New technologies and new challenges in assets recovery

Giovanni Salvi

Prosecutor general – President of the Scientific Committee of Vittorio Occorsio Foundation

Vittorio Occorsio was a prosecutor who spent his professional life in prosecuting organized crime. He was killed on July 10, 1976. The Occorsio Foundation is aimed at disseminating his main lesson: the investigative methodology should be adequate to the object of the investigation itself.

UNTOC (2000) can be considered a sort of *bridge convention*, able to connect the specific field of transnational serious crimes to the main central idea that the rule of law should be always a precondition of a well ordered, safe, fair, and equal society. Idea that characterizes the United Nations Organization.

The Merida Convention (2003) is strictly linked to the UNTOC. The strength of Merida Convention is the specific and detailed attention paid to all the forms of seizure, confiscation, recovery, restitution and reuse of the proceeds of corruption, as shown by Judge Viganò in his contribution.

The Tenth Conference of the Parties, October 2020, approved the Falcone Resolution, stressing the relevance of the Palermo Convention, inter alia, for fighting corruption, in the perspective of a well-ordered economy.

The diktat "Follow the money", at the basis of both Palermo and Merida Conventions, is transformed in a more complex vision, with at the centre the correct, well-disciplined economic order.

Nevertheless, the current Conventional Instruments must be improved to face the new challenges that the growing technological evolution poses. In a global virtual environment, the main question will be how the national jurisdictions could be affirmed and then enforced.

The importance of UNTOC emerged clearly in the trials against trafficking in human beings and smuggling of immigrants by the sea. In those cases, Italy

used UNTOC as a legal basis to establish the domestic jurisdiction in the High Seas, in accordance with Geneva (1958) and Montego Bay (1982) conventions. The capacity of UNTOC to respond to new challenges and phenomena has been positively tested in a consolidated international environment as it is the Law of the Sea.

The question now is: could this approach be expanded and applied in other fields of transnational crime that nowadays pose new challenges for judicial cooperation between states?

The use of Information and Communication Technologies (ICT) to obstacle the identification of provenience and destination of the proceeds is already a daily experience. Therefore, the regulatory Agencies over the world assumed specific measures intended to prevent the criminal use of virtual exchanges. These measures include the recourse to Artificial Intelligence in analyzing big data, so extracting information on anomalies, indicating possible misuse of financial instruments. The issue has been recently addressed by Financial Action Task Force (FATF) and, in more general terms, by the European Parliament.

It is likely that a growing role will be played by virtual currencies (VC). The mole of virtual transactions is growing exponentially over the world, even if only a small percentage could be considered of criminal origin.

VC is a term that covers a wide range of different forms of transactions. There is no unanimous consent on a definition of VC: it is assimilated to a money, a currency, or an asset, that be exchanged or stored.

The VC can be operated in the legitimate web, and it is going to be – at least in part – regulated by national authorities and international instruments.

In the next future, Central Banks will adopt VCs by routine, introducing a complete regulation, but – at the same time – pushing customers towards less regulated markets.

In the partially regulated web environment, as above described, we can identify three different phases, in the passages from the real world (and its

"legal" currencies) to the virtual one: phase 1 from Currency to VC; phase 2 from VC to VC; phase 3 from VC to Currency.

Phases 1 and 3 do not work differently from any ordinary transaction, that generally takes place with financial intermediaries, more or less regulated by the law. The transaction towards and from VC can be addressed as any other kind of transaction, without specific problems. Legal assistance can be obtained in due time, without great danger of evidence dispersion; pieces of evidence, even in digital form, can be frozen and assets can be seized.

Phase 2 is more complicated. The VC was born as a simplification and disintermediation of ordinary financial transactions; at the core of VC there is anonymity, granted by the asserted inviolability of the blockchain and of any single brick of the chain, or – even more – in consideration of the multiple crypto-identities, that each customer can use.

At the same time, the blockchain constitutes a permanent memory of the transactions. Its force, its intrinsic characteristic is the non-modifiability of any block and of the succession of the blocks, so it is trackable for definition. Consequently, the blockchain could be much more "transparent" than other forms of transaction, even for the Anti Money Laundering effects.

With the progress of regulation and of the Law Enforcement Agencies (LEA) ability to track the passages, many additional tools, aimed at enhancing anonymity, appeared on the web market. Operating in different ways, as mixing the VC to be anonymized with others (Mixer), these tools add a sort of shield between different passages of the VC, so making it hard to connect the final destination to the source of the proceedings.

The Mixer can be effective in hiding the provenience and the destination of the VC, being completely out of any legal regulation.

