the companies providing the service, especially if they may be called upon to testify on how the findings presented were arrived at.[126]

D. Open-source intelligence and electronic surveillance techniques

297. The information that emerges from Blockchain analysis can be complemented with data or evidence from other sources, or obtained through the use of traditional investigative techniques, such as surveillance, monitoring, or the interrogation of witnesses or persons of interest. An effective way to exploit the profusion of digital data that characterizes modern societies is to resort to "open-source intelligence" (OSINT) techniques, a term that refers to the systematic collection, processing, and analysis of open access information. That is, information available to the general public without restrictions.[127]

298. With regard to asset investigations into illicit VA activities, OSINT can be used, for example, to obtain data on the holders of Bitcoin addresses or other Altcoins already known to the investigators. To this end, attempts can be made to place the VA address in Internet search engines, as it is quite common for individuals engaged in illicit online trading (or terrorist organizations seeking to raise funds through VAs) to post their address (associating it with their online profile and pseudonym) in forums (such as Reddit, 4Chan, 8Chan) or in the comments

[123] Refer to: DUPUIS, Daniel / GLEASON, Kimberley: "Money laundering with cryptocurrency: Open doors and the regulatory dialectic," Journal of Financial Crime, August 2020.
[124] Refer to: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 31.
[125] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 37 § 123.
[126] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 37 § 124.
[127] Refer to: MEDINA, Manuel: *"Inteligencia de fuente abierta"* [Open-source intelligence], Basel Institute of Governance, Quick Guide Series, No. 17, June 2020.

sections of specialized cryptocurrency or IT websites. In addition, websites specifically dedicated to the identification of Bitcoin users and the addresses associated with them, such as walletexplorer.com, can be consulted.

299. The same technique can be used to obtain information on the Dark Web, where there are multiple forums (Dread, Darknet Avengers, The Hub, Exploit.in) in which, taking advantage of the anonymity conferred by TOR login, people freely share information on hidden services, including their addresses, the products and services they offer, comments on the quality of the service, nicknames of the most (or least) successful traders, etc.

300. In this regard, it is important to bear in mind two issues. Firstly, the pseudonyms or names used online by persons who carry out their illicit activity in this area are rarely modified. This is because, on the one hand, the success of their commercial activity on the Internet is generally closely linked to their online reputation (i.e., to the comments made about them in virtual bazaars or forums). On the other hand, people who spend a large part of their lives on the Internet tend to develop a strong attachment to the pseudonyms that identify them on the Net, and are reluctant to stop using them, even when this would be advisable for reasons of operational security, as reflected in the following case:[128]

Case 5: Albert González. Online identity maintenance as a key element in linking an individual to illicit activity:
After being arrested in the framework of an investigation into the use of cloned debit cards, the American hacker Albert González began to work together with the US Secret Service, advising and training its agents on computer-related issues.
However, at the same time and unbeknown to the authorities, González organized a new group of hackers with which he carried out a series of major computer attacks on the systems of several U.S. companies, obtaining the private data of millions of credit card users, which he sold to buyers in Russia to be used in the development of twin cards.
González's involvement in the aforementioned illicit activity was discovered when his Russian buyer was arrested while trying to enter the U.S., when the analysis of his personal computer revealed that his accomplice's pseudonym was "Soup Nazi," precisely the same one that González had been using since before being apprehended for the first time, and which he maintained even in his interactions with Secret Service agents.

301. Secondly, it should be borne in mind that online pseudonyms often have a correlate either on the surface web (when the individual acts mostly on the dark web) or even in real life, which—if discovered—may allow linking the illicit activity to his or her real identity. In such a context, LEAs can take advantage of mistakes that people often make when splitting their online identity from

[128] Source: BLANCO, Hernán, *Tecnología informática e investigación criminal* [Informatic Technology and criminal investigation], La Ley, Buenos Aires, 2020, p. 233.

their real-life (secret) identity, such as not remembering to use anonymous surfing tools at some point, using the same VA address for illicit and licit activities, or using an e-mail address associated with their real name in connection with their online identity. This is illustrated in the case below:[129]

Case 6: Ross Ulbricht. Use of IRL identity mail for illicit activity:
As part of the investigation into the Silk Road online marketplace, the FBI was able to uncover the identity of its administrator, Ross Ulbricht, through a search of the surface web (not the Dark net). In the initial period of his criminal activity, Ulbricht made a mistake when he began advertising the online marketplace on a surface web forum dedicated to illicit drugs, under the alias "Altoid" (he would later go by the alias "Dread Pirate Roberts" in his role as Silk Road administrator). Months later, he appeared on another online forum with the same nickname—Altoid—requesting information about Bitcoin and asking other users to contact him at his email address, at which point he provided his personal email address. It was this mistake that subsequently allowed Silk Road to be linked to the nickname "Altoid" and then the latter to Ulbricht's personal email address, through which the FBI was able to ascertain his true identity.

302. For the same reasons, OSINT techniques can also be effective in obtaining information on unregistered VASPs providing services to persons engaged in illicit conduct with VAs, including mixers or P2P cryptocurrency exchange platforms, whether on the surface web or on the dark web. This is so, since these are run on the same reputation-based system as illegal online marketplaces, dependent on feedback from market participants in the feedback window or on specialized forums, where other users are alerted about the quality of the service, whether it is still online or down, whether it is fraudulent, etc. In such a context, investigators can anonymously access these forums or pages (just like any other Net user) and obtain useful data on illegal or unregistered VASPs operating in a given country (or providing services to persons from that country) and, on that basis, try to identify those who may be operating with the person(s) under investigation.

303. In addition, OSINT techniques can be applied to link persons suspected of being involved in illicit conduct generating funds with the suspected launderers of such funds. Indeed, even if communications between the two parties are carried out exclusively in cyberspace and through anonymity tools, it is likely that there is data that can be used as evidence of the existence of a relationship between them. This, since it is improbable that a person engaged in a criminal activity would entrust the control of his/her earnings to a launderer, in the absence of a prior bond of trust or any circumstance that would justify the delivery of the funds to a third party.

304. Finally, open-source information may be useful to better understand the lifestyle, the assets of the suspect, or the places where he/she resides or carries out his/her commercial or social activity. This, bearing in mind that sometimes even the most capable criminals (or their family or friends) can reveal compromising information through posts on social media such as Facebook, Instagram, Twitter, TikTok, etc.

[129] Source: Regional Organized Crime Information Center (ROCIC): "Penetrating the Darknet. Silk Road, bitcoins, and The Onion Router," 2013.

305. Also, with respect to this information, it is important to keep in mind that in every application there are at least two layers of data that can be exploited for an investigation. First, the content layer, which includes the information "published" by the user (messages, photos, videos, etc.). In this regard, the images posted can provide a lot of data about a person, not only about their physical appearance, but also about their environment, location, status, ideology, etc. Especially when images are "tagged," associating them to profiles of users of the social media network or even to people who have not logged in to the service).

306. Below the first layer, there is a second layer made up of metadata, which can provide information about the computer through which the content was published, the users themselves, or a description of the files. A typical example of this last type of metadata is given by the EXIF data ("Exchangeable image file format") contained in the videos or images, which describe the equipment and settings with which the video or image was obtained. Depending on the equipment used, the image or video metadata may also include information about the date, time and location in which it was created. This data can create opportunities to obtain clues or draw conclusions about individuals or organizations associated with those files or the social media accounts on which they were posted. Even seemingly innocuous aspects such as SSL ("Secure Sockets Layer") certificates on web pages can provide information about the site owner.

307. The advantage of using OSINT as an investigative tool is that—especially compared to Blockchain analysis—it does not require advanced technical knowledge, which means that the use of this resource is not limited to cybercrime specialists. On the contrary, all investigators should be able to search open sources and collect publicly available information.[130]

308. In addition, a variety of technological tools have been developed in order to make the search process easier and automatic, such as Maltego or Spokeo, among others. There are also a number of purpose-specific search engines on the Web, such as Shodan, which helps locate various technologies including webcams, printers, VoIP devices, and routers, among others; NameCHK, which is a tool for checking whether a user name is available on a variety of online services; Tineye, a reverse image search service (an image is added and it shows whether the image is found somewhere on the Internet); and Pipl, which searches for matches on the Internet based on different criteria such as names, email addresses or telephone numbers. There are also pages on the surface web that provide information about the nature and status (online or offline) of hidden services or pages on the Darknet and its mirrors, such as Dark.fail or the TNO Dark Web Monitor. Other tools, such as GitHub, can be used to perform OSINT tasks on the Darknet.

309. In addition, the Basel Institute has developed a proprietary tool to streamline the search process called "Basel Open Intelligence," which performs automated searches of a person's or

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

organization's name, combined with more than 200 keywords on financial crimes, prosecutions, other crimes, and customized keyword lists. It also searches the Dark Web, selecting any references on sanctions lists and politically exposed persons. The tool can conduct searches in multiple languages and offers its users the option to automatically translate articles into their language to facilitate analysis. Documents found in the search are listed along with the main text extracted from the website, excluding irrelevant content (such as advertising, menus, or cookie notices) and highlighting keywords for easier reading.[131]

310. In addition to the data collected by the investigative agencies themselves using OSINT techniques, already processed information on persons of interest can be obtained by using the services of so-called "data brokers." These companies are engaged in the collection and processing of information from multiple sources and the elaboration of detailed personal profiles,[132] which include data such as age, gender, education, employment, and residential history, relationships, number of children, purchases, activities, use of social media, political opinions, race and religion, income, vehicle and property ownership, details of banking and insurance products purchased, credit card purchases in the last 24 months, socioeconomic status, economic stability, etc.

311. OSINT techniques are most effective when combined with the use of traditional investigative measures such as physical surveillance or monitoring, inspection of waste discarded by the persons of interest, requests for reports, production orders and/or personal or house searches, obtaining witness statements, etc. Many successful asset investigations are based on the effective combination of these traditional practices with more sophisticated techniques, typical of an investigation that is totally or partially linked to activities developed in the online environment. The following cases exemplify the usefulness of adopting this strategy:[133]

Case 7: Investigation with combined techniques:
In 2017, following the arrest of a drug trafficker operating on the Darknet, an investigation involving the cyber customs unit of the French police was launched following the discovery of a user profile and VA address on an online forum of that network. Various methodologies were used, including the action of undercover online agents; the tracing of transactions on the Blockchain in order to reconstruct the network of contacts between cryptocurrency exchange platforms, online marketplaces and mixers, and list the transactions made between these; production orders were issued to obtain and analyze data; requests for information were issued to VA exchange platforms and wallet service providers about online pseudonyms and transactions associated with them; and test purchases were made. Although the investigation was mostly focused on bitcoins, the target also conducted transactions with Bitcoin Cash, Ethereum, Monero, Ripple, Litecoin, and Zcash. The funds involved were estimated at approximately EUR 700,000 over a period of 9 months.

[131] Refer to: MEDINA, Manuel: *"Inteligencia de fuente abierta"* [Open-source intelligence], Basel Institute of Governance, Quick Guide Series, No. 17, June 2020.
[132] For instance: Equifax, Acxiom, Experian, Epsilon, CoreLogic, Datalogix, Intelius, PeekYou, Exactis, and Recorded Future, among others.
[133] Source: FATF: "Guidance on financial investigations involving virtual assets," June 2019, pp. 55/56, § 190 and Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations," 2018, p. 48.

Case 8. "Pedro el grande." Combination of traditional and online techniques.
In February 2017, 18-year-old Aisha Zughbieh-Collins was found lifeless in her apartment from an overdose of the synthetic opioid U-47700 (U4). The victim's mother, suspecting that she had purchased the drug on the Internet, provided detectives with her email address. In addition, evidence was found at the crime scene indicating that the drug had been sent through the mail, concealed in a specific variant of a pregnancy test sold at the Dollar Tree Store pharmacy chain. Although the return address was determined to be false, it was possible to establish from which post office the packaging had been purchased.
The most relevant finding, however, was a notebook in which an alphanumeric code had been written down, which turned out to be the victim's private cryptographic key for Pretty Good Privacy (PGP) communications encryption software. By accessing the victim's email with the code, investigators were able to discover that he had purchased the drugs on a virtual marketplace on the Dark Web from a seller nicknamed "Pedro el grande," who, as indicated on the page itself, had made more than 10,000 transactions.
Investigators made a controlled purchase of U4 from "Pedro el grande," which they received concealed in the same type of pregnancy test found in the victim's apartment. It was determined that these tests had been purchased through an online sales company that only accepted Bitcoin payments, and was linked to two email addresses, the holder of which was identified as Theodore Khleborod, domiciled in Greenville. Investigators were able to determine that Khleborod had received numerous international shipments from China (one of the countries where the drug U4 is manufactured). Also, through analysis of the named individual's social media posts, it was established that he was in a relationship with a woman named Ana Barrero.
Inquiries in the town of Greenville revealed an increase in sales of pregnancy tests at a specific Dollar Tree Store chain store. Footage from the store's video cameras showed that Ana Barrero had made multiple purchases of pregnancy tests at that store. While surveilling the homes of Khleborod and Barrero, investigators witnessed Barrero send numerous packages similar to the one found in the victim's apartment. They were both arrested.

312. In turn, technological advances in recent years have led to traditional measures such as surveillance or tracking with electronic devices that increase their effectiveness, lower their costs, and considerably broaden their scope. In addition to providing useful information or evidence for any investigation into organized crime—such as the identification of other individuals associated with suspects, the reconstruction of links and activities, the discovery of the possible location of assets or property information of interest, etc.—the use of electronic means of surveillance can also serve to ascertain relevant data for investigations into illicit conduct involving VAs, such as connections with cryptocurrency exchange platforms, mixers, online gambling sites, P2P networks dedicated to the transfer of VAs, or cloud storage services. Likewise, the type of computing devices used by the persons under investigation, whether they have one or more online wallets, the preferred methods of communication or whether they use public Wi-Fi connections or other electronic means that can be accessed by the authorities can also be ascertained in this way.[134]

313. To this end, an effective method is the monitoring of the Internet traffic of the persons under investigation.[135] In this regard, it should be noted that this monitoring includes much more than the capture of e-mail exchanges. This is because, in fact, only a small part of Internet traffic comprises "human-to-human" communications such as e-mails. Most Internet communications are

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

between humans and computers, such as World Wide Web (WWW) pages in transit, commands sent to remote servers, and file transfers. Many others involve communications between computers, such as the administrative network traffic that keeps the Internet running. These communications can also provide relevant information, which can be captured in many different formats: large digital documents, images, audio files, videos, and even telephone communications over the Web.

314. It is also important to bear in mind that Internet monitoring, by its very nature, always involves the analysis of all the data traffic flowing through the specific point of the network where the interception takes place, in order to identify, among all of them, those that are of interest to the investigation (just like a policeman who wants to find a suspicious individual in a crowd and must observe, in order to identify him/her, all the people who are there). In this context, this measure requires computer tools specially designed to filter the data, so as to capture only those whose collection is covered by the corresponding judicial authorization.

315. In many cases, the monitoring of network traffic will not allow access to the content of Internet communications, since it is increasingly common for these to be encrypted. In general, however, it will be possible to capture the so-called "wrapper data," i.e. all those that do not form part of the content of the communication, but refer to the mechanisms for its execution (source and destination IP addresses, data volume, Internet nodes involved in the exchange of data packets, etc.).[136] This is unless one of the parties to the communication has resorted to an anonymity tool (such as the TOR system or a VPN) to mask its real IP address.

316. Moreover, modern technologies also facilitate the tracking of individuals, since it is no longer necessary to involve multiple agents and vehicles to physically follow the persons under investigation, but the measure can be carried out by means of GPS devices that allow the simultaneous tracking of several persons, for many days and at a considerably lower cost. In turn, the proliferation of the use of mobile applications on "smart phones" (for navigation, social media, online shopping or banking, etc.), in many cases associated with GPS embedded in the cell phones themselves, offers another means for prospective—or even retrospective— tracking of persons under investigation.[137]

317. Indeed, the very design of cell phone communication networks (3G or 4G) implies constant contact between the devices and the cell phone towers to allow the background operation of network applications, regardless of whether or not the user is using the cell phone to communicate. Each of these contacts between the cell phone and the towers generates a record that is stored by the telephone company, which includes the date and time and the specific cell with which the

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

connection was established. These snippets of information, called "Cell site location information" (CSLI), are extremely useful, as they not only allow us to locate the person at a specific place at a specific time, but also to reconstruct the history of their movements over days or even months.

E. Relevant evidence or clues in the computer systems of persons of interest

318. When—as is the case with the conducts referred to in this guide—the object of an investigation refers to illicit activities carried out in cyberspace or by means of computer equipment (including modern smartphones, which are, in essence, portable computers), the devices that store digital information become a fundamental reservoir, either of evidence or of data relevant to the progress of the investigation. Among the elements that can be obtained there are the following:

- Evidence or indications of VAs use.
- Evidence or indications of contacts with cryptocurrency exchange platforms (either VASP or P2P platforms), mixers, online gambling sites, etc.
- Evidence or indications of use of cloud storage services.
- Evidence or indications of the use of anonymity tools (TOR, I2P, VPNs).
- Evidence or indications of the use of encryption tools.
- Keys or passwords to access information stored in the cloud or to disable encryption.
- Evidence or indications of communications with other suspicious persons (holders of funds of illicit origin, terrorist organizations, money launderers, etc.).
- Property documentation or other relevant evidence in digital format (company incorporation documents, accounting records, images or data on assets, agendas, etc.).

319. This digital information or evidence can be found on an increasingly wide range of technological devices, including desktop computers, laptops, tablets, smartphones, smart readers (such as Kindle), portable GPS equipment, digital cameras, flash drives, SD cards, pen drives, removable hard disks, external "cloud" servers (such as Dropbox, Google Drive, Box. Net, Amazon Cloud Drive) and compact discs (CDs, DVDs, Blurays); as well as smart devices within the so-called "Internet of Things" (IoT).[138] Therefore, as far as possible, a thorough forensic analysis of all electronic devices confiscated from the persons under investigation should be carried out.[139]

[138] Refer to: 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, p. 4.
[139] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 15 § 35.

320. There are several elements that, if found on computer equipment, would indicate that its owner uses or has used VAs. Firstly, the existence of a cryptocurrency wallet. For the main cryptocurrency, Bitcoin, the original wallet is Bitcoin Core, which groups together the vast majority of Bitcoin nodes. One of the main differences between this application and other similar ones is that Bitcoin Core downloads the complete Blockchain to the user's computer, which takes up quite a lot of space (more than 300 GB).[140] Other VAs wallets commonly used on desktop computers include Exodus, mSIGNA, Electrum, Mycelium, Bitcoin Core, Green Address, MultiBit HD, Armory, Copay, and Jaxx. Currently, most wallets are so-called "HD wallets" ("Hierarchical deterministic wallets"), in which all keys are derived from a single master key, known as the "seed."

321. The files containing the wallets are usually identified as wallet.dat. They are in turn represented by identifying icons, as illustrated in the following image, which reproduces those of some of the most popular virtual wallets:

322. VA addresses eventually discovered in the wallets in control of suspicious persons may be subject to Blockchain analysis in order to reconstruct their transfer history, and the addresses of other users with whom they have been linked.

323. The existence of software corresponding to Massively Multiplayer Online Role-Playing Video Games (MMORPGs) may also indicate the use of VAs, since these programs offer virtual assets that can be acquired to interact within the game, such as Second Life Linden Dollars, Project Entropia Dollars, or World-of-Warcraft Gold.[141]

[140] Refer to: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe. February 2021, p. 26.
[141] Refer to: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014, p. 102.

324. Another source of potentially valuable information is found in the browsing history of computers or smartphones, which may reveal contacts with VASPs, or cryptocurrency P2P exchange platforms. The presence of applications such as "Portfolio trackers" (which offer updated information on the price of different cryptocurrencies) also indicate the use of VAs, as well as the record of visits to discussion forums or pages with information on cryptocurrencies.[142]

325. In the case of cell phones, it can be verified whether they contain applications for two-factor authentication linked to online wallets, whether in custody or not. Similarly, the possible use of cloud storage services should also be verified. In this regard, it is worth bearing in mind that VAs do not necessarily have to be on the personal computer or cell phone of the person under investigation, since the wallets—except for the aforementioned Bitcoin Core—generally take up little space (less than 100 bytes) and can be stored on any device, as well as on external servers. Web-based email services can also be used, some of which offer privacy features as an additional service.[143] Cloud storage can be inferred both from the presence of software associated with such services and from records in the browsing history reflecting the use of such services.

326. In addition, the devices of the persons under investigation may contain keys or passwords that allow access to password-protected desktop or mobile VA wallets; to "custodial" online wallets hosted on pages that offer this service; to external servers of cloud data storage companies; or to encrypted documents found in the computer equipment of such persons or in any data storage device that supports the use of such tools. Passwords can be found in:

- Text files such as Word or Notepad, spreadsheets such as Excel or even as images.
- Applications for computers or smartphones that manage user passwords, which are usually also accessed through a password, which can be biometric (fingerprint or facial recognition).
- In some browsers, which also offer the possibility of storing passwords associated with access to web pages (such as those that host "custodial" wallets or provide cloud computing services).[144]

327. Finally, the finding of elements that indicate the use of anonymity tools, although it does not constitute, by itself, evidence of criminal activity, may be relevant if it is suspected that the person under investigation uses such tools to carry out money laundering activities involving VAs.

[142] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 18. § 51.
[143] Refer to: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014, pp. 102/103.
[144] Refer to: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014, pp. 103/104.

