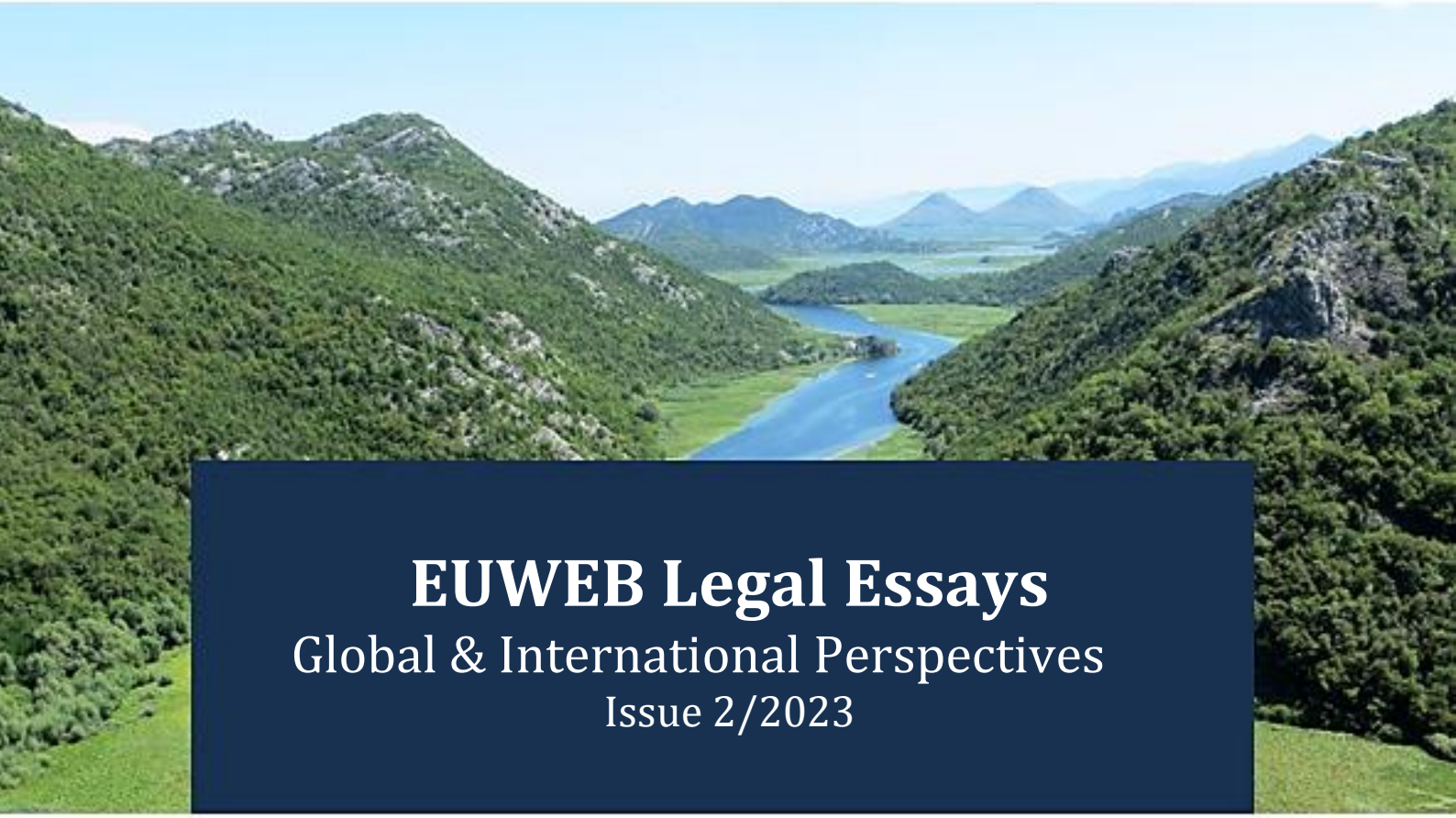
ISSN 2785-5228

EUWEB
EU-WESTERN BALKANS
Cooperation on Justice and Home Affairs



EUWEB Legal Essays

Global & International Perspectives

Issue 2/2023

EDITORIALE SCIENTIFICA

Rivista semestrale on line EUWEB Legal Essays. Global & International Perspectives
www.euweb.org
Editoriale Scientifica, Via San Biagio dei Librai, 39 – Napoli
Registrazione presso il Tribunale di Nocera Inferiore n° 5 del 23 marzo 2022
ISSN 2785-5228