For an investigator, phase 2 is the most interesting. Phase 1 cannot be connected to phase 3, if not through phase 2. Other investigating tools can reach the same result, for example information from witnesses or cooperating defendants; confiscation without conviction could be based only on the lack of

proportion between income and patrimony, at given conditions. But these hypotheses are out of the scope of our discussion, being merely occasional.

Moreover, it must be considered that completing Phase 1 is not strictly necessary to complete the payment of the bribery: the price could be originated in VC or other virtual assets to be converted in VC without leaving the web. That makes investigation even more difficult.

A support could be offered by the above-mentioned AI methodologies, able to bring to light significant anomalies, but not to produce complete and specific forensic evidence, at least at present.

An illegal transaction will more probably take place on the dark web. In this case, the transaction is completely out of the radar of the regulatory authorities and can be identified and followed only by dogged investigations in the dark web. In this environment, a technique of investigation is based on undercover agents, that in international cooperation open the way to joint teams. The last is the direction indicated by the Council of Europe in Budapest Convention (2001) and its Second Additional protocol (2021), not yet in force, when cybercrimes are involved. UNTOC and Merida allowed such approach in the specific field of international corruption, as recently restated by the Working Group on International Cooperation Vienna, 7 and 8 July 2020, "*The use and role of joint investigative bodies in combating transnational organized crime*".

The tools at the hands of LEAs are day by day more effective in identifying the flow of possible illicit transactions, based also on AI. The Italian specialized financial LEA, Guardia di Finanza, has been experiencing similar tools for years.

Nevertheless, gathering evidence that can be used in Court requires a precise identification of a single, specific transaction and its link with the predicate offence.

As a matter of fact, one of the characteristics of web transactions through VC is not only the (semi) anonymity but mainly the no-location (virtuality) and the rapidity of the movement toward new pieces of the chain and new

territories. The conduct involves different nations at the same time, moving continuously without a pre-definite direction that can be foreseen. These characteristics would be soon enhanced by faster mega computers and by Quantum Computing.

Once the asset proceeding from a crime has been singled out, the following problem is how to secure it and proceed to seizure and confiscation. The Italian judiciary and LEAs acquired specific experience on the issue, in the criminal as well in the civil field. Here we take advantage from the experience of the Florence Prosecutor office in cases of corporate insolvency.

Compared to the common seizure of digital documents, the seizure of cryptocurrencies raises some specific issues related to the use of cryptographic techniques.

When enforcement agencies confiscate a wallet, they also need to confiscate private cryptographic keys, that are essential for the control of the wallet and for the spending of cryptocurrencies. In any case, seizing the private keys does not ensure the full control over the asset; for these purposes, it is necessary that enforcement authorities are the only actors to know the keys.

The problems vary depending on the concrete case and on the different type of wallet.

If the wallet is under the control of an intermediary – such as a wallet provider or an exchange, especially if this latter is centralized – and the intermediary has carried out an adequate verification process for all customers, we face the same problems that we encounter with confiscation of goods belonging to third parties.

However, also in this case, it is not possible to determine with certainty whether a person is the effective and exclusive owner of a bitcoin address, since it is sufficient to know the private key to spend the bitcoins.

The object of the seizure, then, varies depending on the type of wallet to be seized. For the "online" wallets, the seizure may concern the computer data stored on the servers of the wallet provider (or exchange); for the "desktop"

wallets, it may concern the hard disk of the computer on which is installed the software of the private keys; for the "paper wallets", it may concern the document on which is printed the public and private key; for the "hardware-wallets", it may concern the USB flash drive or the support on which are stored and generated the private keys.

Finally, there is also the case of "brain-wallet", in which the private key is memorized by an individual and therefore it is not possible to realize the seizure.

There are special precautions to be taken when seizing cryptocurrencies. In the case of software or online wallets, for example, seizing the hard disk or changing the wallet password does not guarantee security, as the user may have backed up the data or he may still know the private key. It may therefore be necessary to transfer the seized bitcoins on offline private key generators (the "cold-wallets") and to adopt multi-signature systems.

Securing assets may involve foreign jurisdictions, as shown by the above-mentioned cases, where the keys to get to the asset could be found in different territories, in material or immaterial form.

But how is possible to enforce jurisdiction in the virtual environment, in times compatible with the transactions' rapidity?

The virtual space where the transactions occur is the Sidera and at the same time the territory belonging to a national state. Thus, a mix of airwaves and land. In the land - and therefore in a State –the infrastructures necessary to operate Internet and the computing at the work are based; the waves live in the free space or in the cables. This mix essentially differentiates the virtual space from the High Sea, where land and waves are well distinguished, regulated under the international framework. Consequently, the experience maturated in the immigration field, as described above, cannot be used in this context.