In this regard, it is necessary to pay attention to the possible discovery of different programs,[145] namely:

- Browsers for the dark web, such as the TOR system, which are used to access hidden services on the dark web such as illicit online marketplaces, where VAs are the only accepted payment currency. These programs can be found not only in desktop (for computers) or mobile (for smartphones) versions, but also in devices—such as Tails—where the browser is hosted on a USB that is connected to the computer when you want to browse anonymously and is removed at the end of the session, leaving no trace of its use on the computer. Below are the browser icons of the TOR and I2P systems:

NAVEGADOR TOR

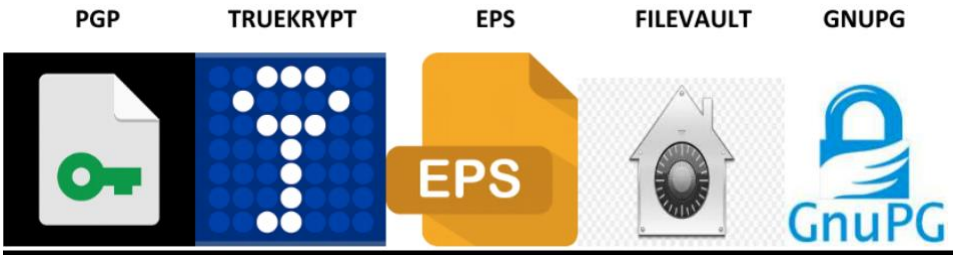
12P

- Presence or use of programs for browsing through virtual private networks (VPNs).

- Presence or use of "virtual machine" programs such as VMware Workstation, OrAOPe VM VirtualBox, QEMU, Parallels Desktop, VMware Fusion, or Microsoft Virtual PC, which allow the user to host a second operating system (called "guest") within his/her main operating system ("host"). Many of these "virtual machines" allow the entire content to be encrypted, so that it cannot be executed without entering the password. Thus, illicit activity with VAs can be carried out entirely through this "virtual machine," without any evidence of it on the "host" operating system, and keeping the evidence encrypted on the parallel operating system ("guest").

- Presence or use of encryption technology such as Pretty Good Privacy (PGP) or other similar programs (such as EFS, FileVault, Utimaco, GnuPG, and TrueCrypt, whose icons are reproduced below), which is often used by those who carry out illicit conducts on the dark web to communicate with each other or to safeguard potentially incriminating information.

[145] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, pp. 17/18, §§ 50/51.



- Presence of applications to erase file metadata.

- Browsing history including searches for information related to browsing the dark web, or tutorials for the use of some of the programs mentioned above.

F. Special investigative techniques

328. Notwithstanding the above, in cases where crypto-laundering schemes using VAs are particularly sophisticated, a possible alternative for obtaining information or evidence that would not otherwise be available is to resort to special investigative techniques such as undercover actions, always within the framework of what is permitted by the procedural legislation in force in each country.

329. In this regard, the FATF[146] emphasizes that the same programs and evasive techniques used by criminals to anonymously carry out their criminal activities in cyberspace can be used by the LEAs to infiltrate criminal organizations on the Internet and promote greater effectiveness in the development of asset investigations on ML/TF schemes with VAs. Indeed, the possibility of surfing anonymously on the Internet through tools such as TOR or VPNs, as well as the common use of "alternative identities" in cyberspace, facilitates the use of "digital undercover agents" to interact on the Internet with persons under investigation and/or potential criminals, infiltrate organizations, and gather evidence that can be used to obtain a conviction.

330. The advantage of undercover operations in cyberspace, compared to those traditionally conducted in the physical world, is that they require far less planning, development, and coordination efforts, while significantly reducing the risks to undercover agents. However, it is important to bear in mind that Blockchain analysis tools can also be used by criminals, which is why if an agent is going to act undercover on the Internet carrying out transactions with VAs, it is important that a transaction history be generated beforehand that is related to the "profile" that he/she will represent on the Net.

331. Anonymity tools are not the only programs commonly used by criminals that can also be of use to investigative agencies. In recent years, the use of spyware or Trojans for investigative

[146] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, pp. 23/25, §§ 71/76.

purposes has become more widespread. These can be used to realize various measures useful for investigations. Namely:

- To remotely access information or digital evidence whose physical location is unknown or impossible to access effectively (e.g., because access could not be achieved before the data is destroyed or altered by the persons under investigation). For this purpose, the spyware is introduced into the suspect's system and programmed to select the relevant data and send it to a computer controlled by the intervening authority.

- To obtain the passwords needed to access the contents of encrypted documents or information stored on external servers. For this purpose, a "keylogger" program is used, which records everything typed by the device user in which the spyware is introduced (including the passwords to be obtained), as occurred in the following case:[147]

Case 9: Nicodemo Scarfo. Use of spyware to obtain the password to an encrypted file:
As part of the ongoing U.S. investigation into two alleged New Jersey mob bosses, Frank Paolercio and Nicodemo Scarfo Jr, the FBI searched the latter's office. Upon searching his computer, they discovered a file protected with Pretty Good Privacy (PGP) encryption software, the contents of which they were unable to access.
Suspecting that the file might contain relevant evidence, the agency obtained a new court order authorizing it to physically install a keylogger on Scarfo's computer for one month.
At the end of that period, the FBI searched the office again and seized the computer. From the analysis of the information collected by the keylogger program, which had recorded everything typed by the computer's users, the agency was able to obtain the password to access the contents of the encrypted file, which included evidence of the illegal activity of Scarfo and his partner and led to their conviction.

- To monitor communications made over the Internet, using communication technologies that make interception by traditional means (VoIP or encrypted messaging systems) impossible. In these cases, the spyware captures the data packets in which the content of the communication is transmitted (in text, audio or video format) not when they are "in transit" on the Internet (since they will usually be encrypted), but just before the information goes out, or just after it enters the device in which the spyware was introduced. This is illustrated in the case below:[148]

[147] Source: CARRELL, Nathan E.: "Spying on the mob: United States v. Scarfo – A constitutional analysis," Journal of Law, Technology & Policy," Vol. 2002, No. 1, 2002, pp. 193/214.
[148] Source: Europol.

Case 10: Encrochat. Use of "supply chain attack" for mass infiltration of encrypted cell phone users:
In the context of a three-year operation by French and Dutch authorities regarding the Encrochat network, used by major criminal organizations in Europe to communicate via fully encrypted modified cell phones, the French justice system authorized the implantation of a computer virus on the company's servers, located in the city of Lille, which was then downloaded on all the devices in the hands of users (more than 60,000) by instrumentalizing updates sent by the company itself (hence the name "supply chain attack").
Once installed on the devices, the spyware sent to the investigation agency's headquarters all the information stored on the cell phones (corresponding to the previous two weeks), as well as the messages exchanged thereafter. Investigators were thus able to analyze more than one million messages, which in turn led—in the Netherlands alone—to the arrest of more than 100 people, the seizure of 8 tons of cocaine, 1,200 kilograms of methamphetamine, and almost EUR 20 million in cash and the dismantling of more than 19 synthetic drug laboratories, as well as preventing the commission of homicides and other serious crimes.

- To conduct acoustic or audiovisual surveillance, using the spyware to remotely enable the microphones or cameras of devices held by (or in the vicinity of) the persons under investigation.

- To locate or track in real time the persons under investigation, either by programming the spyware to remotely turn on the GPS embedded in the devices (e.g. cell phones) carried by the persons under investigation; or, by hacking into the computer of the person under investigation, to detect and transmit to the investigators the real IP address assigned to the equipment he/she uses to surf the Internet. An example of the latter is illustrated in the following case:[149]

Case 11: Playpen. Use of "watering hole attack" for infiltration of multiple suspicious persons:
In 2014, the FBI located in the state of Florida the servers of the "Playpen" page, located on the Dark Web, dedicated to the distribution of child sexual exploitation images.
In order to identify the users who downloaded or uploaded illicit images (whose IP addresses could not be known due to the use of the TOR system to connect to the page), the referred agency obtained judicial authorization to take control and operate Playpen for a month, as well as to introduce in it a spyware program designed to enter the users' computer every time one of them uploaded or downloaded files containing images of child sexual exploitation, and send from there information including the real IP address, the characteristics of the equipment in which it had been introduced, and its geographic location. Based on this information, the FBI obtained search warrants in more than 40 districts in that country, where they seized the computers of Playpen users, which stored files containing evidence of possession and distribution of child sexual exploitation images.

332. Although in the cases described above, the use of spyware by law enforcement agencies occurred in cases involving traditional cybercrimes such as the distribution of images of child

[149] Source: HENNESSEY, Susan: "The elephant in the room: Addressing child exploitation and going dark," Hoover Institution, Stanford University, Aegis Paper Series, No. 1701, 2017.

sexual exploitation or cases related to organized crime, there are also examples of the use of this tool—combined with other measures—in the framework of investigations related to ML schemes involving VAs:[150]

> **Case 12: Mixer Case (Netherlands) Spyware VA investigation?**
> The case focused on the activity of a person acting as a facilitator for criminals in VA markets, advertising services consisting of providing assistance in circumventing know-your-customer policies through the use of mixers (in particular Bitcoin, Bitcoin Cash, and Litecoin). The target claimed to operate from Curacao, with an approximate turnover of USD 200 million (approximately 25,000 bitcoins). However, his operational infrastructure was located in Europe.
>
> During the course of the investigation, standard methods (such as the requesting of asset information or conducting interviews, interception of communications, and the seizure of hardware and other IT infrastructure) were combined with more advanced methods, such as the use of "digital intrusion" techniques.

333. It is likely that state use of spyware is considered as a resource outside the activity of traditional investigative agencies, reserved only to specialized units/in cybersecurity issues; or too controversial to be accepted by the courts. The truth is, however, that in view of the availability of advanced technological tools to act anonymously on the Internet and/or anti-forensic techniques to prevent the collection of digital evidence, it is imperative that the LEAs adapt their strategies and methods to sustain the effectiveness of asset investigations.[151] Such was the recommendation of the International Association of Chiefs of Police (IACP)[152] in the framework of the summit held in 2015 on the influence of new technologies in criminal investigation.[153]

334. The concrete implementation of the state use of programs requires three stages: first, analyzing the use that the person under investigation makes of the networks, to determine which platforms or applications he/she uses (and the possible vulnerabilities of such platforms or applications, which can be exploited to enter the system); second, compromising the platform to introduce the most appropriate "exploit;" and third, monitoring the information captured from the target.

335. The initial recognition stage is essential, since computer intrusion tools are designed to work with respect to specific versions of a given application or operating system. This is done by means of a variant of OSINT techniques (known as "OS fingerprinting") aimed at collecting and analyzing the public information exposed by the systems when connecting to a controlled server (operating system, version, browser, installed plugins, installed fonts, screen resolution, among

[150] Source: FATF: "Guidance on financial investigations involving virtual assets," June 2019, pp. 57/58, §§ 198/200.
[151] In this regard, refer to the statements by the Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations," 2018, p. 47.
[152] It is the world's leading organization of police chiefs, with more than 23,000 members in over 100 countries.
[153] Refer to: 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.

others). The technique consists of grouping this set of data, generating a "fingerprint" of the user, which can be useful for identification purposes. The last phase of this recognition stage consists of analyzing the target's system to discover vulnerabilities and establish what defensive means it has (firewall, antivirus), in order to choose the most suitable means to enter the device in question.

336. The next step is crucial, as it consists of introducing the spyware into the system or equipment of the person under investigation, which nowadays (unlike the "Scarfo" case, described above), is generally done remotely (i.e., without physical access to the intruded system/device). For this purpose, different methods have been developed to send the spyware and compromise the computer system or device of the person under investigation, the choice of which depends on different factors (the purpose for which the spyware is used, the characteristics of the applications or systems to be intruded, the purpose and nature of the investigation, among others). Thus, for example, if spyware is intended to be used to install a "keylogger," or to carry out acoustic or audiovisual surveillance of a particular person, an input vector can be chosen consisting of a text message or email specially designed to pretend to come from a known source, so as to trick the recipients into opening an attachment or clicking on a link that will allow the spyware to enter the system (a method known as "Spear Phishing"). This is illustrated in the case below:[154]

Case 13: "Spear phishing." Sending a link containing spyware to a specific suspicious person:
As part of an investigation into bomb threats to a Washington state school in the U.S., identification of the person responsible was impeded by the instrumentality of computers "infected" by a computer virus for sending the threats.
To circumvent this obstacle, the agency in charge of the investigation requested judicial authorization to insert state spyware into a fake news story praising the technical capabilities of the person responsible for the threats, whose link was sent anonymously to the profile on the Myspace social network controlled by that person. When the person clicked on the link, the program entered his computer and sent information (including the user's real IP address) to investigators, who were then able to establish that he was a former student of the school and arrest him.

337. More recently, some companies specialized in the development of spyware for government use have begun to offer more advanced tools, with the so-called "zero-click" system, which consists of sending an SMS that introduces the spyware upon receipt, which does not require the targeted individual to perform any action to that effect and does not even appear on the screen, which considerably reduces the risk of detection.

338. However, if the objective of the investigation is to identify the users or customers of a clandestine mixer on the dark web, the spyware can be surreptitiously installed on the site itself, programming it so that it is automatically introduced into the computers of any user who performs

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

a certain action—e.g., to carry out a "Coinjoin" or "Chainhopping" operation—and report to the control server the user's real IP address and other relevant data about the computer, allowing the identification and geolocation of these people. This method, known as "Watering hole attack," was the one used in the "Playpen" case, described above (case § 11).

339. Also, to enable monitoring of communications made through some of the closed encrypted messaging systems that have emerged over the last decade (e.g., EncroChat or Sky ECC), which are used by many major criminal organizations, European law enforcement agencies have resorted to a third variant known as "Supply chain attack," as detailed above (case § 10). This consists of introducing the spyware program into the central servers of the companies providing the messaging service, so that it is distributed via system updates to the devices (cell phones) of all network users.

340. In order to realize any of these variants of the use of spyware for criminal investigation purposes, it is essential that the LEAs have the necessary IT tools to carry it out. To this end, each State may choose either to develop them internally (by means of its own specialized human resources, who discover the vulnerabilities in the main systems or applications to be intruded and design software capable of exploiting them) or to acquire those offered by different private companies dedicated to the development and commercialization of spyware for State use.

341. In this regard, it is important to bear in mind that, when it comes to using spyware in the framework of a government investigation, it is necessary to comply with requirements that do not apply when the spyware is used for illicit purposes. The first difference is that, unlike cybercriminals, LEAs cannot use an "opportunistic" criterion to select their targets (focusing on those most vulnerable to a possible attack), but the software tool they use must be able to breach the system of specific individuals who are of interest to the investigation. In addition, state spyware must guarantee a higher level of effectiveness than common malware, both in terms of obtaining the information sought without alerting the targeted person to the existence of the program, and in terms of the reliability of the data obtained, so that it can eventually be presented as evidence in criminal proceedings.

342. Another issue to consider in the use of spyware by the State is the risk of proliferation, understood as the possibility that the computer tools used by LEAs (which generally exploit vulnerabilities unknown to the companies that developed the intruded systems or applications, and against which there is no defense) fall into the hands of illegal actors, who can then use them to perpetrate cybercrime.[155] This is a very specific risk, since the use of spyware always involves introducing the software tool into someone else's system, so that—at least until it completes its function and self-destructs—it remains in the hands of the person(s) under investigation and not

[155] This was the case, for example, with the Wannacry virus used to conduct a massive ransomware attack in May 2017, which was a byproduct of a computer tool stolen in a hack of the U.S. National Security Agency (NSA).

in the hands of the state agency that sent it. In order to reduce this risk, the European Parliament recommends adopting measures such as the implementation of technical measures to prevent the rediscovery of the vulnerability exploited to introduce the spyware; the notification to the corresponding (state) authority of the discovery of a vulnerability and the request for authorization to exploit it; and the regulation of the dual use of vulnerabilities; among others.[156]

343. For the same purposes, it is recommended that the state use of spyware be implemented with the method known as "dropper/payload." According to this method, a "dropper" program is used as a "launcher," which is the one that exploits the chosen vulnerability, enables access to the system and, once this is achieved, deposits a "payload" specifically encrypted for that particular target, which includes both the spyware itself (i.e. the one that will collect the information to be obtained) and the supporting infrastructure (through which the operation of the spyware and the sending of the information to the base is controlled). The "payload" is encrypted as a security measure, to ensure that it is not detected and reused by criminals, and so that it can only be activated on the system chosen as a target: the "launcher" decrypts it when it manages to get into the system. For this purpose, it uses the specific data of the target as a key to encrypt and decrypt the "payload."[157]

344. This separation between the "dropper" program and the one that works as a "payload" also allows defenses to control the way in which the prosecution evidence was obtained in an eventual judicial process, without increasing the risk of proliferation or compromising the future usefulness of the software tool (as would be the case if its operation were disclosed). In this scenario, the "dropper" program, which is the most dangerous in terms of proliferation (because it is the one that exploits an unknown vulnerability), is always kept in reserve, since—on the other hand—it does not take part in the evidence collection phase. For the latter, the "payload" is used, which is the spyware itself. Since the operation of the latter does not require the exploitation of a vulnerability, it can be disclosed without compromising its future effectiveness or increasing the risk of proliferation.

345. In order to prove that the interception was carried out legitimately (i.e., in accordance with the provisions of the court order), it is necessary to document all the steps and actions taken to introduce the "payload" into the equipment of the subject under investigation. This can be done in different ways: filming the entire process, documenting all the steps taken in the log of the computer used to carry out the intrusion or in a record, and/or incorporating a testimonial statement from the technician detailing the actions taken in compliance with the court order. In addition, the characteristics of the program used to carry out the monitoring and the changes that

[156] Refer to: 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, p. 26.
[157] Refer to: 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, No. 1, 2014, pp. 1/64.

this program must make to the system in order to allow the interception and avoid detection must be recorded. This, in order to demonstrate that the evidence has not been destroyed or altered.

346. In countries where the use of spyware is not expressly regulated in the procedural regulations, the investigative benefits offered by the use of this measure can be reconciled with the individual rights of privacy and intimacy potentially affected by it, using the guidelines contained in comparative legislation (see, in this regard, Annex II). Among these, the following are worth mentioning:

- That the judicial authorization specifies: (a) the devices and data or digital content subject to the measure; (b) the scope of the measure; and (c) the manner in which the relevant information is to be accessed and collected.
- That the use of this method be limited only to the investigation of serious crimes.
- That a certification process be established for the software used, providing for the possibility of verifying its operation to ensure impartiality and confidentiality.
- That defense attorneys have the right to obtain the documentation related to the investigative measures carried out by means of computer programs and can verify whether the programs used have been certified.
- That the obligation to uninstall the programs at the end of their use be established.

G. Seizure and confiscation of VAs (1): Overview and preparation

347. The particular characteristics of VAs make their seizure or confiscation, although feasible, considerably more difficult than that of tangible assets such as fiat currency. There are multiple differences between VAs and physical assets, which have an impact on the manner in which their seizure or confiscation should be approached. First, a distinction must be made between centralized and decentralized VAs. In the first case, to the extent that their operation depends on a central administrative authority (the company or entity that developed and operates the currency), the VAs are always under the exclusive control of that authority. This facilitates seizure or confiscation, since there is an authority that can be the subject of a court order providing for the freezing or seizure of the funds. In contrast, in the case of decentralized currencies (such as cryptocurrencies), there is no central bank or similar institution that can freeze the funds pursuant to a court order.

348. Transactions made with most VAs, once finalized, are irreversible. This depends mainly on the type of virtual currency involved. In the case of centralized currencies, the terms and

conditions of use may provide for transactions to be revocable, although they are generally not.[158] In the case of decentralized currencies, on the other hand, transactions are always irreversible once they have been confirmed on the respective Blockchain.

349. The decentralized nature of cryptocurrencies also determines that any person holding the private key can dispose of the funds associated with the VA address corresponding to that key. There may be multiple copies of each private key, stored in different places and in different formats, and to which different persons may have access. This feature prevents the adoption of a precautionary measure that simply freezes the funds without the need for the authorities to take possession of them, such as freezing or seizure, since, as long as the cryptocurrencies are in the wallet of the suspected person, even if that person is in custody, any third party with the key can irrevocably transfer the VAs to another address.

350. Nor is it sufficient, for the purposes of securing the VAs, for the State authorities to obtain the private key that grants control over the address associated with them, since—as has been pointed out—any other person in possession of a copy of the same can transfer them. For the same reason, in order to seize VAs, it is not enough to seize the computer or the device where the cryptocurrency wallet is hosted, or to make a digital image of it. The only way to safeguard the State authorities' ability to seize VAs is to transfer them to a wallet controlled by them as soon as possible, so as to prevent a third party from removing the funds before they can pass into the hands of the State.

351. In view of the potential complexity of seizures of VAs, and their particular characteristics, it is recommended that the agencies that must carry out this type of measures establish beforehand internal policies or protocols that regulate the seizure of VAs and their subsequent treatment.[159] This should include, as a minimum:

- The identification of the officials authorized to carry out seizures or transactions with VAs.
- The details of the internal and external notifications that need to be made when a case involves VAs;
- Standard procedures for collecting and preserving electronic evidence; and
- The chain of custody protocols that should govern all devices that may contain electronic evidence.

[158] Refer to: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014, p. 42.
[159] Refer to: Regional Organized Crime Information Center (ROCIC): "Bitcoin and cryptocurrencies. Law enforcement investigative guide," Special Research Report, 2018, p. 10.

352. The seizure or confiscation of VAs requires considerable prior preparation, beyond the process of obtaining the corresponding judicial authorizations. It consists of three basic stages: (i) prior planning of the seizure; (ii) execution of the seizure; and (iii) post-seizure asset management.[160]

353. As part of the preparation, it is recommended that, to the extent possible, the type of cryptocurrencies and wallets operated by the person under investigation be determined before proceeding.[161] Wallets are the cryptocurrency equivalent of bank accounts. They provide a user-friendly interface for individuals to receive, store and transfer cryptocurrencies to others.[162] They are, in essence, applications that contain the private keys of one or more VA addresses created by the user. With respect to these, the first question to be determined is whether or not the VAs to be seized are housed in a custodial wallet (where the safekeeping of the private keys required to transfer the VAs is in charge of a VASP).