This issue of the Journal intends to illustrate the activities carried out and share the scientific results achieved within the Jean Monnet Chair *Promoting Public Awareness on Enlargement, EU Values and the Western Balkans' Accession* (EUVALWEB), also collecting some of the essays and speeches delivered by our experts and young speakers.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Index
2023, No. 2

TRANSNATIONAL INVESTIGATIONS ON ENCRYPTED PLATFORMS

by Donatella Curtotti[*] and Wanda Nocerino[**]

1. Introduction

The activities on encrypted platforms, recently used by criminal organizations to conduct and plan their trafficking, are the last frontier of investigations. So, the investigators find information in "digital world" for the criminal proceedings, on the server on which all the information of users, who use encrypted communication services, flows[1].

Already from a first analysis, the investigations on encrypted platforms are very complex, operationally and legally. On one hand, it is about investigating platforms equipped with important degrees of encryption with servers often located in different parts of the world, exploiting the potential offered by the so-called big data[2]. In these cases, inevitably, the police forces need the close collaboration of the investigative bodies of other States than the one in which the investigative need originated, thereby exacerbating the already known dysfunctions of transnational cooperation[3]. On the other hand, there are critical issues of the classification nature, determined by the difficulty to identify the category in which to ascribe the activities carried out on encrypted systems.

It should also be noted that national law enforcement is clearly lagging behind other European countries, because, to date, Italy has played the role of "passive observer" with respect to the activities conducted by other countries. In fact, the national police forces have received packets of data to be analyzed and possibly used according to methods defined by others but have not carried out any autonomous investigative activity on the encrypted servers which, moreover, (at least at present) are not located on the national territory.

However, it is not far-fetched to imagine that national authorities will soon find themselves playing the role of actor in investigations into encrypted platforms.

DOUBLE BLIND PEER REVIEWED ARTICLE

[*] Full Professor in Criminal Procedure – University of Foggia (§§ 1 and 5).
E-mail: donatella.curtotti@unifg.it.
[**] Lecturer in Criminal Procedure – University of Foggia (§§ 2, 3, 4, 4.1., 4.2., 4.3.).
E-mail: wanda.nocerino@unifg.it.

[1] Surely, already through the use of the computer sensor the range of action of the interception is enormously expanded, extended to the indeterminate and indeterminable crowd of people, even unrelated to the facts of the investigation, who converse in any place; however, in the case of the *Trojan virus,* the device being monitored is determined, while when investigations are carried out on encrypted platforms, it is the *server* (in its entirety) on which the communications pass that is the object of investigation. For a first overview of the topic under examination, M.T. MORCELLA, *La vicenda dei criptofonini in attesa della decisione della Cassazione,* in *Il penalista,* 6 April 2023.

[2] M. ALAZAB, M. GUPTA (eds.), *Trust, security and privacy for Big Data*, Boca Raton, 2022; A.G. KRAVETS (ed.), *Big Data driven World: Legislation Issues and Control Technologies,* Cham, 2019.

[3] D. CURTOTTI, *Indagini hi-tech, spazio cyber, scambi probatori tra Stati e Internet provider service e "Vecchia Europa": una normativa che non c'è (ancora),* in *Diritto penale e processo,* 2021, p. 745.

ISSN 2785-5228
DOI: 10.1400/293369

It is now necessary to ask about the possibility of carrying out such investigative activities "in first person" on servers located abroad and/or in the national territory.

So, the jurist is called to understand if and in what terms the investigations on encrypted communication platforms can find use in the criminal process and identifying the correct legal framework in which the activities can be subsumed.

2. The Encrypted Communication Platforms

First of all, it is necessary to understand the functioning of cryptophones and encrypted platforms in order to more easily identify the problems of these new investigations.

A cryptophone is a type of smartphone specifically designed to provide secure communications and protect against hacking and surveillance.

More precisely, these are devices configured as company telephones which have the same appearance as traditional devices but which, in substance, do not behave as such as because they are equipped with important cryptography and encryption systems which make them invulnerable[4]. Therefore, they are "modified" smartphones that lack many features present in those on the market[5].