The cyberspace is different also from the Space, for the same and opposite reasons: no territory can compete with sideral spaces. The international regulation of the Space cannot be used as well as a reference in the regimentation of the Cyberspace.

Cyberspace is an *Ircocervo*, mythological being participating in two natures.

The International Community has not yet reached a shared definition of Cyberspace, that is a necessary premise for any international cooperation. Even the name is debated, someone prefer 'cyber environment' rather than cyberspace.

The Mutual Legal Assistance is grounded on the definition of jurisdiction, as an affirmation and at the same time a limitation of national sovereignty; jurisdiction and enforcement of jurisdiction are within the essential attributions of sovereignty. How to apply such principles in the Cyberspace? Can any State simply apply the territorial criteria, interfering with the communication in transit in its own territory, *usque ad Sidera*? Or directly enforcing its own jurisdiction in the territory of another State, grounding it on the territorial criteria, like the effects of the criminal conduct?

On the other hand, the rapidity of the Internet communication and the unpredictability of the next steps or the territory where such steps will take place, makes it very difficult for investigating LEAs to ask the consent of the involved States to oppose criminal actions or – for what is important in the judicial field – to freeze the pieces of information and to gather them in a legit forensic shape. The II Additional Protocol to Budapest Convention addresses this issue, providing effective tools for ordinary cyber cooperation, as previous mutual consent in particular cases or simplified procedures or permanent joint teams. Can these provisions be useful when the fastest and most sophisticated operations are at stake? So, Budapest is a good starting point, but we must look forward.

A similar obstacle appears in the works of the Group of Governmental Experts on *Advancing responsible State behaviour in cyberspace in the context of international security*, established by the Secretary General of United Nation, following the GA resolution 73/266, and would be at the basis of the UN Convention on Cybercrimes, considering the difficulties in defining the concept of sovereignty in Cyberspace.

The existence of different approaches has involved serious concerns regarding the relationships between the freedom of the net and its regulation, the role of the private companies, the limits of free speech and the liberty of political expression, in a word, the relationship between authority and liberty.

Sometimes the Net is defined as an anarchic environment. Such definition covers only a part of reality. The space of Net is a competitive one, where different actors play their political attitude; the private Over The Top (OTT) companies act as regulatory players, in competition with national and supernational regulators, sharing sovereignty in a juridical separate order. New India Companies, they rule the electromagnetic waves with their well-armed vessels. In the judicial cooperation field, the national and supernational authorities are forced to ask permission to access relevant data.

In this context, the increasing volume, variety, speed of the management of transactions, due also to the dramatic rise in computing capacity, constitute an additional difficulty to the access to the information, relevant for the enforcement of the law.

The concrete risk is that the jurisdictional approach to the matter, the penal one in our field, could be compromised by the lack of effectiveness.

Juridical space does not tolerate voids. It is rapidly filled by other powers. When jurisdiction is ineffective, its space, its role is played by other actors with different countermeasures.

We do not talk of the regulation, as certifications or security measures against attacks, that are not in opposition to the penal approach, but concurrent with it.

In the competition between criminal imagination and Law Enforcement, the latter is always the loser.

The escape from jurisdiction is already a reality. The most important part of the reaction to illegal attacks against interests that should be protected by criminal law, resulted in the recent past in immediate and occult punitive reaction of States and private entities.

The alternative in the International Community to the actual judicial cooperation is the hidden field of the use of force. This carries a great risk of escalation and of obscure maneuvers.

Enhancing the effectiveness of the judiciary and of the MLA even in the rapidly evolving field of the ICT is of the utmost importance for the Human Rights protection and for the Peace.

Reaching such a target is not easy. The works in progress for a comprehensive UN convention on Cybercrime is our next challenge. The experience of UNTOC and Merida, their effectiveness born from necessity, grounded in reaction to specific criminal threats, can be a guide. In other words, we can help the progress in drafting the new Convention, by identifying single, specific fields in which penal approach can be sustained by consensus, as a first step toward a more general cooperation.

Hoping that a consensus over definitions, boundaries, attributions on cyberspace and cybercrimes can be soon reached, we can help the efforts of the International Community by making it evident that in some fields we cannot wait for too much time. We can push the commitment of the International Community starting from issues where the consent can be universal, as in the past in the field of counterterrorism, even in the absence of a shared definition of terrorism. Fighting corruption, enhancing Merida can be a good basis.

Sharm El Sheik, 13 December 2021