354. If the answer is yes, it is necessary to find out whether the VASP holding the wallet in custody is registered and subject to AML/CFT regulation and, if so, under the jurisdiction of which country. This is because, once this information is obtained, seizure of the VAs can be achieved by means of a court order requiring the VASP to freeze the funds and/or transfer them to an address controlled by the state authorities.

355. On the contrary, if the VAs to be seized are not housed in custodial wallets, the process is considerably more difficult, since the management of the funds is not in the hands of a third party but of the person under investigation himself (and possibly also his accomplices). Consequently, the only way to carry out the seizure is to find out the private key or the "seed words" that grant management over the VAs or the wallet, respectively, in order to be able to transfer them to a wallet controlled by the State.

356. There are several different types of wallets in which the keys are not "in custody." They may be virtual wallets (software), both desktop and mobile, or hardware wallets (hardware), in which the keys are stored in portable devices such as pen drives, or even printed on paper. Among virtual wallets, the most common are desktop wallets, which function as applications on a computer. There are also online wallets for IOS or Android smartphones, such as Mycelium, Greenbits, Breadwallet, and Airbitz. Also, there are hybrid wallets, which are those that are hosted on the servers of a third party, but in which the custody of the key remains in the possession of

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

the VA holder. Finally, there are "multi-signature" wallets, which require the authorization of more than one person to confirm a transaction.[163]

357. The determination of what kind of VA the person under investigation operates with is also fundamental for the purposes of seizure and confiscation, since cryptocurrencies can only be transferred to an address corresponding to their own Blockchain. Thus, bitcoins can only be sent to a Bitcoin address, moneros to a Monero address, etc. In the course of an asset investigation, this information can be obtained in various ways. For example, if a seller's activity on an illicit online marketplace is investigated, the type of VA accepted as payment is going to be listed in his profile. The data can also be obtained through OSINT techniques, Blockchain analysis, etc. In the image below, the icons of the main cryptocurrencies are reproduced:

358. It is also important to be able to recognize the different VA address formats for each cryptocurrency. Different features of a VA address, such as numbers, type and distribution of characters indicate what type of cryptocurrency is stored in a wallet. In turn, if researchers come across an unknown address form, there are tools on the Internet that can be used to find out what type of VA it is. The following table details the main characteristics of the most important cryptocurrencies.[164]

Table 2: Characteristics of the main cryptocurrencies:

[163] Refer to: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 14.
[164] Source: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 23.

Name	Bitcoin	Ethereum	Ripple	Litecoin	Dash	Monero	Zcash
Abbreviation	BTC	ETH	XRP	LTC	DASH	XMR	ZEC
Beginning of the address	1, 3, bc1	0x	r	L	X	4	t1, t3, z1, z3
Extension of the address	26-35	42 hex	34	34	34	95	35 or 96
Beginning of the private key	5, L, K	random	s, p	6, T	7, X	random	K, L
Extension of the private key	51/52	64 hex	51/52	51/52	51/52	64 hex	51/52

359. There are also certain "best practices" in anticipation of a search that may result in the seizure of VAs,[165] which include:

- Being aware of when the suspected person's devices have been connected or in use (by determining patterns of behavior, network monitoring, surveillance, or undercover action, as appropriate).
- Constant monitoring of the target's activity and the behavior of their VAs address(es).
- Prepare for the possibility of encountering accounts that require two-factor authentication.
- To the extent possible, ensure access to fingerprints or other biometric data that would allow access to devices protected by such means (e.g., by having the holder of such devices in custody or having authorization to arrest the holder during the search and compel the opening of the devices).

360. Given the importance of speed in the seizure of VAs, it is important to obtain judicial authorization to carry it out before proceeding with any search that may result in the discovery of the wallet(s) of the person under investigation.

361. It is also important to request, also beforehand, judicial authorization to seize, in the course of the search, all data storage devices that may be found in the home or offices of the suspect (removable hard disks, CDRs, DVDRs, memory sticks, pendrives, etc.). This, since they can be hardware wallets or contain important information in digital format, such as the "seed words" that

[165] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 47 § 158.

allow reconstructing a VA wallet, the passwords used by the user to access a hybrid wallet, etc. Also, to perform a forensic image and have a specialist analyze the devices for relevant evidence.[166]

362. In particular, it is essential to have judicial authorization so that, in the event that during the search of a home—or the arrest of a suspect—it is found that the suspect's computer or smartphone or tablet is unlocked and active, this circumstance can be used to analyze its contents in search of VA wallets. This is because the ideal opportunity to seize cryptocurrencies is when the wallet containing the private key(s) is open, or when the password to open it or the "seed phrase" that allows it to be reconstructed is found during registration. This also prevents future access to the content from being hindered by encryption. It should be noted, in this regard, that the smartphones and tablets of the main technology companies (Apple and Google) are equipped with a security measure that encrypts the entire content when the equipment is locked, by means of a cryptographic key linked to the password.

363. Regarding the content of the judicial authorizations linked to the VA seizure proceeding, it is also important to bear in mind that in order to prevent any accomplice of the person under investigation from transferring the funds to be obtained while the procedure is in progress, it is essential to isolate that person and all other persons present during the proceedings in order to prevent them from connecting to the Internet or making contact with the outside world until the seizure has been completed. Moreover, the planning of the search must take into consideration the need to neutralize, as soon as possible, any possibility that the person under investigation destroys, alters, or conceals information useful for accessing the VA wallet (handwritten passwords or pins, hardware wallets, etc.) transfer its contents, or give notice to a third party to do it for him, before the authorities access it.

364. A final aspect of pre-seizure or confiscation planning is the generation of VA addresses controlled by the investigating agency or authority in charge of the proceeding in accordance with local law. For this purpose, it is recommended[167] that the public and private keys be generated with a wallet application on a computer not connected to the Internet,[168] and then use a Blockchain browser to verify that there is no record of the public address on it. Finally, the public key (but not the private key) must be transferred from the initial computer to a laptop equipped with the necessary applications to perform a VA transfer, which is the one that is going to be taken to the procedure to realize the seizure.

365. It is necessary to bear in mind that each type of cryptocurrency operates with its own Blockchain and can only be transferred to a VA address within it, which is why it is necessary to

[166] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 26 § 82.
[167] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 27/28, § 84.
[168] To this end, the guide prepared by the Council of Europe on VA seizure contains detailed instructions on the operation of the main wallets. Refer to: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021.

create as many addresses as types of cryptocurrencies to be seized. The same with the wallets, as some support multiple VAs, while others are exclusive.

H. Seizure and confiscation of VAs (2): Relevant evidence or clues in records

366. In general, but especially when investigating possible ML/TF schemes with VAs, the purpose of a search of the property of the person under investigation should not be limited to locating physical assets such as trust money, jewelry, automobiles, etc., or paper documentation (bank account information, checks, documentation referring to transfers, etc.) for eventual seizure or confiscation. On the contrary, investigators should consider the search as a gateway to obtain information that leads to the discovery of less obvious elements, but which may be as or more useful for the asset investigations that are the subject of this guide.

367. Indeed, in the course of a search of a property (be it a home, an office or even cars, boats, etc.), investigators may come across different elements that may be relevant either as evidence, as information leading to evidence, or as a key to enable the seizure or confiscation of VAs of illicit origin. For instance:

- Computers or other devices containing information in electronic format, such as cell phones, tablets, pen drives, removable hard disks, etc.
- VA wallets, either in virtual format (such as applications within the aforementioned electronic equipment) or in physical format, such as hardware or paper wallets.
- Information that allows access to the wallets or the transfer of VAs, such as passwords or pins to access encrypted wallets or online wallets hosted in external servers, VA addresses and—especially—the private keys or "seed words" that are essential for the seizure of decentralized virtual currencies contained in wallets that are not "in custody."

368. VA wallets are, in essence, computer applications that store the VA address(es) belonging to an individual and the public and private keys associated with each address, while facilitating the transfer of cryptocurrencies through a simple interface. Virtual wallets can be "desktop" (for computers), "mobile" (for smartphones) or online, which are those whose use is offered as a service and are stored "in the cloud" (i.e., on external servers). These include Armory, Bitcoin Core, Bitcoin Knots, Bither, Bitpay, Electrum, Wasabi, Mycelium, among many others. They can be searched on Google Apps or Apple's App Store. Wallets are generally identified by an icon on the desktop of the computer or the home page of the cell phone (see image above, at § 325). Otherwise, they can be located by using the computer's search engine to identify the files with the word "wallet" or a ".dat" extension (although in some cases, the user may have saved them with another name or extension).

369. There may also be wallets stored on a physical device ("hardware wallets"), such as a pendrive. Like virtual wallets, the contents of these are also usually protected by encryption, requiring a password to access the addresses and keys in plaintext format. The fundamental difference between physical and virtual wallets is that the former is not connected to the Internet (which is why they are known as "cold wallets"), which offers the holder a higher degree of security against possible hacking. The most common are KeepKey, Nano Ledger S, and Trezor The image below[169] shows one of these hardware wallets.

370. The "paper" wallets basically consist of documents on paper or other material on which information can be printed (such as wood or metal), on which the VA address and the public and private keys are recorded, either in plaintext format or in the form of a QR code, so that they can be "translated" by means of a smartphone or other similar device. The following image shows a paper wallet containing both plaintext and QR keys:

371. The following image, shows a paper wallet with QR codes.[170] On the left is the Bitcoin address, on the right the private key:

[169] Source: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 75.
[170] Source: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 101.

372. If a paper wallet is discovered, it is possible to verify the existence of funds by scanning the QR code and using a mobile application to check it against the information available on the Blockchain of the cryptocurrency in question. The same app can be used to transfer the VAs to a wallet controlled by the authorities, thus making the seizure of the funds a reality. This operation is considerably more difficult if the paper wallet is of the encrypted type, such as the one illustrated in the following image.[171] In such a case, the VAs can only be transferred if the corresponding password is available.

373. VA wallets encountered by investigators during a search are most likely to be protected by passwords (to gain access), pins (to enable transactions) or both. It is therefore essential to carefully check the place being searched—and, in particular, the environment around the location of the person's computer—for handwritten notes, notebooks, jottings, diaries, sticky notes, etc., in which the passwords or pins needed to carry out transactions through such wallets may have been entered. Sometimes, passwords can be obtained through computer techniques such as memory analysis,[172] interrogation of witnesses who have knowledge of them or through the surreptitious installation of "keylogger" spyware.

374. The essential elements for carrying out cryptocurrency transactions (VA address, public key and private key) are relatively large alphanumeric combinations and, therefore, difficult to memorize. Thus, for example, a person using bitcoins must remember a "private key" consisting of a 64-digit access code, which usually has the following form:

A5373D44C6D87DC0FA6A6738334369F4553213303DA61F20BD67FC233AA37485

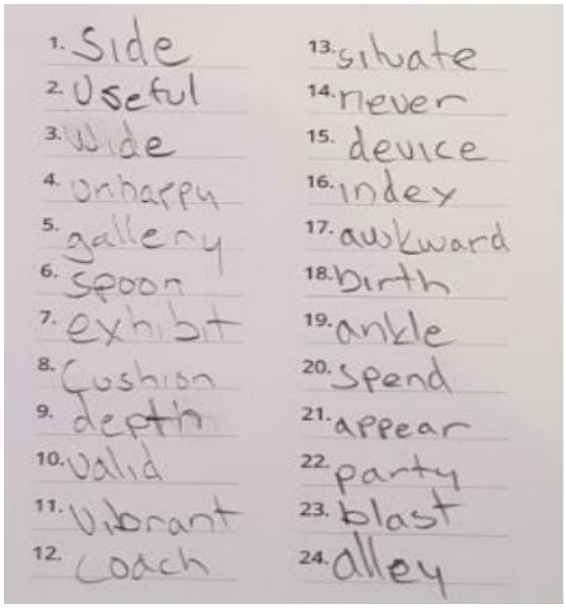
[171] Source: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 101.
[172] Source: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 23.

375. Given the complexity of the keys in this format, Bitcoin generated an algorithm to simplify them (called "Base 58 import format"), converting them into a shorter and simpler cryptographic chain, which is the one usually found in the hands of Bitcoin users. However, even so, the alphanumeric strings used to operate with this, and other cryptocurrencies are still long, as illustrated in the following image:[173]

376. Because of this, VA users are most likely to make a written note of the passwords and put them in a safe place, such as their home, office or cell phone. Therefore, this is where investigators should look.

377. If the person under investigation uses a more sophisticated wallet, such as HD wallets, the relevant information for use includes a list of between 12 to 36 words in different languages (English, Japanese, Korean, Spanish, Chinese, French and Italian) that make up a mnemonic (called "seed words"/"seed phrase"), containing all the information required to recover the wallet in case of loss, damage to the equipment, etc. A list of "seed words" is illustrated in the following image:[174]

[173] There is a Bitcoin address first, then a private key reduced with the Base 58 algorithm (private key) and finally a public key.
[174] Source: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 88.



378. If, during the search, the investigators find the "seed words," they can use them to reconstruct the wallet (including its private key) and thus transfer the VAs to a state-controlled wallet, thus completing the seizure. The procedure is very simple: the 12 or 24 words are introduced—for example, in a hardware wallet such as the Ledger—and at the end of the last one, an exact copy of the original wallet is obtained.

379. It is important to keep in mind, however, that not all wallets follow the same protocols. Therefore, depending on the type of wallet in question, its reconstruction from the seed phrase may yield the same result as if accessing the original (all the VAs contained in it), or an empty wallet.[175] There are applications that make it possible to determine what type of result the reconstruction of a given wallet by means of the seed phrase will produce.

380. An additional piece of information, very useful for asset investigations, which may be found during a physical search is the "Returning customer number" with which some VA mixers identify the persons that use their services more than once, in order to avoid that the illicit cryptocurrencies held in reserve are paid twice to the same customer. To this end, after each "mixing," the customer is given a number that must be presented if the mixer's services are used again, and which is used by the platform to determine which VAs not to use in the new mixing process.[176] Finding this number, although it does not facilitate the seizure of cryptocurrencies of illicit origin, is useful as evidence of the use of mixers, as well as—potentially—to identify the specific mixer that processed

[175] Source: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 116.
[176] Refer to: 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, No. 2, 2018, pp. 423/424.

the VAs of the person under investigation and allow an eventual traceability through "Chain analysis" techniques.

I. Seizure and confiscation of VAs (3): Execution

381. Except in cases where the VAs to be seized are centralized virtual currencies, or cryptocurrencies themselves but housed in a custodial wallet (in which case, the measure may be carried out with the assistance of the central administrative authority of the centralized currency or with that of the VASP that holds the VAs in custody), in all other cases the seizure of VAs begins with obtaining the private keys, seed words and/or wallets of the person under investigation.

382. Due to its greater technical difficulty, compared to the seizure of physical assets, it is preferable that the measure be carried out by specialized and trained personnel, since, in addition, speed may be essential to ensure the success of the seizure. Therefore, it is necessary for those carrying out the measure to be aware of the different varieties of VA wallets that exist and the security mechanisms they have, such as hidden sub-wallets or the existence of ways to regain control of the account after the authorities have taken control of it[177] (for example, through seed words).

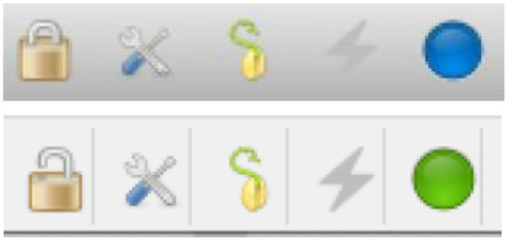
383. In view of the existence of such security measures, it should be borne in mind that, in practice, the best—and in some cases, perhaps the only—way to carry out the seizure of VAs contained in a wallet controlled by the person under investigation is to do so while the wallet is unblocked and in use. Otherwise, access to the wallet would probably require the entry of a password, and its contents would be protected by encryption.

384. To this effect, it should be ensured, if possible, that the procedure aimed at obtaining control over the device containing the wallet is carried out in such a way as to surprise the person under investigation when he/she is using it. Thus, in a notorious case, a suspect's computer (protected by a powerful encryption tool) was hijacked in order to ensure access to its contents in plaintext format.[178]

Case 14: Ross Ulbrich. Capture of computing devices while they are in operation:
The FBI's arrest of the head of the Silk Road "virtual marketplace" was carefully planned to ensure access to his laptop, the contents of which the agency knew were protected by full-disk encryption technology when it was at rest.
To that end, and after learning that Ulbrich was using the computer at a public library, the FBI dispatched two plainclothes agents who created a distraction in the suspect's vicinity, an opportunity that was seized by another agent to take the laptop while it was open and running. Thus, while Ulbrich was being detained, the computer was handed over to a specialized technician who was able to start analyzing it immediately and access the information contained on it in plaintext format.

[177] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 29 § 86.
[178] Source: KERR, Orin S. / SCHNEIER, Bruce: "Encryption workarounds," Georgetown Law Journal, Vol. 106, No. 4, 2018, pp. 989/1019.

385. The icons corresponding to a locked and encrypted (closed padlock) or unlocked and in use (open padlock) wallet are illustrated below:[179]



386. If during the search, the intervening agents come across the blocked wallet and are unable to find the password required to access it, the device containing it must be seized (as would be done with any other device containing relevant digital evidence), adopting the necessary precautions established in the protocols on the treatment of electronic evidence. Subsequently, and bearing in mind the need to act as quickly as possible, the relevant investigative measures should be taken to try to obtain the passwords and seize the VAs associated with it.

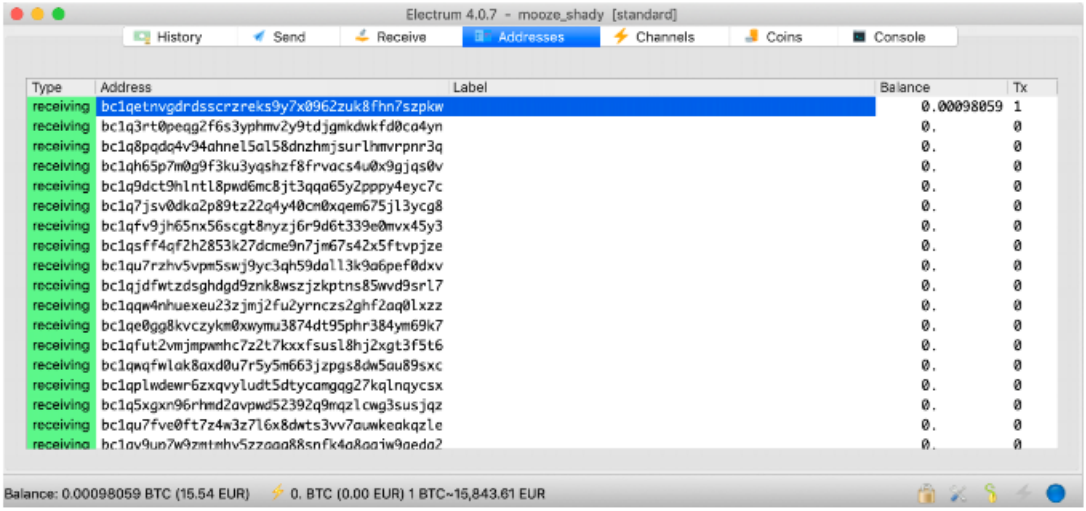
387. If this is not possible, because access to the wallet cannot be obtained (or because it is found empty once it has been opened), an alternative is the seizure of assets of equivalent value.[180] For this purpose, the public nature of Blockchains is a key source of information, since it facilitates the determination of the precise amount of the substitute funds subject to seizure. This is so, since all transactions involving VAs are undoubtedly recorded therein. Therefore, once the address(es) of the person subject to the measure have been identified, the exact amount of the transactions carried out by such person, including those made with funds of illicit origin, can be consulted in the Blockchain.

388. If, on the other hand, the wallet is found to be unblocked, the seizure must be carried out as soon as possible. Likewise, in such a case—as in any other involving access to digital evidence contained in devices that can be blocked or turned off by themselves—it is essential to adopt the necessary measures to ensure that they are kept on and in use, in order to prevent them from being blocked again, hindering access to the wallet or protecting the contents by means of encryption, as occurred in the case detailed below:[181]

[179] Source: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 35.
[180] Refer to: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014, p. 156.
[181] Source: judgment rendered in re "Boucher;" 2007 WL 4246473, District Court of Appeals for the District of Vermont, 2009.

Case 14: "Boucher." Loss of access to data due to error in the manipulation of a computer:
Suspect Boucher was apprehended while entering the U.S. from Canada, when a customs agent checked the suspect's laptop, which was turned on and in use, and viewed images of child sexual exploitation on the laptop.
At the time of Boucher's arrest, the computer was seized, at which time the agents in charge turned it off. As a result, when it was turned back on to analyze its contents, a protection program was put in place that encrypted it in its entirety, preventing access to it in plaintext format in the absence of the password required to disable it.
In order to carry out the forensic analysis of the content, the U.S. authorities had to request a court order to compel the detainee to provide the password, which was initially denied on the grounds that it violated the prohibition against compulsory self-incrimination. Only on appeal was the requested authorization granted.

389. In addition, agents taking part in the procedure should be aware that a cryptocurrency wallet may host multiple addresses (in some cases, even of different cryptocurrencies) containing VAs potentially subject to seizure. The image below shows the screen of a wallet (for Windows operating system) displaying multiple Bitcoin addresses:[182]



390. Digital files containing virtual wallets (desktop or mobile) must be exported from the device of the person under investigation with the help of a computer forensic tool. A digital image of the entire wallet must be made, as well as copies or digital images (as the case may be) of the private keys or seed words found in paper documents or in text or Word files. They should then be imported into the computer of the investigative agency that has the necessary software to carry out the seizure.[183]

391. The final step consists of the actual seizure, which takes place when the VAs are transferred from the address of the person under investigation to the one controlled by the

[182] Source: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 36.
[183] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 29 § 87.

competent authority, for which purpose the computer used by the agents must be connected to the Internet and, where appropriate, also synchronized with the corresponding Blockchain.[184] For greater efficiency in the realization of the seizure of VAs, it is recommended to adopt a series of good practices, including the following:

- As far as possible, have the state address(es) converted in advance to QR format, in order to avoid typing errors (especially if the seizure is conducted with mobile wallets, where it is more feasible to make such errors).