The entire communication network is managed through an infrastructure created by the cryptophony service provider, with servers spread all over the world, often located in "offshore" countries. Furthermore, these devices use Hardened Secure Communication Platforms (HSCP), more commonly referred to as encrypted platforms, that is operating systems and applications installed on secure and physically protected communication

[4] These platforms should not be confused with the best-known secure messaging applications, i.e. private chat applications that use encryption algorithms (end-to-end) to protect data throughout the journey from sender to recipient (such as, for example, Signal, Telegram and WhatsApp). In these cases, the data is encrypted as it is sent and then decrypted once it reaches its destination. The fundamental difference between secure messaging applications and cryptophones is that in the latter, incoming and outgoing communications are always end-to-end encrypted and are transmitted over an encrypted channel to further protect the information.

[5] In cryptophones all those services that can be easily intercepted are disabled, such as: GPS localization, Google services, Bluetooth, camera, microphones, USB port (which remains in operation only for battery charging). The use of external SD cards is also prohibited. The calls remain active but only in VoIP mode (Voice over IP), without the use of the GSM network. Messaging is also present but uses proprietary and encrypted applications.

devices. The best known are EncroChat[6] and Sky ECC[7], although there are several on the market with even more sophisticated features[8].

The purchase price is very high[9], confirming the main destination in support of illegal activities. Furthermore, in most cases, they are sold "directly", without the intermediation of known commercial suppliers but through unknown resellers, making use of the Dark and Deep Web.

From a strictly technical point of view, cryptophones use dedicated applications and services that guarantee the inaccessibility of the system and the security of the data contained therein. Among these should be mentioned:

a) Zero attack surface. All entry points of modern mobile devices – such as Google services, GSM services, SMS, Bluetooth, NFC, GPS, USB port enabled for charging only – are disabled.

b) Trusted updates. Updates are issued and digitally signed exclusively through the Secure Administration System (SAS): devices apply updates only after verifying the authenticity of the digital signature.

c) Multiple password protection. The device's storage, operating system, and secure applications are all protected by separate passphrases, each set to trigger an erasure procedure if it fails a consecutive number of times.

d) Multiple levels of encryption. Incoming and outgoing communications are end-to-end encrypted and transmitted over an Encrypted Network (VPN). The VPN configuration is dynamic and can be changed remotely by administrators. All data stored on the device is also encrypted.

e) Encrypted VoIP. Some cryptophones allow the user to disguise their voice with a number of preconfigured digital vocoders, including: robots and generic male and female voices.

f) Volatile Date. Data can be destroyed: by remote deletion performed by the dealer using the software Mobile Device Management by activating a procedure by typing in an "anti-panic" code (so-called panic or SOS code), for which the device sends an automatic message to the user's emergency contacts. This can occur after seven days (default) or even less from the last time the device was switched on; after system reboot (in some configurations); after a certain amount of time in which the device is not connected to the

[6] EncroChat is a European-based communications network and service provider that offers modified smartphones enabling encrypted communications between subscribers (about 60 thousand users). It is an OTR-based messaging app that routes conversations through a central server based in France, EncroTalk, a ZRTP-based voice calling service, and EncroNotes, which allows users to write private encrypted notes. The EncroChat encrypted messaging service and related personalized phones were discovered by the French gendarmerie in 2017, which decommissioned the platform.

[7] Sky Global is a communications network and service provider headquartered in Vancouver, Canada. Its flagship products are the Sky ECC secure messaging application and cryptophones. There are over 171,000 registered devices, mainly in Europe, North America, various countries in Central and South America – mainly Colombia – and the Middle East. A quarter of active users were in Belgium (6,000) and the Netherlands (12,000). One of its features is the self-destruction of messages after a user-defined expiration period. The system is used on specially modified phones (Nokia, Google, Apple and BlackBerry) where the camera, microphone and GPS are completely disabled; messages are encrypted and automatically deleted after thirty seconds. On 9 March 2021, France, Belgium and the Netherlands, through an investigation carried out following the establishment, in the judicial channel, of a joint investigation team, managed to violate the servers *on* which communications are kept.