- Otherwise, it is recommended to double, or triple check the destination address individually before making the transfer. In this regard, it is worth remembering that cryptocurrency transactions are irrevocable, so if VAs are sent to the wrong address, they cannot be recovered.

- It is convenient to use the "sweep" function of VA wallets, which simply transfers the entire balance of the wallet being seized to the destination wallet (in this case, the one previously set up by the authorities carrying out the seizure).

- For the purpose of speed, both the FATF and the Council of Europe recommend, in their respective guidelines, to set the highest fee that is authorized, in order to ensure that Blockchain miners place it in the nearest block and that it is realized more quickly.

- If state-controlled addresses are stored in paper wallets, it is necessary to ensure that the private keys are not visible, or that they are multi-signed, in order to reduce the risk of theft of seized VAs.

- In this regard, it is also essential that when the minutes or report on the seizure of VAs are drawn up, the private key or the seed phrase that enables their transfer should not be recorded in any case.

- Finally, once the seizure has been completed, the balance of the previously emptied VA address(es) should be periodically verified, since it may happen that transfers or payments are received after the procedure.

J. Seizure and confiscation of VAs (4): Post-Seizure Treatment

392. During the post-seizure stage, there are a number of considerations to be made by the competent authorities in order to decide whether or not to liquidate the seized VAs or convert them to fiat currency, such as the need to preserve the value of the cryptocurrencies in custody

[184] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 29 § 88.

against fluctuations in their price, or whether there is a legitimate use in the market for the specific class of seized VAs.

393. Broadly speaking, there are two alternatives with respect to the treatment of seized VAs. Namely:

a. **Retain them until the final confiscation decision is issued:** In this case, once the VAs are seized, they are entrusted to the custody of a previously designated authority, which administers them until a final decision on their confiscation is made and their liquidation is authorized. The advantage of this alternative is that the VAs are only sold once the final decision on the conviction or acquittal of the accused has been handed down and are therefore available if they need to be returned. The disadvantage lies in the risks inherent in the maintenance of VAs, and the costs associated with it.

b. **Immediately (or within a short period of time) converting them into fiat currency:** In contrast to the alternative described above, the advantage of this alternative lies in the reduction of the security risks associated with the maintenance of VAs and the costs associated with it. The disadvantage lies in the possibility of loss of quotation with respect to the time at which they may eventually have to be returned to the accused in the event that he/she is found not guilty. At the regional level, the OAS generally recommends, for all seized assets (virtual or physical), to proceed with the anticipated sale and invest the resulting funds until the resolution on the merits is issued.

394. In this context, in some jurisdictions (e.g., the Netherlands), the prior owner of the seized VAs (i.e., the person under investigation) is consulted in writing as to whether he/she prefers them to be kept in their original state or converted into fiat currency. In this way, if they are to be returned at a later date, the State is released from liability for any loss of value resulting from fluctuations in the price of the cryptocurrency(ies) in question.

395. Another alternative is to establish in advance (either through a regulation or written internal policies) a fixed term for the conversion of seized VAs into fiat currency (for example, three days), so that the decision to carry out such conversion does not depend on a judgment about its convenience in economic terms, based on the quotation of the cryptocurrency(ies) in question at a given time.

396. Once the decision to liquidate the seized or confiscated VAs has been taken, and in accordance with the provisions of the applicable legislation or the decision of the competent authority, the sale may be carried out directly or through a public auction, always in an attempt to maximize the value obtained. An agreement may also be reached with a private operator specialized in the exchange of VAs (i.e., a VASP) to undertake the conversion of cryptocurrencies into fiat currency. In case the competent authorities do not have a reliable cybersecurity structure

for the storage of VAs, such a VASP may also be entrusted with the administration of the seized assets.

397. Some jurisdictions (such as, for example, the USA) have decided not to liquidate certain seized VAs, when they consider that there are no legitimate uses for them in the market. Such is the case of "private currencies" such as Monero. In the event that such a decision is made, the necessary security measures must be taken to ensure effective permanent storage of the VAs in question.

398. In this regard, it is recommended that the seized VAs be stored in cold storage wallets (e.g., a hardware wallet, or a virtual one, but contained in a computer not connected to the Internet, or even in paper wallets).[185] Similarly, seized VAs may be stored in multi-signature wallets, so that they cannot be stolen by illicitly obtaining a single private key.

399. It is also recommended that a list of passwords for access to each of the electronic devices (including computers and smartphones), encrypted external storage units and seized VA wallets be kept in the hands of a specifically designated official, restricting access to them as much as possible. Seed phrases, passwords, private keys, pins and VA addresses obtained can be kept in text files, in a designated folder for each seized VA on an external storage drive (e.g., a removable hard drive), if possible encrypted for security. These drives should be kept offline in a specific secure location until required by the competent authorities to receive or transfer the VAs.[186]

K. Multidisciplinary approach

400. In view of the constant evolution of ML/TF typologies and the emergence of new technologies that facilitate the commission of such crimes, agencies in charge of preventing and prosecuting money laundering and terrorist financing need to acquire up-to-date knowledge and skills with respect to cybercrime, the anti-forensic technological tools used by criminals and the methods and techniques available to counteract them.[187] All the more so given the growing involvement, worldwide, of criminal organizations in criminal activity in cyberspace (in all its variants), which gained remarkable momentum during the global Covid-19 pandemic, as highlighted by the FATF in a report published in 2020.[188]

[185] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, pp. 31/32, § 99. In this regard, the guide prepared by the Council of Europe contains a detailed explanation of how to use the main hardware wallets, as well as how to make a paper wallet. Refer to: Council of Europe: "Guide on seizing cryptocurrencies", Cybercrime Programme Office of the Council of Europe, February 2021.
[186] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 32 § 101.
[187] Refer to: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014. In turn, the aforementioned organization referred to the problem of new technologies in relation to cybercrime in a study on the subject published in 2013 (see: United Nations Office on Drugs and Crime (UNODC), *Comprehensive study on cybercrime*, 2013).
[188] Refer to: FATF: Covid-19-related ML/TF. Risks and Responses," May 2020.

401. The growing prevalence of cybercrime in recent years (including its ML/TF counterpart, crypto-laundering) has forced the LEAs to rethink their organizational and operational structures, strengthening units specialized in crimes involving the use of ICTs and training in the use of IT tools. In such a context, the specific skills required for the effective investigation of this type of crime mean that it is not sufficient to relocate existing personnel, even if they are provided with additional training: new personnel with such skills, including from the private sector, must be brought in.[189]

402. In this regard, the Meeting of Ministers of Justice and Other Ministers and Attorneys General of the Americas (REMJA) of the Organization of American States (OAS) recommends that states that have not yet done so establish, as soon as possible, units or entities specifically responsible for directing and developing the investigation and prosecution of cybercrime and assign them the human, financial, and technical resources necessary to perform their functions in an effective, efficient, and timely manner.

403. In particular, the investigation of criminal behaviors involving VAs requires trained investigators who are familiar with the technologies that allow for the identification, tracing, and seizure of such assets. In many cases, the personnel with some of these capabilities are found in some of the cybersecurity units existing in the countries of the region, whose operation is generally not integrated with that of the units or agencies in charge of investigating ML/TF schemes, with or without VAs.

404. In this regard, the FATF notes that, depending on the specificities of each country, it is possible that different agencies or authorities are responsible for conducting asset investigations, seizure or confiscation of funds of illicit origin, ML/TF prevention, combating cybercrime and computer forensic analysis. Therefore, cooperation among all of them is a fundamental condition for the success of criminal investigations and prosecutions concerning these crimes.[190]

405. In this context, organizations such as Interpol, Europol,[191] and UNODC[192] emphasize the importance of a multidisciplinary approach in investigations of ML/TF schemes involving VAs. This is because they require a combination of traditional investigative techniques and new approaches based on ICTs. Thus, agents specialized in asset investigations can contribute their knowledge of financial fraud and accounting or tax crimes, in addition to their knowledge of the activity of organized criminal groups, while cybercrime units have relevant knowledge in terms of the use of

[189] Refer to: Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations," 2018, pp. 54/56. In the same sense: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014, pp. 61/62.
[190] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 45 § 151.
[191] Refer to: INTERPOL / Basel Institute on Governance / EUROPOL: "Recommendations. 4th Global Conference on Criminal Finances and Cryptocurrencies," November 2020, p. 3.
[192] Refer to: United Nations Office on Drugs and Crime (UNODC) "Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies," June 2014, p. 67.

advanced technological tools and the processing of digital evidence. The synergy between these two categories of investigators is essential for the effective prosecution of crypto-laundering, which is why the formation of multidisciplinary groups composed of professionals from both areas is strongly recommended.[193] This, in turn, responds to FATF Recommendation 30.

406. In addition, given that the prosecution of crimes involving the use of VAs requires specific knowledge, it is recommended that the agencies responsible for investigating this type of illicit behavior act in coordination with prosecutors or judicial operators trained in the field, especially with regard to the collection, analysis, and processing of electronic evidence and the seizure and confiscation of VAs.[194] The use of advanced technological investigation techniques or tools, such as chain analysis, OSINT, digital undercover agents, and the use of spyware, where their use is permitted by local procedural legislation, should also be considered.

L. International cooperation

407. The transnational nature of the Internet and the VA ecosystem makes international cooperation an essential element of asset investigations into the criminal behavior associated with them. In order for such investigations to yield satisfactory results, all channels (formal and informal) of collaboration must be used effectively and, above all, in a timely manner. The latter, in view of the importance of speed in allowing the preservation of digital evidence, as it is often routinely disposed of as a result of automated procedures.

408. In this scenario, it is recommended that the agencies or authorities responsible for investigating ML/TF schemes with VAs use all available means to connect with their counterparts abroad,[195] including cooperation mechanisms between law enforcement agencies (INTERPOL, EUROPOL); contact points for the exchange of information related to the seizure and confiscation of illicit assets (RRAG, CARIN, ARIN networks, StAR and GFPN); contact points for the exchange of information linked to cybercrime (Inter-American Cybercrime Cooperation Portal and G-7 24/7 Contact Network); channels for international legal cooperation such as IberRed; networks for the exchange of financial intelligence information gathered by FIUs (Egmont Group); as well as requests for mutual legal assistance.

409. The FATF[196] stresses the importance of fully exploiting international cooperation tools possible, especially the possibility of requesting digital evidence preservation measures such as those provided for in the international instruments on cybercrime outlined in § IV.6 of this guide, in order to prevent the loss of relevant evidence or the leakage of assets that may be subject to confiscation. Although, in contrast to the speed required for investigations involving illicit activity

[193] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 17 § 49.
[194] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 44 § 150.
[195] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 46 § 156.
[196] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 46 § 154.

in cyberspace, recourse to legal cooperation tools such as mutual legal assistance requests may be excessively slow or cumbersome, there are ways to maximize the possible results. In this regard, it is recommended that direct contact be established with authorities in the foreign counterpart who are familiar with the subject matter of the cooperation request (investigations of illicit activity with VAs) and—in general—with the issue of digital evidence, as well as the establishment of informal channels of communication with similar agencies in other countries to facilitate collaboration.

410. With regard to the subject matter of this guide, the RRAG is a fundamental tool for identifying assets and persons abroad that may be relevant in the framework of an investigation into ML/TF schemes using VAs and for learning about criminal proceedings underway in other countries. To this end, general, social, tax, property and financial data may be requested through the network's secure platform, either to enrich the information available to investigators in the requesting country, or to facilitate the preparation of requests for international legal assistance with accurate data, thus increasing the chances of success.

411. In this regard, the RRAG currently has 48 contact points from twenty-two (22) countries with direct access to the secure RRAG platform from prosecutors' offices, police, FIU, and other law enforcement authorities. This platform allows for the exchange of information between RRAG countries and the 54 jurisdictions belonging to the CARIN Network. In addition, RRAG contact points can access information held by other international organizations involved in asset confiscation, such as the Camden Asset Recovery Inter-Agency Network (CARIN), the Global Asset Recovery Focal Point Network (GFPN), and Interpol's Stolen Asset Recovery (StAR) Initiative. In addition, information collected by ARIN networks around the world, including the Asset Recovery Inter-Agency Network for Asia Pacific (ARIN-AP) and West and Central Asia (ARIN-WCA), the Caribbean Asset Recovery Inter-Agency Network (ARIN-CARIB), the Asset Recovery Inter-Agency Network for Eastern Africa (ARIN-EA), Southern Africa (ARIN-SA) and West Africa (ARIN-WA) can also be accessed through this channel.[197]

412. Moreover, within the OAS, the Technical Secretariat of the Meeting of Ministers of Justice and Other Ministers and Attorneys General of the Americas (REMJA) is in charge of the Inter-American Cooperation Portal on Cyber-Crime, created in 1999, whose purposes are to strengthen international cooperation in the prevention, investigation, and prosecution of cyber-crime; facilitate the exchange of information and experiences among its members; and make the necessary recommendations to improve and strengthen cooperation among OAS member states and with international organizations and mechanisms.

413. In turn, the REMJA Technical Secretariat (Department of Legal Cooperation of the Secretariat for Legal Affairs of the OAS) maintains an updated directory of criminal prosecution

[197] Refer to: RRAG/GAFILAT: "Inventory of existing global networks for the identification and recovery of proceeds of crime," June 2021.

and police authorities that serve as contact points for international cooperation on cybercrime and electronic evidence.

414. With regard to international cooperation on cybercrime (including crypto-laundering through VAs), the REMJA recommended that member countries strengthen mechanisms for information exchange and cooperation with other international organizations and agencies in the area of cybercrime, such as the United Nations, the Council of Europe, the European Union, the Asia-Pacific Economic Cooperation (APEC), the Organization for Economic Cooperation and Development (OECD), the G-7, the Commonwealth and INTERPOL, so that OAS Member States can take advantage of developments in those areas. States that have not yet done so were also urged to join the G-7 "24/7 High Tech Crime Contact Network" as soon as possible.

415. In this regard, REMJA XI concluded that the new information and communication technologies (ICTs) are useful tools for strengthening international legal cooperation in the various branches of law and are ideal means for facilitating the establishment by states of mechanisms for contact, collaboration, and coordination among the various authorities responsible for processing requests for legal cooperation and mutual assistance in the various areas of law. Accordingly, it was recommended that the member states adopt the necessary measures to promote the use of new ICTs, such as the electronic processing of mutual legal assistance requests, including the acceptance of official documents with electronic or digital signatures, and videoconferencing, in a secure and responsible manner, to make international legal cooperation in the Americas more effective, efficient, and expeditious.

M. Education and training

416. Investigating the illicit use of VAs involves the analysis of complex technologies and, therefore, requires the development of novel investigative techniques and the acquisition of new resources and capabilities. Given that illicit actors generally tend to adapt to a changing context faster than the authorities, it is essential to take the necessary steps for LEAs to acquire the required levels of competence to successfully investigate the exploitation of VAs for criminal purposes.[198]

417. To this end, it is necessary to implement training programs aimed at the widest possible range of personnel, so that they acquire the minimum knowledge necessary to carry out—or at least, not compromise—asset investigations referring to the illicit use of VAs.

[198] Refer to: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 64.

418. In such context, there are three categories of training relevant to procure the adaptation of LEAs to the new technological scenario.[199] Namely:

a. **Training for investigators** regarding the new technologies involved in asset investigations on the illegal use of VAs.

b. **Training for police officers in general** on how to recognize and react to the existence of digital evidence relevant to those kinds of investigations; and

c. **Training for forensic investigators** regarding the new technologies involved.

419. With regard to the first category, while not all investigative personnel need to specialize in the use of VAs, it is necessary to have a number of experts (proportional to the size of the jurisdiction) who are trained to reconstruct a chain of transactions on the Blockchain and/or to seize or confiscate VAs. Other personnel should only have the minimum knowledge necessary to recognize clues about the possible use of cryptocurrencies if they come across them in the course of an investigation or when conducting a search, as well as be aware of how to contact specialized law enforcement officers within their jurisdiction.[200]

420. In this context, it is important that a sufficient number of agents receive training in the use of forensic tools for traceability of VAs that are available on the market or, alternatively, those developed internally by each country, if it decides to do so.[201] This, since the participation of agents lacking adequate preparation in these tasks generates the risk of misinterpreting the information available in the Blockchain, which may lead to pursuing false leads or overlooking really relevant data.[202]

421. Similarly, it is vital that the seizure of VAs be carried out by specialized personnel, to avoid errors that could lead to the loss of funds. Therefore, the relevant authorities (be they police agencies or competent prosecutors' offices) must be trained to handle the different types of VA wallets that may be used in these procedures, as well as the cybersecurity issues inherent to the management of the seized assets.

422. Notwithstanding the above, in view of the possibility that agents not belonging to specialized units may come across cryptocurrencies in compliance with search warrants, etc., it is necessary that LEA personnel who may potentially find themselves in such a situation know how to recognize at least the most important features of the use of VAs (QR codes, seed phrases, public

[199] Refer to, as applicable: Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations," 2018, p. 59.
[200] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 42 § 139.
[201] Refer to: Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021, p. 65.
[202] Refer to: FATF: "Guidance on financial investigations involving virtual assets," June 2019, p. 25 § 79.

or private keys, different cryptocurrency address formats and different types of wallets, passwords, pins, etc.).[203] Also, on a more general level, they should be able to recognize devices that may contain digital evidence.[204]

423. The actions aimed at providing this training are varied, including the organization of training programs, the preparation of handbooks, exchange programs and/or participation in international conferences or seminars. In this direction, and in order to expand as much as possible the scope of knowledge on VAs among law enforcement personnel, it is advisable to distribute reference material (brochures, instructions) containing detailed pages or applications related to VAs, exchange platforms, payment processors, and cryptocurrency wallet service providers, images of seed phrases, QR codes, paper or hardware wallets and VA ATMs, etc.

424. Finally, the implementation of instances of public-private cooperation with private sector actors specialized in these new technologies is also recommended, aimed at ensuring that the LEAs and public prosecutor units with competence in the field are kept up to date with respect to new developments in this area.[205]

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

ANNEX I: GUIDELINES FOR INVESTIGATION, IDENTIFICATION, SEIZURE, AND CONFISCATION OF VIRTUAL ASSETS

A. BASIC CONCEPTS

1. **Virtual Asset (VA):** As defined by the FATF, a digital representation of value that can be digitally exchanged or transferred and used as a form of payment or investment instrument. VAs do not include digital representations of fiat currency, securities, and other financial assets that are already covered elsewhere in the standards.

2. **Fiat money:** It refers to real (non-virtual) currency or money, or national currency. It differs from virtual currency in that it functions as the currency and paper money of a country, designated as legal tender; it circulates, is used, and accepted as a means of exchange in the country of issuance.

3. **Cryptocurrencies:** These are open source, convertible and decentralized VAs that operate in a distributed peer-to-peer network that applies mathematical and cryptographic principles to provide security to the system. Transfers between users are carried out "peer-to-peer," without intermediaries, based on a set of public and private cryptographic keys, and require cryptographic signature to be completed. The transparency of the system is ensured by the recording of transactions in a sort of distributed "ledger" (called Blockchain in most cryptocurrencies), maintained by a network of mutually "untrusted" parties (called "miners" in the Bitcoin and other cryptocurrencies ecosystem) that elaborate the cryptographic blocks of the chain and are rewarded for it with fees paid by the users.

Icons of the main cryptocurrencies:

4. **Bitcoin:** Launched in 2009, it was the first decentralized convertible VA, and the first cryptocurrency. Bitcoins are account units composed of unique alphanumeric sequences that constitute units of currency (divisible, in turn, into smaller units, called Satoshis) and

have value only because individual users are willing to pay for them. Bitcoins are traded digitally between users in a partially anonymous form (the persons or entities involved in each transaction are identified only by alphanumeric pseudonyms called "Bitcoin addresses") and can be exchanged for fiat currency or other cryptocurrencies. The software required to send, receive, and store bitcoins or to monitor transactions can be downloaded free of charge. Users can also obtain their Bitcoin addresses (which function as accounts) from Bitcoin exchange platforms or online wallet services. Transactions (flows of funds) are recorded in a shared public registry (the "blockchain"), where they are identified by Bitcoin addresses.

5. **VA or cryptocurrency address (e.g., Bitcoin address):** It is an alphanumeric code that identifies the virtual location associated with a certain amount of VAs, necessary to be able to send or receive cryptocurrencies. It works like a bank account in the traditional financial system to receive or send transfers. For example, Bitcoin addresses are between 26 and 32 characters long. They start with the number 1 for standard addresses and number 3 for multi-signature addresses. Other cryptocurrencies have their own systems for representing their addresses. VA addresses can also be represented by means of QR codes.

6. **Blockchain:** It is a form of registry or "ledger" used by Bitcoin and most cryptocurrencies and works by chaining together blocks of data. Each of these blocks contains information about the transaction being carried out. The initial and final elements of the block are related, respectively, to the previous and next block. Thus, modification of the block would corrupt the entire chain, although it is practically impossible to alter it. In addition, blockchain-based technology works in a distributed fashion, with multiple computers operating simultaneously with the chain, which makes it extremely difficult to compromise it through a computer attack. Each cryptocurrency has its own Blockchain.

7. **Private key:** It is a random number that functions as a secret key, generated through an asymmetric cryptographic process, and is used to safeguard the ownership and management of cryptocurrencies. During the process of creating a VA wallet, first the private key is generated and then, from it, the public key, which is mathematically related to the former. The process, however, is impossible to realize in reverse (deducting the private key from the public one), providing a high level of security. The private key is the one that assigns to the holder the control of the funds associated with a given VA address.

8. **Cryptocurrency Wallets:** Software applications that allow interacting with the VA Blockchain in order to generate and/or store cryptocurrency addresses and their corresponding public/private key sets. It is an interface that allows users to manage, transfer, or receive VAs. There are several types of VA wallets.

9. **Hosted / Custodial wallets:** These are virtual wallets that are hosted on an external server (i.e., in "the cloud"), and are offered through VA wallet service providers. The name

refers to the fact that the private keys are not held by VA holders, but "in custody" of the service provider.

10. **Self-custody/ Self-hosted wallets:** These are the wallets that cryptocurrency users themselves keep in their possession, for their own use of the VAs associated with the addresses stored in them. These wallets may be virtual or hardware wallets.

11. **Software wallets:** These are downloadable desktop or mobile applications that can be kept on a desktop computer or on a mobile device (smartphone) to enable secure storage of keys on the device.

12. **Hardware wallets:** Wallet applications hosted on physical devices such as pen drives or USB, which allow the user to store his/her keys offline, on portable physical devices such as pen drives.

13. **Paper wallets:** These are sheets of paper or other material on which the cryptocurrency addresses, and the set of public/private keys used to manage the exchange of cryptocurrencies are printed, either in plaintext format or in the form of a QR code, by means of a VA wallet program. They are used for the storage and safekeeping of funds that will not be used or moved for a long time, since they offer a higher level of security, as they are not susceptible to cyber theft.

14. **"Seed words" or "Seed phrase":** They are used by many VA wallet applications to generate private keys from a single "seed," which takes the form of a mnemonic consisting of a sequence of between 12 and 24 words in different languages (English, Japanese, Korean, Spanish, Chinese, French, and Italian), which function as a backup for the wallet, allowing that in case of loss of control over the wallet (for example, due to theft, loss or technical malfunction of the device in which it is stored), it is possible to recreate it by entering the words in the order originally provided in the corresponding application.

15. **Virtual Asset Service Providers (VASPs):** As defined by the FATF, comprises any natural or legal person not covered elsewhere under the Recommendations who, as a business, carries out one or more of the following activities or transactions for/on behalf of another natural or legal person:

a. Exchange between virtual assets and fiat currency.

b. Exchange between one or more forms of VAs.

c. Transfer of VAs.

d. Custody or administration of VAs or instruments that allow controlling VAs; and

e. Participation in, and provision of financial services in connection with an issuer's offering or sale of a VA.

16. **VA/cryptocurrency exchange platforms (cryptocurrency exchanges):** These are those operated by persons or entities commercially engaged in the exchange of cryptocurrencies for fiat currency, funds, precious metals, or other cryptocurrencies (or vice versa), in exchange for a fee (commission). They generally accept a wide variety of payment methods (cash, wire transfers, credit cards or other cryptocurrencies) and are used to deposit or withdraw funds from VA accounts. They are included in the FATF definition of VASP.

17. **Mixers:** These are platforms that offer cryptocurrency users the possibility of obscuring the transaction chain in the Blockchain through the use of anonymity software tools that link multiple transactions to a single VA address and send them together in a way that makes them appear to come from a different address. The mixer or tumbler intervenes when it receives an instruction from the customer to send funds to a certain address. In order to conceal the origin and destination of the transaction, the mixer combines it with a complex and semi-random series of fictitious transactions, so as to prevent the transfer to the final destination from being associated with the address of origin.

18. **TOR (The Onion Router):** It is a distributed network of computers on the Internet that is used to conceal the real IP addresses (and therefore the true identity) of users by routing communications through multiple nodes (randomly chosen for each communication) around the world and shielding the data packets indicating the origin and destination of the communication in several layers of encryption.

19. **Hidden services:** These are web pages located on the "dark web," which can only be accessed through the use of anonymous communication systems such as TOR. This prevents their true location (IP address) from being identified, since they are masked by the "layered" routing provided by TOR. Communication between these sites and their users takes place through a "rendezvous point" that provides an additional layer of protection against traffic analysis.

20. **Encryption:** It is a data encryption method that consists of encoding the contents using a mathematical formula or algorithm that disorganizes them, so that if the corresponding key (called a "cryptographic key") is not available, they look like a set of alphanumeric characters with no meaning or reading logic.

21. **Blockchain analysis:** It is the process of inspection, identification, segmentation, and modeling for the visual representation of the public data contained in the Blockchain, in order to obtain useful information about those who carry out transactions with cryptocurrencies. This analysis is usually carried out by private companies that use proprietary algorithms to map the transactions carried out by cryptocurrency users and link them to each other.

22. **Open-Source Intelligence (OSINT):** A term that refers to the systematic collection, processing, and analysis of open access information. That is: information available to the general public without restrictions (on social networks, websites, search engines, news portals, public records, etc.).

23. **Spyware:** It is a type of malware (malicious program) designed to operate surreptitiously within a computer system and secretly record information. It can monitor and copy what is typed ("keylogger"), what enters or leaves the system, capture stored information, or even activate the computer's microphones or cameras.

24. **Electronic (or digital) evidence:** Information generated, stored, or transmitted by means of electronic devices that may be used as evidence in court.

B. INVESTIGATION AND IDENTIFICATION OF VIRTUAL ASSETS

25. Agencies responsible for conducting asset investigations on ML/TF schemes with VAs should have at their disposal the widest possible range of information, whether from their own sources, from exchanges with other national authorities, or from cooperation with third parties (e.g., in the private sphere). The information should include:

- Information collected by LEAs on persons under investigation for the suspected illicit activity on the Dark Web; identification of their pseudonyms or aliases; addresses of known cryptocurrencies or accomplices (and their pseudonyms or aliases); prior arrests or convictions; physical or electronic addresses, telephone numbers or email addresses that they may have used in connection with criminal activity.

- Information coming from the reporting institutions under the AML/CFT obligations, including information from suspicious transaction reports (STRs), as well as information obtained within the framework of know-your-customer (KYC) policies. This includes records of transactions carried out through VASPs, or of VASPs with traditional financial entities, or any other asset activity that may generate suspicions of the possible use of VAs to recycle funds of illicit origin.

- Information from regulatory bodies such as central banks, tax authorities, securities, or insurance regulators, etc.

- Information from open sources, including data such as the price of different cryptocurrencies, contact information or VASPs data, or links between the persons under investigation and potential identifying information (cryptocurrency addresses, wallets, links to criminal activity or criminals, etc.).

- Information held by national units specialized in cybersecurity, including reports on incidents involving the financial sector; information on malware aimed at identity theft or unauthorized collection of confidential and/or financial information (including data or programs used for VA management); and intelligence on the hacker community or on cybersecurity threats.

26. For the purposes of collecting information on persons under investigation who have activity or nexus with other persons of interest outside their borders, GAFILAT member country investigative agencies may consult the list of open sources in member countries compiled by the RRAG.

27. Special attention should be paid to the links between the possible illicit use of VAs for ML/TF and VASPs, through which the exchange between VAs and fiat currency usually takes place, since this is the vulnerability of any ML/TF scheme involving such assets, especially when significant amounts are involved, given that the (relatively) small nature of the cryptocurrency markets makes it more sensitive to massive inflows or outflows of funds.

28. Countries that have not yet done so should adapt their domestic regulations in order to impose registration and AML/CFT compliance obligations on VASPs, in accordance with the provisions of the new FATF Recommendation 15.

29. It should be borne in mind that VASPs that are subject to compliance with AML/CFT obligations constitute a source of information of great importance for ML/TF investigations with AML/CFT (since they can connect pseudo-anonymous transactions with VAs with identified customers) and, in addition, can facilitate the freezing, seizure, and confiscation of funds involved in or derived from illicit behaviors.

30. The STRs submitted by VASPs are very useful for the asset investigations covered by this guide, since they contain both information on transactions (issuing customer, beneficiary, addresses of the customer's wallets, balance in the wallets, date and time of the transactions, type of VA transferred, location of the transfer, canceled transactions, bank accounts registered or verified, and type of devices used); as well as customer information (name, user identification, IP address, physical billing address, e-mail address, date of birth, nationality, citizenship, economic profile and commercial activity).

31. For the detection of possible ML/TF schemes with VAs by means of VASPs, the "red flags" outlined in the FATF report on "Warning signs of money laundering and terrorist financing with virtual assets," published in 2020, should be taken as a reference.

32. Investigative agencies should pay particular attention to the activity of unregistered VASPs, or those that conceal their true location in order to circumvent locally

established AML/CFT compliance regulations, as such actors in the VA ecosystem often process a high percentage of illicitly sourced VA transactions.

33. In particular, the actions of mixers, tumblers, and online bookmakers operating outside the law should be investigated. In this regard, investigations related to the use of VAs should aim not only to identify and prosecute persons who exploit the use of cryptocurrencies to carry out criminal activities, but also to prosecute and eventually stop the activity of VASPs or other service providers when such activity is aimed at favoring or facilitating criminal operations.

34. It is important to keep in mind that, in general, criminal activity with VAs is concentrated in a few VASPs that facilitate the commission of ML/TF operations with cryptoassets. Therefore, if it is discovered which VASPs receive the highest volume of transactions with illicitly sourced VAs, investigations focused on them are more likely to generate positive results in terms of identification of persons involved in criminal conduct and seizure and confiscation of VAs.

35. It should be noted that the exchange between VAs and fiat currency can also be carried out through P2P exchange platforms, which are not covered by AML/CFT regulations in accordance with FATF Recommendation 15. Although, for the time being, such platforms process a low percentage of transactions with illicitly sourced VAs, operations that make it difficult to trace VAs and mask its origin, such as “chain hopping” or “coinjoin,” can be carried out through them.

36. Investigative agencies should be vigilant about the possible use, by the persons under investigation, of cryptocurrency kiosks or “Bitcoin ATMs” for the exchange of VAs and fiat currency. In this regard, it should be borne in mind that companies operating such ATMs fall under the FATF definition of VASP, so they are required to obtain information about their customers and report transactions considered suspicious.

37. The location of the ATMs allegedly used by the persons under investigation can be taken as a starting point for surveillance or monitoring of that person or his possible accomplices, either physically or by electronic means.

38. If the surveillance of the VA ATM makes it possible to determine the precise date and time of an exchange transaction carried out by the person under investigation, that data can be used to request information from the company responsible for that transaction, including the amount, the type of cryptocurrency traded, and the VA addresses of the participants. From this, a reconstruction of the origin and destination of the VAs involved can be performed.

39. For the purpose of tracing the origin and destination of VAs allegedly associated with illicit activity, the Blockchain offers an important source of information that is both relevant and reliable (since the decentralized structure of cryptocurrencies prevents the alteration of the records in the Blockchain).

Virtual asset tracking

40. From the data recorded in the Blockchain, investigative agencies can learn the complete transaction history of a given VA address, including the addresses of all the users with whom it carried out transactions and the date, time, and exact amount transferred (which can be useful as a search criterion when analyzing many transactions simultaneously); as well as the complete chain of transactions made by each VA since its creation and the IP addresses associated with each VA address (unless the user connects to the network through an anonymity tool such as a VPN or TOR system).

41. The analysis of this dataset, and its cross-checking with information obtained from other sources (especially if carried out by means of "Big data" IT tools) can be crucial to detect criminal activity with VAs, identify its perpetrators and obtain incriminating evidence. In this regard, the possibility of tracing the movements of VAs from and to a VASP is of particular relevance. If the VASP is registered in a jurisdiction that imposes AML/CFT obligations, it is likely to have information that allows the identification of the users involved in transactions with VAs.

42. For the purposes of present or future identification of persons under investigation for suspected illegal activity with VAs, it is important to register, sort, and categorize all VA addresses of cryptocurrency exchange platforms, mixers, online bookmakers, illicit markets on the dark web, persons already identified as likely suspects of engaging in illicit fund-generating activity, or ML/TF, among others, that have been identified in the course of investigations.

43. Investigative agencies should have as broad a base as possible of VA addresses with identified holders, as this facilitates the use of the Blockchain to allow the identification of other users who have contact with them.

Tools or techniques that can be used to identify virtual assets and related transactions

(i) Blockchain analysis

44. Blockchain analysis (or "Chain analysis") requires the use of the appropriate technological tools, in addition to the necessary technical knowledge to use them.

45. One tool that can be found in open-source versions freely available on the Internet are Blockchain explorers, network applications that operate as search engines in the VA ecosystem, allowing to locate addresses, transactions and other data linked to them.

46. There are also more sophisticated computer resources, specifically designed for the needs of investigative agencies, in the hands of private companies specialized in Blockchain analysis.

CARIN and other international organizations recommend the establishment of public-private cooperation instances by contracting the services of these companies, which have proven to be effective in asset investigations on ML/TF schemes with VAs.

47. In the latter case, it is necessary that authorities have agents or officials prepared to explain the findings of these companies in the framework of the judicial proceedings that take place in connection with the criminal behavior with VAs under investigation. In this regard, it is recommended that a good working relationship be maintained with the personnel of the companies providing the service, especially if they may be called upon to testify on how the findings presented were arrived at.

48. The information obtained from the Blockchain analysis can be complemented with "Open-Source Intelligence" (OSINT) techniques, which involve the systematic collection, processing and analysis of information available to the general public, without restrictions.

(ii) OSINT

49. In the context of asset investigations under this guide, OSINT can be used, for example, to obtain data on the holders of VA addresses already known to the investigators. To this end, attempts can be made to place the VA address in Internet search engines, as it is quite common for individuals engaged in illicit online trading (or terrorist organizations seeking to raise funds through VAs) to post their address (associating it with their online profile and pseudonym) in forums (such as Reddit, 4Chan, and 8Chan) or in the comments sections of specialized cryptocurrency or IT websites. In addition, websites specifically dedicated to the identification of VA users and the addresses associated with them, such as walletexplorer.com, can be consulted.

50. The same technique can be used to obtain information on the Dark Web, where there are multiple forums (Dread, Darknet Avengers, The Hub, Exploit.in) in which, taking advantage of the anonymity conferred by TOR login, people freely share information on hidden services, including their addresses, the products and services they offer, comments on the quality of the service, nicknames of the most (or least) successful traders, etc.

51. Secondly, it should be borne in mind that online pseudonyms often have a correlate either on the surface web (when the individual acts mostly on the dark web) or even in real life, which—if discovered—may allow linking the illicit activity to his or her real identity. In such a context, investigators can take advantage of mistakes that people often make when splitting their online identity from their real-life (secret) identity, such as not remembering to use anonymous surfing tools at some point, using the same VA address for illicit and licit activities, or using an e-mail address associated with their real name in connection with their online identity.

52. OSINT techniques can also be effective in obtaining information on unregistered VASPs providing services to persons engaged in illicit conduct with VAs, including mixers or P2P cryptocurrency exchange platforms, whether on the surface web or on the dark web, since they operate on the same reputation-based system as illegal online marketplaces.

53. In addition, OSINT techniques can be used to gather information that would allow to link persons suspected of being involved in illicit conduct generating funds with the suspected launderers of such funds. Finally, open-source information may be useful to better understand the lifestyle, the assets of the suspect, or the places where he/she resides or carries out his/her commercial or social activity.

54. It is also possible to obtain already processed information on persons of interest or suspected of being involved in illegal activities with VAs by resorting to the services of the so-called "Data brokers," which are companies dedicated to the collection and processing of information from multiple sources and the elaboration of detailed personal profiles.

55. In order to improve the effectiveness of asset investigations, it is recommended to combine the techniques described above with the use of traditional investigative measures, such as physical surveillance, inspection of waste discarded by the persons of interest, requests for reports, production orders and/or personal or house searches. Also, the questioning of witnesses, who can provide valuable insights into the lifestyle, activities and assets of suspects.

56. In this context, electronic means of surveillance can be used to obtain data relevant to investigations into unlawful behaviors involving VAs, such as the suspected person's connections to cryptocurrency exchange platforms, mixers, online gambling sites, P2P networks dedicated to the transfer of VAs, or cloud storage services. Similarly, the type of computing devices used by the persons under investigation, whether they have one or more online wallets, preferred methods of communication or whether they use public Wi-Fi connections or other electronic means that can be accessed by the authorities can also be ascertained in this way.

(iii) Network monitoring tools

57. Network monitoring software tools can be used for this purpose. These tools make it easy to obtain relevant information in different formats: large digital documents, images, audio files, videos and even telephone communications over the Internet. Even if the content of the intercepted communications is encrypted, it will be possible to capture the so-called "wrapper data," i.e. all those that do not form part of the content of the communication, but refer to the mechanisms for its execution (source and destination IP addresses, data volume, Internet nodes involved in the exchange of data packets, etc.).

58. The use of technological tools also facilitates the tracking of persons under investigation, either through the installation of GPS devices or by exploiting data from mobile applications on "smartphones" (for navigation, social media, online shopping or banking, etc.), associated with the GPS embedded in the cell phones themselves. In addition, prospective or retrospective monitoring can be carried out on the basis of the information that telecommunications companies collect as a result of the constant contact between cell phones and cell phone towers, linked to 3G or 4G operation.

(iv) Forensic analysis

59. In order to identify relevant information or evidence for ML/TF investigations with VAs, a forensic analysis of electronic devices owned by (or used by) the person under investigation is recommended. In this regard, evidence or information of interest may be found in desktop computers, laptops, tablets, smartphones, smart readers, portable GPS equipment, digital cameras, flash memories, SD cards, pen drives, removable hard disks, external servers in the "cloud;" compact disks and in smart devices included in the so-called "Internet of Things."

60. The important information or evidence that can be found in such devices includes:

- Evidence or indications of VAs use.
- Evidence or indications of contacts with cryptocurrency exchange platforms (either VASP or P2P platforms), mixers, online gambling sites, etc.
- Evidence or indications of use of cloud storage services.
- Evidence or indications of the use of anonymity tools (TOR, I2P, VPNs).
- Evidence or indications of the use of encryption tools.
- Keys or passwords to access information stored in the cloud or to disable encryption.
- Evidence or indications of communications with other suspicious persons (holders of funds of illicit origin, terrorist organizations, money launderers, etc.).
- Property documentation or other relevant evidence in digital format (company incorporation documents, accounting records, images or data on assets, agendas, etc.).

Special investigative techniques

61. When the characteristics of the operation under investigation so require (due to its complexity or the difficulty of obtaining relevant information or evidence by traditional means),

the use of special investigative techniques such as undercover actions may be used, always within the framework of the procedural legislation in force in each country.

62. In this regard, it is possible to take advantage of the evasive programs and techniques used by criminals to anonymously carry out their criminal activities in cyberspace (such as the use of tools like TOR or VPNs to surf the Internet anonymously, or the assumption of alternative identities on the Internet) to infiltrate LEA agents within criminal organizations operating in cyberspace, or to interact with persons offering illegal goods or services on the Internet.

63. In these cases, given that Blockchain analysis tools can also be used by criminals, it is recommended to previously generate a transaction history related to the "profile" to be assumed by the agent who intends to act covertly on the Internet by carrying out transactions with VAs.

Use of spyware

64. Another advanced investigative technique that may be used in the context of complex ML/TF investigations involving VAs is the use of spyware or "Trojans" by LEAs. Another advanced investigative technique that may be used in the context of complex ML/TF investigations involving VAs is the use of spyware or "Trojans" by LEAs. This tool can be used to remotely access information or digital evidence whose physical location is unknown or impossible to access effectively (for example, to obtain the passwords needed to access the contents of encrypted documents, or information stored on external servers); to monitor communications made over the Internet, using communication technologies that make interception by traditional means impossible (VoIP or encrypted messaging systems); to carry out acoustic or audiovisual surveillance, using the spyware to remotely enable microphones or cameras of devices in possession of (or in the vicinity of) the persons under investigation; or to locate or follow in real time the persons under investigation.

65. The implementation of state use of spyware requires three stages: *(i)* analysis of the target's use of the networks, to determine which platforms or applications he/she uses (and the possible vulnerabilities of such platforms or applications that can be exploited to enter the system); *(ii)* compromise of the platform through the most appropriate "exploit," in order to introduce the spyware; and *(iii)* monitoring of the information captured from the target.

66. The computer tools necessary for the use of spyware for investigative purposes can be obtained through the State's own technological development, or by acquiring the programs offered by private companies dedicated to the development and commercialization of spyware for State use.

Challenges related to the use of spyware

67. In order to reduce the risk of proliferation inherent in the use of spyware, it is recommended to adopt mitigating measures such as the implementation of technical measures to prevent the rediscovery of the vulnerability to introduce the spyware; the notification to the corresponding (state) authority of the discovery of a vulnerability, and the request for authorization to exploit it; and the regulation of the dual use of vulnerabilities.

68. Likewise, for the purpose of implementing the state use of spyware, the "dropper/payload" model should be adopted, which consists of the use of a (confidential) software to intrude into the target's system or device (the "dropper"), and a different one (the "payload") to capture the information or digital evidence included in the judicial authorization, whose operation can be disclosed or divulged to the defense of the eventual defendants.

69. In all cases, it must be ensured that the software tool is encrypted based on the specific characteristics of the target system (in order to prevent it from being downloaded by mistake to another system or device), and that it is programmed to self-destruct once the investigative measure is completed.

70. All steps and actions taken to introduce the spyware into the target's equipment should be documented. In addition, the characteristics of the program used to carry out the monitoring and the changes that this program must make to the system in order to allow the interception and avoid detection must be recorded. This, in order to be able to demonstrate that the evidence has not been destroyed or altered.

71. In view of the potential impact that the use of spyware for investigative purposes may have on the right to privacy of citizens, it is recommended that the use of this measure be expressly regulated in the procedural regulations, establishing as clearly as possible the requirements for the use of such a computer tool and the precautions to be taken in its implementation, in accordance with the legal principles in force in each State. If the state use of spyware is carried out by analogically applying other procedural rules or by virtue of the principle of freedom of evidence, the adoption of certain precautions is suggested so that the investigation measure through the use of spyware affects as little as possible the right to intimacy and privacy of the persons who are the object of the investigation. Among them:

- That the judicial authorization specifies: (a) the devices and data or digital content subject to the measure; (b) the scope of the measure; and (c) the manner in which the relevant information is to be accessed and collected.