[8] Think, just to name a few, to Ennetcom, Exclu, Silent phone, Zphone, X1 and X1 black from the Secure Group and the platforms from the Sikur company.

[9] The price for acquiring and managing a cryptophone is quite high (up to €1,500 - €2,000 every six months just to get a subscription for the device) and is mainly due to data roaming SIMs (dedicated SIMs other than of traditional carriers that connect to the server network made available by the service provider).

Network (for example when it is placed in a faraday bag); or if users enter their passcode four times in the calling function and then dial the number.

g) Data dissimulation. Using anti-tracking features, such as fake IMEI, IMSI and Apps to mislead police checks.

h) IMSI Catcher Detector. Detect and avoid fake base station in GSM/UMTS networks.

From an operational point of view, the investigators – not being able to directly interfere in the communication as it is equipped with impressive and almost insurmountable degrees of encryption – need to "interfere" directly on the server to acquire the information useful for the investigations.

In this context, are envisaged two investigative possibilities: proceeding with the takedown, that is the apprehension of all the data stored on the platform through the "freezing" of the server, or, by penetrating it, capturing live the flow of communications in transit.

3. The Recent Decisions of the Court of Cassation

National jurisprudence, in the wake of what is happening in other European states[10], has already expressed itself on the matter[11], with the aim of outlining a "statute" for investigations into encrypted communication platforms.

Before analyzing the content of the pronouncements that follow each other frantically on the matter, it is necessary to dwell briefly on the specific case from which the various decisions on the matter originate.

Although it is not currently possible to know the individual investigative steps that led to the apprehension of the evidence through access to the servers of the Canadian company Sky ECC, it is known that the investigation originates from a joint investigative action by the law enforcement agencies (that is a team made up of the police forces of Belgium, France and the Netherlands) conducted with the support of Europol and Eurojust, in order to acquire the content of chats exchanged through encrypted devices used to plan criminal activities on an international scale.

Materially, the acquisition of the messaging content takes place through the French authorities – place where the server of the company Sky ECC is located – according to

[10] The French Court of Cassation, taking up the decision of the *Conseil Constitutionnel* of 8 April 2022 on the constitutionality of the art. 706-102-1, recognizes the applicability of the provision to the case under examination, given that the investigators have legitimately accessed and acquired the data allocated on the server, according to the provisions of the regulatory provisions. Cass. Crim., Judgment of 11 October 2022, no. 21-85.148, in *www.legifrance.fr*, p. 1; Cass. Crim., Judgment of 25 October 2022, no. 21-85.763, in *www.legifrance.fr*, p. 2. See also the decisions of the Superior Court of Berlin and the German Federal Court which sanction the full usability of the evidentiary material obtained through the EIO See KG Berlin 2. Strafsenat, Judgment of 30 August 2021, 2 Ws 79/21, 2 Ws 93/21, in *www.gesetzeberlin.de*; *Bundesgerichtshof Beschluss*, Judgment of 2 March 2022, 5 StR 457/21, at *www.juris.bundesgerichtshof.de.* The same result is also achieved in a recent decision of the Norwegian Supreme Court. In decision HR-2022-1314-A, the judges of legitimacy admit the acquisition of computer data through collaboration between police forces. See Supreme Court of Norway, Judgment of 30 June 2022, HR-2022-1314-A, at *www.domstol.no*.

[11] It should be noted that the jurisprudence of legitimacy has ruled on the subject with various more or less contemporary decisions. Court of Cassation, Section IV, 5 Judgment of April 2023, no. 16347; Court of Cassation, Section VI, Judgment of 25 October 2022, no. 48330; Court of Cassation, Section I, Judgment of 13 October 2022, no. 6363; Court of Cassation, Section IV, Judgment of 15 July 2022, no. 32915, in *Giurisprudenza penale*, with note by A. BARBIERI *The usability limits of encrypted messages downloaded from a foreign server and acquired through a European investigation order*; Court of Cassation, Section I, Judgment of 1 July 2022, no. 34059.

the provision of art. 706-102-1 of *Code de procédure pénale*, which allows to access, store, record and transmit data stored on computer systems[12].

The operation does not remain confined to the countries directly affected by the operation in question: in fact, in various national criminal proceedings, the need emerges to acquire, through the European Investigation Order (EIO), the transcript of the messages exchanged by subjects operating on Italian territory.