- That the use of this method be limited only to the investigation of serious crimes.

- That a certification process be established for the software used, providing for the possibility of verifying its operation to ensure impartiality and confidentiality.

- That defense attorneys can access the documentation related to the investigative measures carried out by means of computer programs and can verify whether the programs used have been certified.

- That the obligation to uninstall the programs at the end of their use be established.

C. SEIZURE AND CONFISCATION OF VIRTUAL ASSETS

Overview – Centralized and decentralized VAs

72. For the purposes of seizure or confiscation of VAs, a distinction must be made between centralized and decentralized virtual currencies. In the first case, the measure on VAs can be carried out by addressing a court order to the central administrative authority that maintains exclusive control over the assets, ordering the freezing or seizure of the funds.

73. When dealing with decentralized currencies (such as cryptocurrencies), the non-existence of a central bank or similar institution that can freeze the funds in compliance with a court order determines that, in many cases, the intervening state authority will have to carry out the seizure or confiscation by its own means, without the intervention of any intermediary.

74. One exception is in cases where the VAs subject to seizure or confiscation are housed in a "custodial" wallet (where the private key that controls the movement of the VAs is in the hands of a VASP and not the holder). In this case, as in the case of centralized currencies, the asset measure can be carried out by addressing a judicial order to the VASP, ordering the freezing or seizure of the assets.

75. When the private keys controlling the VAs are in the hands of their holders, on the other hand, the freezing of funds is not feasible. This is because, in practice, any person holding the private key can dispose of the funds associated with the address of the VA corresponding to that key, while there may be multiple copies of each private key, stored in different places and in different formats, and to which different persons may have access. Therefore, as long as the cryptocurrencies are in the wallet of the suspected person, even if that person is in custody, any third party with the key can irrevocably transfer the VAs.

Securing measures

76. In this case, the only way to safeguard the State authorities' ability to seize VAs is to transfer them to a wallet controlled by them as soon as possible, so as to prevent a third party from removing the funds before they can pass into the hands of the State. To this end,

it is necessary to obtain either the private key associated with the VA address corresponding to the assets to be seized or confiscated, or the "seed phrase" that makes it possible to reconstruct the wallet in which the VAs are housed.

Policies or protocols

77. It is recommended that the agencies that may have to carry out this type of measures establish beforehand internal policies or protocols that regulate the seizure of VAs and their subsequent treatment. This should include, as a minimum:

- The identification of the officials authorized to carry out seizures or transactions with VAs.
- The details of the internal and external notifications that need to be made when a case involves VAs.
- Standard procedures for collecting and preserving electronic evidence.
- The chain of custody protocols that should govern all devices that may contain electronic evidence.

Preparatory or pre-seizure measures for seizure of VAs

78. As part of the preparation prior to the seizure or confiscation procedure, it is recommended that the type of cryptocurrencies and wallets operated by the person under investigation be determined before proceeding. The identification of the wallet is necessary, since not all wallets support multiple cryptocurrencies, and the differences between the various types of wallets influence the technical methodology to be used to transfer the VAs contained therein, for the purposes of seizure and confiscation. Moreover, the identification of the specific class of cryptocurrency(ies) involved is essential, since these can only be transferred to an address corresponding to their own Blockchain.

79. Such information can be obtained in various ways. For example, if a seller's activity on an illicit online marketplace is investigated, the type of VA accepted as payment is going to be listed in his profile. The data can also be obtained through OSINT techniques, Blockchain analysis, etc.

80. It is also recommended that certain "best practices" be adopted in anticipation of a search that may result in VA seizure, including:

- Being aware of when the suspected person's devices are logged in or in use (by determining patterns of behavior, network monitoring, surveillance, or undercover action, as appropriate).

- Constant monitoring of the target's activity and the behavior of their VAs address(es).

- Prepare for the possibility of encountering accounts that require two-factor authentication.

- To the extent possible, ensure access to fingerprints or other biometric data that would allow access to devices protected by such means (e.g., by having the holder of such devices in custody or having authorization to arrest the holder during the search and compel the opening of the devices).

81. Given the importance of speed in the seizure of VAs, it is important to obtain judicial authorization to carry it out before proceeding with any search that may result in the discovery of the wallet(s) of the person under investigation. It is also important that the judicial authorization includes the following:

- Permission to seize, in the course of the search, all data storage devices that may be found in the home or offices of the person under investigation (removable hard disks, CDRs, DVDRs, memory sticks, pendrives, etc.). This, since they can be "hardware wallets" or otherwise contain important information in digital format, such as the "seed words" that allow reconstructing a VA wallet, the passwords used by the user to access a hybrid wallet, etc.

- Authorization so that, in the event that during the search of a home—or the arrest of a suspect—it is found that the suspect's computer or smartphone or tablet is unlocked and active, this circumstance can be used to analyze its contents in search of VA wallets. This is because the ideal opportunity to seize cryptocurrencies is when the wallet containing the private key(s) is open, or when the password to open it or the "seed phrase" that allows it to be reconstructed is found during registration.

- Permission to isolate the persons present during the procedure in order to prevent them from connecting to the Internet or making contact with the outside world, until the seizure has been completed. This, in order to prevent that while the measure is being developed, any accomplice of the person under investigation transfers the funds to be obtained.

Registration or search of domiciles

82. In planning home searches that may result in seizure or confiscation of VA, consideration should also be given to the need to neutralize, as soon as possible, any possibility that the person under investigation destroys, alters or conceals information useful for accessing the VA wallet (handwritten passwords or pins, hardware wallets, etc.) transfer its contents or give notice to a third party to do it for him before the authorities access it.

83. Pre-seizure or confiscation planning also includes the generation of VA addresses controlled by the LEA or authority in charge of the proceeding in accordance with local law. For this purpose, it is recommended that the public and private keys be generated with a wallet application on a computer not connected to the Internet, and then use a Blockchain browser to verify that there is no record of the public address on it. Finally, the public key (but not the private key) must be transferred from the initial computer to a laptop equipped with the necessary applications to perform a VA transfer, which is the one that is going to be taken to the procedure to realize the seizure.

84. If a search of a property (whether a home, an office or even cars, boats, etc.) is carried out in the context of an investigation for possible illicit use of VAs that may lead to their seizure, emphasis should be placed on the detection of different elements that may be relevant either as evidence, as information leading to evidence, or as a key to enable the seizure or confiscation of VAs of illicit origin. For instance:

- Computers or other devices containing information in electronic format, such as cell phones, tablets, pen drives, removable hard disks, etc.
- VA wallets, either in virtual format (such as applications within the aforementioned electronic equipment) or in physical format, such as hardware or paper wallets.
- Information that allows access to the wallets or the transfer of VAs, such as passwords or pins to access encrypted wallets or online wallets hosted in external servers, VA addresses and—especially—the private keys or "seed words."

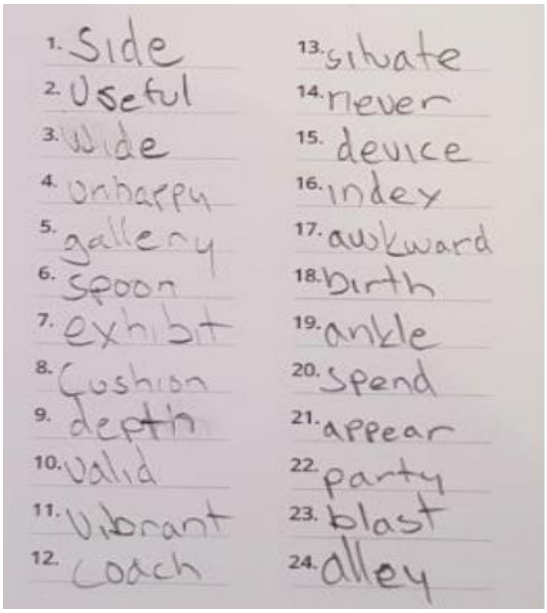
Wallets

85. Virtual wallets (desktop or mobile) are generally identified by an icon on the computer desktop or cell phone home page. Otherwise, they can be located by using the computer's search engine to identify the files with the word "wallet" or a ".dat" extension (although in some cases, the user may have saved them with another name or extension). The following image illustrates the icons of some of the most popular wallets:

86. If a paper wallet is discovered (as the one illustrated in the following image), it is possible to verify the existence of funds by scanning the QR code and using a mobile application to check it against the information available on the Blockchain of the cryptocurrency in question. The same app can be used to transfer the VAs to a wallet controlled by the authorities, thus completing the seizure of the funds.

87. Since VA wallets are usually protected by passwords (to gain access) or by pins (to enable transactions), the searched location—and especially the environment around the location of the investigated person's computer—should be carefully checked for handwritten notes, notebooks, journals, diaries, sticky notes, etc., in which the passwords or pins necessary to carry out transactions may have been entered.

88. If, during the search, the investigators find the "seed words" (as shown in the following image), they can use them to reconstruct the wallet (including its private key) and thus transfer the VAs to a state-controlled wallet, thus completing the seizure. To this effect, 12 or 24 words are introduced and at the end of the last one, an exact copy of the original wallet is obtained.



89. Not all wallets follow the same protocols. Therefore, depending on the type of wallet in question, its reconstruction from the seed phrase may yield the same result as if accessing the original (all the VAs contained in it), or an empty wallet. There are applications that make it possible to determine what type of result the reconstruction of a given wallet by means of the seed phrase will produce.

90. It is also useful to find the "Returning customer number" with which some VA mixers identify people who use their services more than once. Although this number does not facilitate the seizure of cryptocurrencies of illicit origin, it is useful as evidence of the use of mixers, as well as—potentially—to identify the specific mixer that processed the VAs of the person under investigation and allow an eventual traceability through "Chain analysis" techniques.

91. Due to its greater technical difficulty, it is preferable that the seizure of VAs be carried out by specialized and trained personnel, since, in addition, speed may be essential to ensure the success of the seizure. Therefore, it is necessary that those carrying out the seizure are aware of the different varieties of VA wallets and the security mechanisms they have.

92. The best way to carry out the seizure of VAs contained in a wallet controlled by the person under investigation is to do so while the wallet is unblocked and in use. To this effect, it should be ensured, if possible, that the procedure aimed at obtaining control over the device containing the wallet is carried out in such a way as to surprise the person under investigation when he/she is using it.

93. Once access to the wallet has been obtained, it is essential to take the necessary measures to ensure that they are kept on and in use, in order to prevent them from being blocked again, hindering access to the wallet or protecting the contents by means of encryption.

94. It is important to keep in mind that a cryptocurrency wallet may host multiple addresses (in some cases, even of different cryptocurrencies) containing VAs potentially subject to seizure.

95. Digital files containing virtual wallets (desktop or mobile) must be exported from the device of the person under investigation with the help of a computer forensic tool. A digital image of the entire wallet must be made, as well as copies or digital images (as the case may be) of the private keys or seed words found in paper documents or in text or Word files. They should then be imported into the computer of the investigative agency that has the necessary software to carry out the seizure.

Perfection of the seizure

96. The actual seizure takes place when the VAs are transferred from the address of the person under investigation to the one controlled by the competent authority, for which purpose the computer used by the agents must be connected to the Internet and, where appropriate, also synchronized with the corresponding Blockchain.

Additional recommendations for the effective seizure and confiscation of VAs

97. In relation to the seizure and confiscation of VAs, it is recommended to adopt a number of best practices, including the following:

- As far as possible, have the state address(es) converted in advance to QR format, in order to avoid typing errors (especially if the seizure is conducted with mobile wallets, where it is more feasible to make such errors).
- Otherwise, it is recommended to double, or triple check the destination address individually before making the transfer.
- Use the "sweep" function of VA wallets, which simply transfers the entire balance of the wallet being seized to the destination wallet (in this case, the one previously set up by the authorities carrying out the seizure).
- For the purpose of speed, set the highest fee that is authorized, in order to ensure that Blockchain miners place it in the nearest block and that it is realized more quickly.
- If state-controlled addresses are stored in paper wallets, ensure that the private keys are not visible, or that they are multi-signed, in order to reduce the risk of theft of seized VAs.
- When the minutes or report on the seizure of VAs are drawn up, the private key or the seed phrase that enables their transfer should not be recorded in any case.
- Once the seizure has been completed, the balance of the previously emptied VA address(es) should be periodically verified, since it may happen that transfers or payments are received after the procedure.

98. If the wallet is blocked and the password required to access it cannot be found, the device containing it must be seized (as would be done with any other device containing relevant digital evidence), adopting the necessary precautions established in the protocols on the treatment of electronic evidence. Subsequently, and bearing in mind the need to act as quickly as possible, the relevant investigative measures should be taken to try to obtain the passwords and seize the VAs associated with it.

99. If the seizure of VAs proves impossible, the information contained in the Blockchain can be used to establish the value of the funds subject to confiscation and proceed to the seizure of assets of equivalent value.

Post-seizure steps

100. Once VAs have been seized, the choice is between: (a) holding them until the final confiscation order is issued; or (b) converting them immediately (or within a short period of time) into fiat currency. In order to choose one or the other option, the risk of VAs depreciation due to the fluctuation in the cryptocurrency price, on the one hand, and the security risks and costs associated with the storage of VAs, on the other hand, must be taken into account.

Management of VAs during the course of the process

101. It may be desirable to establish a procedure for consultation with the previous holder of the seized VAs (i.e., the person under investigation) in order to obtain his or her written opinion as to whether he or she prefers that they be kept in their original state or converted into fiat currency. In this way, if they are to be returned at a later date, the State is released from liability for any loss of value.

102. A fixed time frame for the conversion of seized VAs into fiat currency (e.g., three days) can also be established in advance (either through a regulation or written internal policies), so that the decision to convert seized VAs into fiat currency does not depend on a judgment of their economic convenience.

Liquidation of the VAs

103. Once the decision to liquidate the seized or confiscated VAs has been taken, the sale may be carried out directly or at public auction in an attempt to maximize the value obtained, in accordance with the provisions of the applicable legislation or as decided by the competent authority. An agreement may also be reached with a private operator specialized in the exchange of VAs (i.e., a VASP) to undertake the conversion of cryptocurrencies into fiat currency.

104. If it is decided not to liquidate certain seized VAs (e.g., private currencies such as Monero), because it is considered that there are no legitimate uses for them in the market, the necessary security measures should be taken to ensure effective permanent storage of the VAs in question.

105. It is recommended that the seized VAs be stored in cold storage wallets (e.g., a hardware wallet, or a virtual one, but contained in a computer not connected to the Internet, or even in paper wallets). Similarly, seized VAs may be stored in multi-signature wallets, so that they cannot be stolen by illicitly obtaining a single private key.

106. It is also recommended that a list of passwords for access to each of the electronic devices (including computers and smart phones), encrypted external storage units and seized VA wallets be kept in the hands of a specifically designated official, restricting access to them as much as possible. Seed phrases, passwords, private keys, pins and VA addresses obtained can be kept in text files, in a designated folder for each seized VA on an external storage drive (e.g., a removable hard drive), if possible encrypted for security. These drives should be kept offline in a specific secure location until required by the competent authorities to receive or transfer the VAs.

D. CLOSING REMARKS

Multidisciplinary approach

107. In order to achieve greater efficiency in the investigation of ML/TF schemes involving VAs, it is essential to adopt a multidisciplinary approach that combines the expertise of agents with experience in asset investigations with that of personnel from specialized cybercrime or cybersecurity units. The formation of multidisciplinary groups composed of professionals from both areas is strongly recommended, in line with FATF Recommendation 30.

108. It is also important that the agencies responsible for investigating this type of illicit conduct act in coordination with prosecutors or judicial operators trained in the field, especially with regard to the collection, analysis and processing of electronic evidence and the seizure and confiscation of VAs; as well as the use of advanced technological investigation techniques or tools, such as chain analysis, OSINT, digital undercover agents and the use of spyware, where their use is permitted by local procedural legislation.

International cooperation

109. The transnational nature of the Internet and the VA ecosystem makes international cooperation an essential element of asset investigations into the criminal behavior associated with them.

110. It is recommended that the agencies or authorities responsible for investigating ML/TF schemes with VAs use all available means to connect with their counterparts abroad, including cooperation mechanisms between law enforcement agencies (INTERPOL, EUROPOL); contact points for the exchange of information related to the seizure and confiscation of illicit assets (RRAG, CARIN, ARIN networks, StAR and GFPN); contact points for the exchange of information linked to cybercrime (Inter-American Cybercrime Cooperation Portal and G-7 24/7 Contact Network); channels for international legal cooperation such as IberRed; networks for the exchange of financial intelligence information gathered by FIUs (Egmont Group); as well as requests for mutual legal assistance.

111. It is also important that direct contact be established with authorities in the foreign counterpart who are familiar with the subject matter of the cooperation request (investigations of illicit activity with VAs) and—in general—with the issue of digital evidence, as well as the establishment of informal channels of communication with similar agencies in other countries to facilitate collaboration.

112. It is strongly recommended to use the RRAG for identifying assets and persons abroad that may be relevant in the framework of an investigation into ML/TF schemes using VAs and for learning about criminal proceedings underway in other countries. To this end, general, social, tax, property, and financial data may be requested through the RRAG's secure platform, either to enrich the information available to investigators in the requesting country, or to facilitate the preparation of requests for international legal assistance with accurate data, in order to increase the chances of success.

113. This platform allows for the secure exchange of information between RRAG countries and the 54 jurisdictions belonging to the CARIN Network. In addition, RRAG contact points can access information held by other international organizations involved in asset confiscation, such as the Camden Asset Recovery Inter-Agency Network (CARIN), the Global Asset Recovery Focal Point Network (GFPN), and Interpol's Stolen Asset Recovery (StAR) Initiative.

114. Also, information collected by ARIN networks around the world, including the Asset Recovery Inter-Agency Network for Asia Pacific (ARIN-AP) and West and Central Asia (ARIN-WCA), the Caribbean Asset Recovery Inter-Agency Network (ARIN-CARIB), the Asset Recovery Inter-Agency Network for Eastern Africa (ARIN-EA), Southern Africa (ARIN-SA) and West Africa (ARIN-WA) can also be accessed through this channel.

115. Information can also be exchanged through the Inter-American Cooperation Portal on Cyber-Crime, which is managed by the Technical Secretariat of the Meeting of Ministers of Justice and Other Ministers and Attorneys General of the Americas (REMJA) of the OAS. For this purpose, the Department of Legal Cooperation of the Secretariat for Legal Affairs of the OAS maintains an updated directory of criminal prosecution and police authorities that serve as contact points for international cooperation on cybercrime and electronic evidence.

116. It is recommended that states that have not yet done so join, as soon as possible, the G-7 "24/7 High Tech Crime Contact Network" and strengthen mechanisms for information exchange and cooperation with other international organizations and agencies on cybercrime, such as the United Nations, the Council of Europe, the European Union, the Asia-Pacific Economic Cooperation (APEC), the Organization for Economic Cooperation and Development (OECD), the Commonwealth, and INTERPOL.

Capacity building and enhancement

117. Given that the investigation of the illicit use of VAs involves the analysis of complex technologies and, therefore, requires the development of new investigative techniques and the acquisition of new resources and capabilities, training programs should be implemented for the widest possible range of personnel, so that they acquire the minimum knowledge necessary to carry out—or, at least, not to compromise—asset investigations related to the illicit use of VAs.

118. In this context, it is necessary to provide training to:

a. Investigators, regarding the new technologies involved in asset investigations on the illegal use of VAs.

b. Police officers in general on how to recognize and react to the existence of digital evidence relevant to those kinds of investigations; and

c. Forensic investigators regarding the new technologies involved.

119. Not all investigative personnel need to specialize in the use of VAs. However, it is necessary to have a number of experts (proportional to the size of the jurisdiction) who are trained to reconstruct a chain of transactions on the Blockchain and/or to seize or confiscate VAs. Other personnel should only have the minimum knowledge necessary to recognize clues about the possible use of cryptocurrencies if they come across them in the course of an investigation or when conducting a search, as well as to contact specialized law enforcement officers within their jurisdiction.

120. In this context, it is important that a sufficient number of agents receive training in the use of forensic tools for traceability of VAs that are available on the market or, alternatively, those developed internally by each country, if it decides to do so.

121. Similarly, the relevant authorities (be they police agencies or competent prosecutors' offices) must be trained to handle the different types of VA wallets that may be used in these procedures, as well as the cybersecurity issues inherent to the management of the seized assets.

122. In view of the possibility that agents not belonging to specialized units may come across cryptocurrencies in compliance with search warrants, etc., it is necessary that LEA personnel who may potentially find themselves in such a situation know how to recognize at least the most important features of the use of VAs (QR codes, seed phrases, public or private keys, different cryptocurrency address formats and different types of wallets, passwords, pins, etc.). Also, on a more general level, they should be able to recognize devices that may contain digital evidence.

123. Training of personnel can be carried out through the organization of training programs, the development of handbooks, exchange programs, and/or participation in international conferences or seminars.

124. In order to expand the scope of knowledge on VAs as much as possible among law enforcement personnel, it is advisable to distribute reference material (brochures, instructions) containing detailed pages or applications related to VAs, exchange platforms, payment processors, and cryptocurrency wallet service providers, images of seed phrases, QR codes, paper or hardware wallets, and VA ATMs, etc.

Public-private cooperation

125. Finally, it is also recommended that public-private cooperation with private sector actors specialized in these new technologies be implemented in order to ensure that the LEAs and the Public Prosecutor's Office units with competence in this area are kept up to date with new developments in this field.

ANNEX 2: COMPARATIVE LEGISLATION ON THE USE OF ADVANCED INVESTIGATIVE TECHNIQUES (DIGITAL UNDERCOVER AGENT / SPYWARE)

1. This section accompanies, for the purpose of illustration, the parameters established in comparative legislation with respect to the regulation of advanced investigative techniques (in particular, the computer or digital undercover agent and the state use of spyware).