In this context, the judges of legitimacy[13] were called to decide on the limits of use procedural of the "pre-established data", that are the contents of the messages exchanged through cryptophones procured by the police forces of other European states and acquired through the EIO.

More specifically, the Court is faced with the issue from a dual point of view: on one hand, it intervenes to define the correct legal framework for the acquisition of chat content on encrypted platforms, and, on the other, to determine the ways in which the data obtained abroad can pass through the criminal process.

Under this first aspect, the judges of legitimacy[14] underlined the need to distinguish two different types of operations that investigators can carry out to acquire information on encrypted platforms. Precisely, it is possible both to capture and record the encrypted message while it is in transit from the sender's device to that of the recipient, and to acquire data after decrypting the content of the conversations to transform mere computer strings into intelligible communicative data. In their opinion, in the first case there is an hypothesis of telematic interception, pursuant to art. 266-*bis* of the Italian Code of Criminal Procedure, given that the collection concerns communication flows in transit; in the second, the archived messages can be subsumed in the context of documentary evidence, which can be acquired according to the provisions of art. 234 of the Code of Criminal Procedure.

On the basis of this reasoning, the judges clarified that, in the present case, the activity of acquiring and deciphering the communication data located on foreign servers cannot fall within the category of interceptions, since instead they are computer documents that can be fully used in compliance with the provisions pursuant to art. 234-*bis* of the Code of Criminal Procedure[15].

With reference to the acquisition methods, for the Court[16], electronic documents can be obtained and used in the national criminal trial through the EIO, an investigative cooperation tool to be used to facilitate the circulation of evidence in EU countries.

---

[12] The rule (modified by art. 46, Law 23 March 2019, no. 2019-222) states that: "*It may be necessary to set up a technical device whose purpose, without the consent of the interested parties, is to access, anywhere, computer data, to record, store and transmit them, as well as that they are stored in a computer system, such as are displayed on a screen to the user of an automated data processing system, as he introduces them by entering characters or as they are received and transmitted by peripherals. The public prosecutor or the investigating judge may appoint any natural or legal person authorized and registered in one of the lists envisaged by article 15T, in order to carry out the technical operations which allow the creation of the technical device referred to in the first paragraph of this article. The public prosecutor or the judge may also prescribe the use of state resources subject to national defense secrecy according to the forms provided for in Chapter 1 of Title IV of Book 1*".

[13] *Infra*, nt. 11.

[14] Court of Cassation, Section I, Judgment of 1 July 2022, no. 34059, cit.; Court of Cassation, Section I, Judgment of 13 October 2022, no. 6363, cit.

[15] It is not superfluous to specify that the data are located in a foreign state (namely France) and are "owned" by the state which gives its consent to the acquisition of the same.

[16] Court of Cassation, Section VI, Judgment of 25 October 2022, no. 48330, cit.

In this case, according to the majority jurisprudence (in five out of seven rulings)[17], the compatibility of the process of acquiring probative data with the right of defense is not frustrated by the choice of the prosecution to make available only the results of the activity carried out abroad and not also the process of acquiring those data[18], given that the foreign judicial authority has guaranteed compliance with the correct procedures for acquiring the computer data aimed at preventing its alteration[19].

4. The Compatibility with the Proceedings' Rules of Evidence

The legitimacy of the investigative documents deriving from the investigations on encrypted communication platforms is closely connected to the legal qualification recognized to them. In fact, only if such acts fall within the probative categories already tested by the system, there would not be precluded the possibility of using investigative acts in the trial.

Hence, given the centrality of the topic in the future debate, the compatibility of the activities carried out on the encrypted platforms with the institutes typified by the legislator will be verified in the continuation of the discussion.

One fact, however, should be immediately underlined: the differential profiles of the investigative technique compared to the "traditional" probative categories make the subsumption of the activities carried out on the encrypted platforms into the context of the evidence-seeking means already known to the system complex. And yet, unable to surrender to the idea that new investigations end up being unprofitable due to old legislation, the interpreter must make an interpretative effort to adapt, in compliance with the principles of the legal system, the current legislation to the new challenges of the 'modern era.