2. For this purpose, an article that is part of the Model Legislative Texts of the Caribbean Community (ITU/CARICOM/CTU Model Legislative Texts) is reproduced, since it is the first international multilateral instrument that expressly contemplates the incorporation of the use of "remote forensic software" (i.e., spyware) as an investigative tool.

3. Likewise, the relevant articles of the Spanish Criminal Procedure Law (LEC) are reproduced, in accordance with the reform introduced by Organic Law (LO) 13/2015. In this last reform, on the one hand, the concept of the "undercover computer agent" was incorporated into Spanish procedural law in paragraph 6 of article 282 bis, which already regulated the "traditional" undercover agent.

4. Moreover, the contents of Chapters IV to X of the LEC are reproduced, which include provisions on the interception of telephone and telematic communications, the recording of oral communications by means of electronic devices, the use of technical devices for tracking, locating, and capturing images, the recording of massive information storage devices, and the remote recording of computer equipment.

5. Although these provisions only expressly refer to the use of forensic software in connection with the remote recording of computer equipment (Chapter IX, art. 588 septies a), the above mentioned chapters are transcribed in their entirety because, on the one hand, the regulation does not exclude the possibility of using spyware also for the interception of telematic communications, the recording of oral communications, the tracking and or the capture of images;[206] and, on the other hand, it is valuable for the thoroughness with which the requirements to carry out this kind of measures have been established, in order to minimize the potential impact on the right to privacy of citizens resulting from the use of spyware.

[206] Refer to: Blanco, Hernán: *"El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre,"* [Hacking with a judicial order in the Spanish procedural law from Organic Law 13/2015 of October 5], in InDret, No. 1/2020, January 2020.

Model Legislative Texts of the Caribbean Community (ITU/CARICOM/CTU Model Legislative Texts): Model Policy Guidelines and Legislative Texts on Cybercrimes – HIPCAR:

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 cannot 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 by the use of such software need to be protected again 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 are 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 be 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].

CRIMINAL PROCEDURE LAW – SPAIN: PROVISIONS INCORPORATED BY ORGANIC LAW 13/2015:

Section 282 bis:

1. For the purposes provided for in the preceding article and in the case of investigations involving organized crime activities, the competent investigating judge or the Public Prosecutor's Office, immediately reporting to the judge, may authorize officers of the Judicial Police, by means of a well-founded resolution and taking into account their need for the purposes of the investigation, to act under cover of assumed identity and to acquire and transport the objects, effects, and instruments of the crime and to defer their seizure. The assumed identity will be granted by the Ministry of the Interior for a period of six months, extendable for periods of the same duration, being legitimately authorized to act in everything related to the specific investigation and to participate in the legal and social traffic under such identity. The resolution by which it is agreed shall state the real name of the agent and the presumed identity under which he or she will act in the specific case. The resolution will be confidential and must be kept outside the proceedings with due security. The information obtained by the undercover agent must be brought to the attention of the person who authorized the investigation as soon as possible. Likewise, said information must be provided to the process in its entirety and shall be thoroughly evaluated by the competent judicial body.

2. Judicial Police officers who have acted in an investigation under a false identity in accordance with the provisions of paragraph 1, may maintain that identity when testifying in the process that may arise from the events they may have participated in and provided that this is agreed by a grounded judicial decision, being also subject the provisions of Organic Law 19/1994, of December 23.

No officer of the Judicial Police may be forced to act as an undercover agent.

3. When the investigative actions may affect fundamental rights, the undercover agent must request the authorization from the competent judicial body as established by the Constitution and the Law, as well as comply with the other applicable legal provisions.

4. For the purposes indicated in paragraph 1 of this article, organized crime shall be considered as the association of three or more persons to carry out, on a permanent or reiterated basis, conducts aimed at committing any or some of the following crimes:

(a) Offenses involving the procurement, illicit trafficking of human organs and transplantation thereof, provided for in Article 156 bis of the Criminal Code.

(b) Kidnapping of persons, as provided for in articles 164 to 166 of the Criminal Code.

(c) Trafficking in human beings, as provided for in article 177 bis of the Criminal Code.

(d) Crimes related to prostitution provided for in articles 187 to 189 of the Criminal Code.

(e) Offenses against patrimony and against the socioeconomic order provided for in articles 237, 243, 244, 248, and 301 of the Criminal Code.

(f) Crimes related to intellectual and industrial property provided for in articles 270 to 277 of the Criminal Code.

(g) Crimes against the rights of workers provided for in articles 312 and 313 of the Criminal Code.

(h) Crimes against the rights of foreign citizens provided for in article 318 bis of the Criminal Code.
(i) Crimes involving trafficking in endangered species of flora or fauna provided for in articles 332 and 334 of the Criminal Code.
(j) Crimes involving trafficking in nuclear and radioactive material provided for in article 345 of the Criminal Code.
(k) Crimes against public health provided for in articles 368 to 373 of the Criminal Code.
(l) Currency counterfeiting offenses, provided for in article 386 of the Criminal Code, and counterfeiting of credit or debit cards or traveler's checks, provided for in article 399 bis of the Criminal Code.
(m) Trafficking and deposit of arms, ammunition or explosives, provided for in articles 566 to 568 of the Criminal Code.
(n) Terrorism offenses provided for in articles 572 to 578 of the Criminal Code.
(o) Crimes against the historical patrimony foreseen in article 2.1.e of Organic Law 12/1995, of December 12, 1995, for the repression of smuggling.
5. The undercover agent shall be exempt from criminal liability for those actions that are a necessary consequence of the development of the investigation, as long as they keep due proportionality with the purpose of the same and do not constitute a provocation to the crime. In order to be able to proceed criminally against the same for the actions carried out for the purposes of the investigation, the Judge competent to hear the case shall, as soon as he becomes aware of the actions of any undercover agent, request a report on such circumstance from the person who authorized the alleged identity, in view of which he shall decide what he deems appropriate.
6. The investigating judge may authorize officers of the Judicial Police to act under assumed identity in communications maintained in closed channels of communication for the purpose of clarifying any of the crimes referred to in paragraph 4 of this article or any of the crimes provided for in article 588 ter a. The undercover computer agent, with specific authorization to do so, may himself exchange or send illicit files due to their content and analyze the results of the algorithms applied for the identification of such illicit files.
7. In the course of an investigation carried out by means of an undercover agent, the competent judge may authorize the taking of images and the recording of the conversations that may take place during the planned meetings between the agent and the person under investigation, even if they take place inside a home.

CHAPTER IV
Common provisions on the interception of telephone and telematic communications, the recording of oral communications by means of electronic devices, the use of technical devices for tracking, locating, and capturing images, the recording of massive information storage devices and the remote recording of computer equipment.

Article 588 bis a. *Guiding principles.*
1. During the investigation of the cases, any of the investigative measures regulated in this chapter may be agreed upon, provided that judicial authorization is granted in full compliance

with the principles of specialty, suitability, exceptionality, necessity, and proportionality of the measure.
2. The principle of specialty requires that a measure be related to the investigation of a specific crime. Technological investigative measures aimed at preventing or discovering crimes or clearing suspicions without an objective basis may not be authorized.
3. The principle of suitability shall serve to define the objective and subjective scope and duration of the measure by virtue of its usefulness.
4. In application of the principles of exceptionality and necessity, the measure may only be granted:
(a) when other measures less burdensome to the fundamental rights of the investigated or accused person and equally useful for the clarification of the event are not available for the investigation, or
(b) when the discovery or verification of the event under investigation, the determination of its author or authors, the ascertainment of their whereabouts, or the location of the proceeds of crime would be seriously hindered without recourse to this measure.
5. The investigative measures regulated in this chapter shall only be considered proportionate when, taking into consideration all the circumstances of the case, the sacrifice of the rights and interests affected resulting from their adoption is not greater than the benefit to the public interest and to third parties. For the weighing of the conflicting interests, the assessment of the public interest will be based on the seriousness of the events, their social transcendence or the technological scope of production, the intensity of the existing evidence and the relevance of the result pursued with the restriction of the right.

Article 588 bis b. *Request for judicial authorization.*
1. The judge may order the measures regulated in this chapter ex officio or at the request of the Public Prosecutor's Office or the Judicial Police.
2. When the Public Prosecutor's Office or the Judicial Police request a technological investigation measure from the investigating judge, the request must contain:
1. The description of the event under investigation and the identity of the investigated person or any other person affected by the measure, provided that such data are known.
2. The detailed statement of the reasons justifying the need for the measure in accordance with the guiding principles set forth in article 588 bis a, as well as the indications of criminality that have been revealed during the investigation prior to the request for authorization of the event in question.
3. The identification data of the investigated or accused and, where appropriate, of the means of communication used to enable the execution of the measure.
4. The extent of the measure with specification of its content.
5. The investigative unit of the Judicial Police that will be in charge of the intervention.
6. The form of execution of the measure.
7. The duration of the requested measure.

8. The reporting institution that will carry out the measure, in case it is known.

Article 588 bis c. *Court Decision.*
1. The investigating judge will authorize or deny the requested measure by self-motivation, after hearing the Public Prosecutor's Office. This resolution will be issued within a maximum period of twenty-four hours from the filing of the request.
2. Whenever it is necessary to resolve on the fulfillment of any of the requirements expressed in the previous articles, the judge may require, with interruption of the term referred to in the previous paragraph, an extension or modification of the terms of the request.
3. The judicial decision authorizing the measure shall specify at least the following:
(a) The punishable act under investigation and its legal description, with an expression of the rational indications on which the measure is based.
(b) The identity of the investigated persons and of any other person affected by the measure, if known.
(c) The extent of the measure taken, specifying its scope, as well as the reasoning regarding compliance with the guiding principles set forth in article 588 bis a.
(d) The investigative unit of the Judicial Police that will be in charge of the intervention.
(e) The duration of the measure.
(f) The form and periodicity with which the applicant will inform the judge about the results of the measure.
(g) The purpose of the measure.
(h) The reporting institution who will carry out the measure, if known, with express mention of the duty of collaboration and secrecy, where appropriate, under penalty of incurring a crime of disobedience.

Article 588 bis d. *Secrecy.*
The request and the subsequent proceedings relating to the requested measure shall be substantiated in a separate and secret piece, without the need to expressly agree on the secrecy of the case.

Article 588 bis e. *Duration.*
1. The measures regulated in this chapter shall have the duration specified for each one of them and may not exceed the time necessary for the clarification of the facts.
2. The measure may be extended, by means of self-motivation, by the competent judge, ex officio or at the reasonable request of the applicant, provided that the causes for which it was granted still exist.
3. Once the term for which the measure was granted has elapsed, and its extension has not been agreed upon, or, as the case may be, once it has been terminated, it shall cease for all purposes.

Section 588 bis f. *Request for extension.*

1. The request for extension shall be addressed by the Public Prosecutor's Office or the Judicial Police to the competent judge with sufficient time before the expiration of the term granted. It shall in any case include:
(a) A detailed report on the outcome of the measure.
(b) The reasons justifying the continuation of the measure.
2. Within two days following the filing of the request, the judge shall rule on the termination of the measure or its extension by self-motivation. Before issuing the decision, the judge may request clarifications or further information.
3. Granted the extension, its computation shall start from the date of expiration of the term of the agreed measure.

Article 588 bis g. *Control of the measure.*
The Judicial Police shall inform the investigating judge of the development and results of the measure, in the manner and with the periodicity determined by him and, in any case, when for any reason the measure is terminated.

Article 588 bis h. *Involvement of third parties.*
The measures of investigation regulated in the following chapters may be agreed upon even when they affect third parties in the cases and under the conditions regulated in the specific provisions of each one of them.

Article 588 bis i. *Use of information obtained in a different procedure and casual discoveries.*
The use of information obtained in a different procedure and casual discoveries shall be regulated in accordance with the provisions of Article 579 bis.

Article 588 bis j. *Termination of the measure.*
The judge will agree on the termination of the measure when the circumstances that justified its adoption disappear or it is evident that through it the intended results are not being obtained, and, in any case, when the term for which it was authorized has elapsed.

Article 588 bis k. *Destruction of records.*
1. Once the proceeding is terminated by means of a final decision, the erasure and elimination of the original records that may be contained in the electronic and computer systems used in the execution of the measure shall be ordered. A copy shall be kept in the custody of the court clerk.
2. The destruction of the preserved copies shall be ordered when five years have elapsed following the execution of the sentence, or when the crime or sentence has expired, or when the dismissal of the case has been decreed, or a final judgment of acquittal has been handed down in respect of the person under investigation, provided that their preservation is not necessary in the opinion of the Court.
3. The courts shall issue the appropriate orders to the Judicial Police to carry out the destruction contemplated in the preceding paragraphs.

CHAPTER V
Interception of telephonic and telematic communications

Section 1. General Provisions

Article 588-ter a. *Preconditions.*
The authorization for the interception of telephone and telematic communications may only be granted when the investigation has as its object any of the crimes referred to in article 579.1 of this law, or crimes committed through computer tools or any other information or communication technology or communication service.

Article 588-ter b. *Scope.*
1. The terminals or means of communication object of intervention must be those regularly or occasionally used by the investigated person.
2. The judicially agreed intervention may authorize access to the content of the communications and to the electronic traffic data or data associated to the communication process, as well as to those produced regardless of the establishment of a specific communication or not, in which the subject under investigation participates, either as sender or receiver, and may affect the terminals or the means of communication of which the subject under investigation is the owner or user.
The terminals or means of communication of the victim may also be tapped when a serious risk to his life or integrity is foreseeable.
For the purposes of this article, electronic traffic or associated data shall be understood as all those generated as a consequence of the conduction of the communication through an electronic communications network, of its availability to the user, as well as of the provision of a service of the information society or telematic communication of analogous nature.

Article 588-ter c. *Affectation to third parties.*
The judicial intervention of the communications emitted from terminals or means of telematic communication belonging to a third person may be agreed provided that:
1. there is evidence that the subject under investigation uses it to transmit or receive information, or
2. the owner collaborates with the person under investigation in his illicit purposes or benefits from his activity.
Such intervention may also be authorized when the device under investigation is used maliciously by third parties by telematic means, without the knowledge of its owner.

Article 588-ter d. *Request for judicial authorization.*
1. The application for judicial authorization shall contain, in addition to the requirements mentioned in Article 588 bis b, the following:
(a) the identification of the subscriber number, terminal or technical label,

(b) the identification of the connection that is the object of the intervention or
(c) the data necessary to identify the means of telecommunication in question.
2. In order to determine the extent of the measure, the request for judicial authorization may have as its object any of the following:
(a) The recording and registration of the content of the communication, with an indication of the form or type of communications concerned.
(b) The knowledge of its origin or destination, at the moment in which the communication is made.
(c) The geographical location of the origin or destination of the communication.
(d) Knowledge of other traffic data associated or not associated, but of added value to the communication. In this case, the request shall detail the specific data to be obtained.
3. In cases of urgency, when the investigations are carried out for the investigation of crimes related to the actions of armed gangs or terrorist elements and there are well-founded reasons that make the measure provided for in the previous sections of this article essential, it may be ordered by the Minister of the Interior or, in his absence, by the Security Secretary of State. This measure will be communicated immediately to the competent judge and, in any case, within a maximum period of twenty-four hours, stating the reasons that justified the adoption of the measure, the action taken, the manner in which it has been carried out and its result. The competent judge, also in a grounded manner, shall revoke or confirm such action within a maximum period of seventy-two hours from the time the measure was ordered.

Article 588-ter e. *Collaboration duty.*
1. All telecommunications service providers, providers of access to a telecommunications network or information society services, as well as any person who in any way contributes to facilitating communications by telephone or any other means or system of telematic, logical or virtual communication, are required to provide the judge, the Public Prosecutor's Office and the agents of the Judicial Police appointed to carry out the measure with the assistance and collaboration necessary to facilitate compliance with the orders to intercept the telecommunications.

2. The subjects required to collaborate shall be obliged to maintain secrecy regarding the activities required by the authorities.
3. The reporting institutions who fail to comply with the above duties may incur in the crime of disobedience.

Article 588-ter f. *Control of the measure.*
In compliance with the provisions of article 588 bis g, the Judicial Police shall make available to the judge, with the periodicity determined by him and on different digital supports, the transcription of the passages it considers of interest and the complete recordings made. The origin and destination of each of them shall be indicated and the authenticity and integrity of the information transferred from the central computer to the digital media on which the communications have been recorded shall be ensured by means of an advanced electronic sealing or signature system or a sufficiently reliable verification system.

Article 588-ter g. *Duration.*
The initial maximum duration of the interception, which shall be computed from the date of judicial authorization, shall be three months, extendable for successive periods of equal duration up to a maximum period of eighteen months.

Article 588-ter h. *Request for extension.*
For the substantiation of the request for the extension, the Judicial Police shall provide, where appropriate, the transcription of those passages of the conversations from which relevant information can be deduced to decide on the maintenance of the measure.
Before issuing the decision, the judge may request clarifications or further information, including the full content of the intercepted conversations.

Article 588-ter i. *Access of the parties to the recordings.*
1. When the secrecy is lifted and the validity of the measure of intervention has expired, a copy of the recordings and of the transcriptions made shall be delivered to the parties. If the recording contains data referring to aspects of the intimate life of the persons, only the recording and transcription of those parts that do not refer to them shall be delivered. The non-inclusion of the entire recording in the transcript shall be expressly stated.
2. Once the recordings have been examined and within the time limit set by the judge, in view of the volume of the information on the media, any of the parties may request the inclusion in the copies of those communications that they consider relevant, and which have been excluded. The investigating judge, after hearing or examining such communications, shall decide on their exclusion or inclusion in the case.
3. The investigating judge shall notify the persons involved in the intercepted communications of the fact of the interception and shall inform them of the specific communications in which they have participated that are affected, unless it is impossible, requires a disproportionate effort or may prejudice future investigations. If the person notified so requests, a copy of the recording or transcript of such communications shall be provided, insofar as this does not affect the right to privacy of other persons or is contrary to the purposes of the proceedings in the framework of which the interference measure was taken.

Section 2. Incorporation of electronic traffic data or associated data into the proceedings

Article 588-ter j. *Data contained in automated files of the service providers.*
1. Electronic data retained by service providers or persons facilitating communication in compliance with the legislation on retention of data relating to electronic communications or on their own initiative for commercial or other reasons and which are linked to communication processes, may only be disclosed for incorporation into the process with judicial authorization.

2. When the knowledge of such data is indispensable for the investigation, authorization shall be requested from the competent judge to obtain the information contained in the automated files of the service providers, including the cross-referenced or intelligent search of data, provided that the nature of the data to be known and the reasons justifying the transfer are specified.

Section 3. Access to data necessary for the identification of users, terminals, and connectivity devices.

Article 588-ter k. *Identification by IP number.*
When in the exercise of the functions of prevention and discovery of crimes committed on the Internet, the agents of the Judicial Police have access to an IP address that is being used for the commission of a crime and there is no identification and location of the equipment or the corresponding connectivity device or the personal identification data of the user, they will request the investigating judge to require the agents subject to the duty of collaboration under Article 588 ter e, the transfer of the data that allow the identification and location of the terminal or connectivity device and the identification of the suspect.

Article 588-ter l. *Identification of terminals by capturing identification codes of the device or its components.*
1. Whenever in the framework of an investigation it has not been possible to obtain a certain subscriber number and this is indispensable for the purposes of the investigation, the Judicial Police agents may use technical devices that allow access to knowledge of the identification codes or technical labels of the telecommunication device or any of its components, such as the IMSI or IMEI numbers and, in general, any technical means that, according to the state of technology, is suitable for identifying the communication equipment used or the card used to access the telecommunication network.
2. Once the codes allowing the identification of the device or any of its components have been obtained, the agents of the Judicial Police may request from the competent judge the intervention of the communications under the terms established in article 588 ter d. The request must inform the court of the use of the devices referred to in the previous paragraph.
The court shall issue a grounded decision granting or denying the application for interception within the time limit established in article 588 bis c.

Article 588-ter m. *Identification of holders or terminals or connectivity devices.*
When, in the exercise of their functions, the Public Prosecutor's Office or the Judicial Police need to know the ownership of a telephone number or any other means of communication, or, conversely, require the telephone number or the identification data of any means of communication, they may directly contact the providers of telecommunications services, of access to a telecommunications network or of information society services, who will be required to comply with the request, under penalty of incurring the crime of disobedience.

CHAPTER VI

Recording and taping of oral communications by means of the use of electronic devices

Article 588-quater a. *Recording of direct oral communications.*

1. The placement and use of electronic devices that allow the capture and recording of the direct oral communications that are maintained by the investigated person, on public spaces or in other open spaces, in his domicile or in any other closed places, may be authorized.

The listening and recording devices may be placed both outside and inside the domicile or enclosed place.

2. In the event that it is necessary to enter the home or any of the spaces intended for the exercise of privacy, the enabling resolution shall extend its motivation to the appropriateness of access to such places.

3. The listening and recording of the private conversations may be complemented with the obtaining of images when expressly authorized by the judicial resolution that grants it.

Article 588-quater b. *Preconditions.*

1. The use of the devices referred to in the previous article must be linked to communications that may take place in one or more specific encounters of the investigated person with other persons and whose foreseeability has been revealed by the investigation.

2. It can only be authorized when the following requirements are met:

(a) That the events being investigated are constitutive of any of the following crimes:

1. Fraudulent offenses punishable by a penalty with a maximum limit of at least three years imprisonment.

2. Crimes committed within a criminal group or organization.

3. Terrorist crimes.

(b) That it can be rationally foreseen that the use of the devices will provide essential data of evidential relevance for the clarification of the facts and the identification of the perpetrator.

Article 588-quater c. *Content of the judicial resolution.*

The judicial resolution authorizing the measure must contain, in addition to the requirements regulated in article 588 bis c, a specific mention of the place or premises, as well as the meetings of the investigated person that are going to be subject to surveillance.

Article 588-quater d. *Control of the measure.*

In compliance with the provisions of article 588 bis g, the Judicial Police will provide the judicial authority with the original support or authentic electronic copy of the recordings and images, which must be accompanied by a transcript of the conversations it considers of interest.

The report shall identify all the agents who have participated in the execution and monitoring of the measure.

Article 588-quater e. *Termination.*
Once the measure has been terminated for any of the causes foreseen in article 588 bis j, the recording of conversations that may take place in other encounters or the capturing of images of such moments will require a new judicial authorization.

CHAPTER VII
Use of technical devices for image capture, tracking and tracing

Section 588 quinquies a. *Capture of images in public places or spaces.*
1. The Judicial Police may obtain and record by any technical means images of the person under investigation when he is in a public place or space, if this is necessary to facilitate his identification, to locate the instruments or effects of the crime or to obtain relevant data for the elucidation of the facts.

2. The measure may be carried out even when it affects persons other than the person under investigation, provided that otherwise the usefulness of the surveillance would be significantly reduced or there are well-founded indications of the relationship of such persons with the person under investigation and the events under investigation.

Section 588 quinquies b. *Use of tracking and tracing devices or technical means.*
1. When there are proven reasons of necessity and the measure is proportionate, the competent judge may authorize the use of tracking and tracing devices or technical means.
2. The authorization shall specify the technical means to be used.
3. The providers, agents and persons referred to in article 588 ter are obliged to provide the judge, the Public Prosecutor's Office and the agents of the Judicial Police appointed to carry out the measure with the assistance and collaboration necessary to facilitate compliance with the orders ordering the monitoring, under penalty of incurring the crime of disobedience.
4. When there are reasons of urgency that make it reasonably to fear that failure to immediately place the device or technical means of tracking and tracing will frustrate the investigation, the Judicial Police may proceed with its placement, reporting as soon as possible, and in any case within a maximum period of twenty-four hours, to the judicial authority, who may ratify the measure adopted or agree to its immediate termination within the same period. In this last case, the information obtained from the placed device will lack effects in the process.

Section 588 quinquies c. *The duration of the measure.*
1. The measure of use of technical tracking and tracing devices provided for in the previous article shall have a maximum duration of three months from the date of its authorization. Exceptionally, the judge may grant successive extensions for the same or a shorter period up to a maximum of eighteen months, if so, justified in view of the results obtained with the measure.

2. The Judicial Police shall deliver to the judge the original media or authentic electronic copies containing the information collected when requested to do so by the judge and, in any case, when the investigations are completed.
3. The information obtained through the technical tracking and tracing devices referred to in the preceding articles shall be duly guarded to avoid its improper use.

CHAPTER VIII
Registration of massive information storage devices

Section 588 sexies a. *Necessity of individualized motivation.*
1. When on occasion of a home search the seizure of computers, telephone or telematic communication instruments or massive digital information storage devices or the access to telematic data repositories is foreseeable, the decision of the investigating judge shall extend its reasoning to the justification, as the case may be, of the reasons that legitimize the access of the authorized agents to the information contained in such devices.
2. The simple seizure of any of the devices referred to in the preceding paragraph, carried out during the course of the search, does not legitimize access to its contents, without prejudice to the fact that such access may be subsequently authorized by the competent judge.

Section 588 sexies b. *Access to the information of electronic devices seized outside the domicile of the investigated person.*
The requirement provided for in paragraph 1 of the preceding article shall also apply to those cases in which computers, communication tools or mass data storage devices, or access to telematic data repositories, are seized independently of a house search. In such cases, the agents will inform the judge of the seizure of such items. If the judge considers access to the information stored in its contents to be essential, he shall grant the corresponding authorization.

Section 588 sexies c. *Judicial authorization.*
1. The decision of the investigating judge authorizing access to the information contained in the devices referred to in this section shall establish the terms and scope of the search and may authorize the making of copies of the computer data. It shall also lay down the conditions necessary to ensure the integrity of the data and the guarantees of their preservation in order to enable, where appropriate, an expert opinion to be given.
2. Unless they constitute the object or instrument of the offence or there are other reasons that justify it, the seizure of the physical supports containing the data or computer files shall be avoided, when this could cause serious prejudice to their holder or owner and it is possible to obtain a copy of them under conditions that guarantee the authenticity and integrity of the data.
3. Where those who carry out the search or have access to the information system or part thereof in accordance with the provisions of this Chapter have reasonable grounds to consider that the data sought are stored in another computer system or part thereof, they may extend the search, provided that the data are lawfully accessible by means of or available to the initial

system. This extension of the search must be authorized by the judge, unless otherwise authorized in the initial authorization. In case of urgency, the Judicial Police or the prosecutor may carry it out, informing the judge immediately, and in all cases within a maximum period of twenty-four hours, of the action taken, the manner in which it was carried out and its result. The competent judge, also in a grounded manner, shall revoke or confirm such action within a maximum period of seventy-two hours from the time the measure was ordered.

4. In cases of urgency in which a legitimate constitutional interest that makes the measure provided for in the previous sections of this article indispensable is deemed to exist, the Judicial Police may carry out the direct examination of the data contained in the seized device, communicating it immediately, and in any case within a maximum period of twenty-four hours, in a well-founded written document to the competent judge, stating the reasons that justified the adoption of the measure, the action taken, the manner in which it has been carried out and its result. The competent judge, also in a grounded manner, shall revoke or confirm such action within a maximum period of 72 hours after the measure was ordered.

5. The authorities and agents in charge of the investigation may order any person with knowledge of the operation of the computer system or the measures applied to protect the computer data contained therein to provide the necessary information, provided that this does not result in a disproportionate burden for the affected party, under penalty of being guilty of disobedience.

This provision shall not be applicable to the investigated or accused person, to persons who are exempted from the obligation to testify due to kinship and to those who, in accordance with Article 416.2, cannot testify by virtue of professional secrecy.

CHAPTER IX

Remote records on computer equipment

Section 588 septies a. *Preconditions.*

1. The competent judge may authorize the use of identification data and codes, as well as the installation of software, which allow, remotely and telematically, the remote examination without the owner's or user's knowledge of the content of a computer, electronic device, computer system, instrument of massive storage of computer data or database, provided that it pursues the investigation of any of the following crimes:

(a) Crimes committed within criminal organizations.

(b) Terrorist crimes.

(c) Crimes committed against minors or persons with judicially modified capacity.

(d) Crimes against the Constitution, treason, and crimes related to national defense.

(e) Crimes committed through computer instruments or any other information or telecommunication technology or communication service.

2. The judicial resolution authorizing the search shall specify:

(a) The computers, electronic devices, computer systems or part thereof, computer data storage media or databases, data, or other digital contents that are the object of the measure.

(b) The scope of the measure, the way in which the access and seizure of the data or computer files relevant to the case will be carried out, and the software by means of which the control of the information will be executed.
(c) The agents authorized for the execution of the measure.
(d) The authorization, if applicable, for the creation and preservation of copies of the computer data.
(e) The measures necessary for the preservation of the integrity of the stored data, as well as for the inaccessibility or deletion of such data from the computer system to which access has been gained.
3. When the agents carrying out the remote search have reasons to believe that the data sought are stored in another computer system or in a part thereof, they shall bring this fact to the attention of the judge, who may authorize an extension of the terms of the search.

Section 588 septies b. *Collaboration duty.*
1. The service providers and persons referred to in article 588 ter e and the owners or persons responsible for the computer system or database subject to the search are obliged to provide the investigating agents with the necessary collaboration for the execution of the measure and access to the system. They are also obliged to provide the necessary assistance so that the data and information collected can be examined and visualized.
2. The authorities and agents in charge of the investigation may order any person with knowledge of the operation of the computer system or the measures applied to protect the computer data contained therein to provide the necessary information, provided that this does not result in a disproportionate burden for the affected party, under penalty of being guilty of disobedience.
This provision shall not be applicable to the investigated or accused person, to persons who are exempted from the obligation to testify due to kinship and to those who, in accordance with Article 416.2, cannot testify by virtue of professional secrecy.
3. The subjects required to collaborate shall be obliged to maintain secrecy regarding the activities required by the authorities.
4. The persons referred to in paragraphs 1 and 2 of this article shall be subject to the liability regulated in paragraph 3 of article 588 ter e.

Section 588 septies c. *Duration.*
The measure shall have a maximum duration of one month, extendable for equal periods up to a maximum of three months.

CHAPTER X
Securing measures

Article 588 octies. *Data preservation order.*
The Public Prosecutor's Office or the Judicial Police may require any natural or legal person to conserve and protect specific data or information included in a computer storage

system that is at their disposal until the corresponding judicial authorization is obtained for its transfer in accordance with the provisions of the preceding articles.
The data shall be kept for a maximum period of ninety days, which may be extended once until the transfer is authorized or one hundred and eighty days have elapsed.
The requested party will be obliged to collaborate and keep secret the development of this diligence, being subject to the responsibility described in section-3 of article 588 ter e.

On the detention and opening of written and telegraphic correspondence

Article 579. *On written or telegraphic correspondence.*
1. The judge will be able to order the detention of the private, postal and telegraphic correspondence, including faxes, bureaufaxes and money orders, that the investigated person sends or receives, as well as its opening or examination, if there were indications that the discovery or the verification of some fact or relevant circumstance for the cause could be obtained by these means, as long as the investigation pursues some of the following crimes:
1. Fraudulent offenses punishable by a maximum penalty of three years' imprisonment.
2. Crimes committed within a criminal group or organization.
3. Terrorist crimes.
2. The judge may order, in a grounded resolution, for a period of up to three months, extendable for equal or lesser periods up to a maximum of eighteen months, the monitoring of the postal and telegraphic communications of the investigated person, as well as of the communications used for the realization of his criminal purposes.
3. In cases of urgency, when the investigations are carried out for the investigation of crimes related to the actions of armed gangs or terrorist elements and there are well-founded reasons that make the measure provided for in the previous sections of this article essential, it may be ordered by the Minister of the Interior or, in his absence, by the Security Secretary of State. This measure will be communicated immediately to the competent judge and, in any case, within a maximum period of twenty-four hours, stating the reasons that justified the adoption of the measure, the action taken, the manner in which it has been carried out, and its result. The competent judge, also in a grounded manner, shall revoke or confirm such action within a maximum period of seventy-two hours from the time the measure was ordered.
4. Judicial authorization shall not be required in the following cases:
(a) Postal items which, by their own external characteristics, are not usually used to contain individual correspondence, but to transport and traffic goods or on the outside of which the contents are stated.
(b) Those other forms of dispatch of correspondence under the legal format of open communication, in which an external declaration of contents is obligatory, or which incorporate the express indication that their inspection is authorized.
(c) When the inspection is carried out in accordance with customs regulations or proceeds in accordance with the postal regulations governing a certain class of mail.

5. The request and the subsequent proceedings relating to the requested measure shall be substantiated in a separate and secret piece, without the need to expressly agree on the secrecy of the case.

Section 579 bis: *Use of information obtained in a different procedure and casual discoveries.*
1. The result of the arrest and opening of written and telegraphic correspondence may be used as a means of investigation or evidence in another criminal proceeding.
2. To this effect, the deduction of testimony of the individuals necessary to prove the legitimacy of the interference shall be made. Among the necessary background information shall be included, in all cases, the initial application for the adoption, the judicial decision granting it, and all the petitions and judicial decisions of extension issued in the original proceeding.
3. The continuation of this measure for the investigation of the incidentally discovered crime requires the authorization of the competent judge, for which, the latter will verify the diligence of the action, evaluating the framework in which the casual finding took place, and the impossibility of having requested the measure that included it at the time. Likewise, it will be informed if the proceedings continue to be declared secret, in order to ensure that such declaration is respected.

BIBLIOGRAPHY

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, July 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), November 2019.

ALLEN, Franklin / GU, Xian / JAGTIANI, Julapa: "A survey of Fintech research and policy discussion," Federal Reserve Bank of Philadelphia Research Department, Working Papers 20-21, June 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, pp. 34/51.

AUCOIN, Kaleigh E.: "The spider's parlour: Government malware on the dark web," Hastings Law Journal, Vol 69, No. 5, 2018, pp. 1433/1469.

Basel Committee on Banking Supervision: "Prudential treatment of cryptoassets exposures," Bank for International Settlements, June 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 No. 05-15, 2005.

BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan: "Going bright: Wiretapping without weakening communications infrastructure," IEEE Security & Privacy, Vol 11, No. 1, 2013, pp. 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, No. 1, 2014, pp. 1/64.

BIRYUKOV, Alex / KHOVRATOVICH, Dimitry / PUSTOGAROV, Ivan: "Deanonymization of clients in Bitcoin P2P network," AAVV, *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Scottdale, 2014, pp. 15/29.

BIRYUKOV, Alex / FEHER, Daniel: "Deanonymization of hidden transactions in Zcash," University of Luxembourg, 2018; Herrera-Joancomartí, Jordi:

BLANCO, Hernán, *Tecnología informática e investigación criminal* [Informatic Technology and criminal investigation], 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*," [Hacking with a judicial order in the Spanish procedural law from Organic Law 13/2015 of October 5], in InDret, No. 1/2020, January 2020.

BOJARSKI, Kamil: "Dealer, hacker, lawyer, spy. Modern techniques and legal boundaries of counter-cybercrime operations," The European Review of Organized Crime, Vol. 2, No. 2, 2015, pp. 25/50.

BRILL, Alan / KEENE, Lonnie: "Cryptocurrencies: The next generation of terrorist financing," Defence Against Terrorism Review, Vol. 6, No. 1, 2014, pp. 7/30.

BRYANS, Danton: "Bitcoin money laundering: Mining for an effective solution," Indiana Law Journal, Vol. 89, 2014, pp. 441/472.

Camdem Asset Recovery Inter-Agency Network (CARIN): "CARIN Manual" (5a Edition), Guernsey Law Offices, 2015.

CARRELL, Nathan E.: "Spying on the mob: United States v. Scarfo – A constitutional analysis," Journal of Law, Technology & Policy," Vol. 2002, No. 1, 2002, pp. 193/214.

CipherTrace: "Cryptocurrency crime and anti-money laundering report," February 2021.

League of Arab States Convention.

Council of Europe Convention on Cybercrime (Budapest Convention).

Council of Europe: "Guide on seizing cryptocurrencies," Cybercrime Programme Office of the Council of Europe, February 2021.

DASKAL, Jennifer; "The un-territoriality of data," The Yale Law Journal, Vol. 125, No. 2, 2015, pp. 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, pp. 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, pp. 42/59.

DUPUIS, Daniel / GLEASON, Kimberley: "Money laundering with cryptocurrency: Open doors and the regulatory dialectic," Journal of Financial Crime, August 2020.

European Banking Authority (EBA): "Warning to consumers on cryptocurrencies," December 2013.

European Banking Authority (EBA): "EBA opinion on 'virtual currencies,'" EBA-Op-2014-08, July 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, August 2016.

European Central Bank (ECB): "Virtual currency schemes," Frankfurt, October 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, No. 223, May 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, May 2018.

European Union Agency for Cybersecurity (ENISA) and Europol: "On lawful criminal investigation that respects 21st century data protection. Europol and ENISA joint statement," statement of May 20, 2016.

European Union Agency for Cybersecurity (ENISA): "Crypto assets. An introduction to digital currencies and distributed ledger technologies," February 2021.

Europol: "Dismantling of an encrypted network sends shockwaves through organized crime groups across Europe," July 2020.

FALIERO, Johanna C., *Criptomonedas: La nueva frontera regulatoria del Derecho informático*, [The new regulatory border of computer law] 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, January 2018.

Federal Bureau of Investigations (FBI): "Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity," Criminal Intelligence Section / Cyber Intelligence Section, April 2012.

Financial Stability Institute: "Supervising cryptoassets for anti-money laundering," FSI insights on policy implementation, No. 31, April 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, No. 5, 2019, pp. 1798/1853.

FORGANG, George: "Money laundering through cryptocurrencies," Economic Crime Forensics Capstones, La Salle University, Vol. 40, 2019.

FATF: "Report on new payment methods," October 2006.

FATF: "Money laundering using new payment methods," October 2010.

FATF: "Virtual currencies. Key definitions and potential AML/CFT risks," June 2014.

FATF: "Guidance for a risk-based approach: Virtual currencies," June 2015.

FATF: "Emerging terrorist finance risks," October 2015.

FATF: "FATF report to G20 Finance Ministers and Central Bank Governors," July 2018.

FATF: "Professional money laundering," July 2018.

FATF: "Financing of terrorism for recruitment purposes," October 2018.

FATF: "Virtual assets and virtual assets service providers. Guidance for a risk-based approach," June 2019.

FATF: "Guidance on financial investigations involving virtual assets," June 2019.

FATF: "FATF report to the G20 Ministers and Central Bank governors on the so-called stablecoins," June 2020.

FATF: "Money laundering and terrorist financing red flag indicators associated with virtual assets," September 2020.

FATF: "International standards on the fight against money laundering and terrorist financing and the financing of the proliferation of weapons of mass destruction," December 2020.

FATF: "12-month review of the revised FATF standards on virtual assets and virtual asset service providers," June 2020.

GAFILAT: "2020–2025 GAFILAT Strategic Plan."

GAFILAT: "Tenth Anniversary of the Asset Recovery Network of the Financial Action Task Force of Latin America - RRAG," September 2020.

GAFILAT: "Inventory of existing global networks for the identification and recovery of proceeds of crime," June 2021.

GAFILAT /RRAG: "List of open sources of RRAG member countries," June 2021.

GHAPPOUR, Ahmed: "Searching places unknown: Law enforcement jurisdiction on the dark web," Stanford Law Review, Vol. 69, No. 4, 2017, pp. 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, February 2016.

HENNESSEY, Susan: "The elephant in the room: Addressing child exploitation and going dark," Hoover Institution, Stanford University, Aegis Paper Series, No. 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, p. 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, pp. 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," November 2020.

JOHNSON, David R. / POST, David: "Law and borders – The rise of law in cyberspace," Stanford Law Review, Vol. 48, No. 5, 1996, pp. 1367/1402.

JONES, Phil: "*Habilidades fundamentales para rastrear activos*," [Fundamental capacities to track assets], Basel Institute of Governance, Quick Guide Series, N° 14, November 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, pp. 58/69.

KERR, Orin S. / SCHNEIER, Bruce: "Encryption workarounds," Georgetown Law Journal, Vol. 106, No. 4, 2018, pp. 989/1019.

KOOPS, Bert-Jaap: "Police investigations in open sources: Procedural-law issues," Computer Law & Security Review, Vol. 29, No. 6, 2013, pp. 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 No. 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, pp. 2145/2150.

MAYER, Jonathan, "Constitutional malware," en Social Sciences Research Network (SSRN), November 2016.

MBIYANGA, Stefan "Cryptolaundering: Anti-money laundering regulation of virtual currency exchanges," Journal of Anti-Corruption Law, Vol. 3, No. 1, 2019, pp. 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" [Open-source intelligence], Basel Institute of Governance, Quick Guide Series, No. 17, June 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, pp. 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, London, 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," Proceedings on Privacy Enhancing Technologies, Vol. 3, 2018, pp. 143-163.

NAKAMOTO, Satoshi: "Bitcoin: A peer-to-peer electronic cash system," 2008.

Organization of American States (OAS): *"Recomendaciones de la 9ª reunión del Grupo de Trabajo en Delito Cibernético,"* [Recommendations of the 9th Meeting of the Working Group on Cybercrime], Meetings of Ministers of Justice or Other Ministers, Attorneys or Attorneys General of the Americas (REMJA), December 12-13, 2016.

Organization of American States (OAS): "*Recomendaciones de la 11ª Reunión de Ministros de Justicia u Otros Ministros, Procuradores o Fiscales Generales de las Américas*" (REMJA XI), [Recommendations of the 11th Meeting of Ministers of Justice or Other Ministers, Attorneys General or Prosecutors General of the Americas] OEA/ser.K/XXXIV.11 REMJA-XI/DOC.2/21 rev. 1, May, 2021

Organization of American States (OAS): "*Estudio sobre nuevas tipologías en el lavado de dinero, específicamente en el uso de moneda virtual*" [Study on new typologies in money laundering, specifically in the use of virtual currency], conclusions of the XLV Meeting of the Expert Group for the Control of Money Laundering – FIU/OIC Sub-Working Group 2016-2018, OAS/Ser.L/XV. 4.45 DDOT/LAVEX/doc. 16/18, October 2018.

United Nations Organisation (UN): "El derecho a la privacidad en la era digital," [The right to privacy in the digital age] Statement 68/167, December 18, 2013.

United Nations Organisation (UN): "*El derecho a la privacidad en la era digital*" [The Right to Privacy in the Digital Age]" Statement A/HRC/27/37, Report of the Office of the United Nations High Commissioner for Human Rights, June 2014, pp.

United Nations Organisation (UN): "El derecho a la privacidad en la era digital," [The right to privacy in the digital age] Statement 69/166, December 18, 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, No. 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, pp. 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, pp. 55/99.

Police Executive Research Forum (PERF): "The changing nature of crime and criminal investigations," 2018.

Draft Directive of the Economic Community of West African Countries (ECOWAS Draft Directive).

Draft African Union Convention.

Regional Organized Crime Information Center (ROCIC): "Penetrating the 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, pp. 197/223.

RICHET, Jean-Loup "Laundering money online: A review of cybercriminals methods," Tools and Resources for Anti-Corruption Knowledge, UNODC, June 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, No. 1, 2005, pp. 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, pp. 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 No. 31, 2010.

Model Legislative Texts of the Caribbean Community (ITU/CARICOM/CTU Model Legislative Texts).

SWIRE, Peter / AHMAD, Kenesa: "'Going dark' versus a 'golden age for surveillance'," CDT Fellows Focus Series, published on 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, No. 2, 2018, pp. 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," June 2014.

VACIAGO, Giuseppe / SILVA RAMALHO, David: "Online searches and online surveillance: The use of trojans and other types of malwares as means of obtaining evidence in criminal proceedings," Digital Evidence and Electronic Signature Law Review, Vol. 13, 2016, pp. 88/86.