Beyond the difficulties highlighted, further criticalities are found in relation to the "place" where the server is located, given that, if this were located beyond the borders of the national territory, the investigative cooperation tools would come into play which, as best it will be said below, they are not always suitable for guaranteeing the transnational collection of computer data. Therefore, we will try to discern three possible scenarios of intervention that differ according to the place where the server on which the data to be

[17] The consideration of the judges of legitimacy is relevant, for which "*(...) the use of that form of cooperation which, for the purpose of acquiring evidence within the European Union, is represented by the EIO, is governed by the d Legislative Decree 27 June 2017, no. 108, issued to implement directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014. The sixth recital of this directive states that in the Stockholm program, adopted by the European Council of 10-11 December 2009, the European Council considered further pursuing the establishment of a global system of obtaining evidence in cases with a cross-border dimension, based on the principle of mutual recognition*". Court of Cassation, Section I, Judgment of 13 October 2022, no. 6363, cit.

[18] Specifically, the lawyer complains that the prosecutor has made available to the defense only the results of the police activity carried out, without sharing the path (that is the investigative documents) that led to the acquisition of the decrypted chats and, in particular, the Europol documentation (with decrypted files) with precise indication of the data acquisition methods on the *server* and the attached police reports. See Cassation, Section VI, Judgment of 25 October 2022, no. 48330, cit.

[19] In an isolated ruling (Cass., Section IV, Judgment of 15 July 2022, no. 32915, cit.), the Court maintains that the acquisition of the probative data (the decrypted *chats) is unusable, since the right to* defence. Precisely, the Cassation states that the principle of the adversarial process implies a procedural dialectic not only on the results of the acquired material, but also on the methods with which said material was acquired. It follows that, *pursuant to* art. 191 Code of Criminal Procedure, evidence is useless if it violates the prohibitions established by law. In conclusion, for the judges of legitimacy, the defense enjoys the right to access the documentation of the investigative activity carried out and to know the ways in which these encrypted messages were acquired, by virtue of the observance of the right of defense and of hearing.

learned is located is located, distinguishing, for each hypothesis, the activities that can be carried out according to whether they are conducted from Italy as "passive observer" – i.e. when the results of investigations carried out by other countries are requested, or pre-established data – or whether it concerns "live" investigations conducted by the national state.

4.1. Investigations on Servers Located in Italy

The first hypothesis to be examined pertains to the case in which the server on which the encrypted communications transit is located on the national territory.

In this context, it is necessary to distinguish according to whether the acquisition of communications takes place at the same time as the transmission of the information, or, at a time subsequent to the communication exchange.

By limiting the analysis to the hypothesis in which the acquisition action is "live", the probative category with which it seems appropriate to deal with is represented by telematic interceptions, regulated by art. 266-*bis* of the Code of Criminal Procedure[20], which, as known, have as their object a "*flow of communications relating to computer or telematic systems or between multiple systems*"[21], i.e. between computers connected to each other on the Net, via modem, via radio (if the devices are connected with wireless technology) or with any other form of interconnection.

Certainly, from a technical-operational point of view, access to a server to capture communications in progress can be included in the context of telematic interceptions, the character of the contextuality of the capture of a communication flow between systems connected on the Network being highlighted.

However, even if we want to assimilate these captive forms to "classic" interceptions, it cannot be denied that the formers are characterized by significant peculiarities, resulting in being much more intrusive for those subjected to them.

It will be agreed that it is one thing to capture telematic flows between two or more systems subject to interception, but it is quite another to directly access the server on which all the communications of all users who use that service pass. From here, it could be doubted that these activities can be traced back to the discipline of art. 266 bis Code of Criminal Procedure, which, as specified, "*allows targeted limitations*"[22].

If this is an acceptable exception, an "evolutionary" interpretation of the regulatory provision seems possible, moreover suggested by the jurisprudence of the ECHR, for which "*it must be considered sufficient that the authorization decree indicates the recipient of the collection and the type of environments where this is conducted*"[23].

---

[20] M. TORRE, *L'intercettazione di flussi telematici (art. 266* bis *c.p.p.),* in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (eds.), *Cybercrime,* Turin, 2019, p. 1472.

[21] The "flow" can be defined as the succession of ongoing communications within a system or between multiple computer systems, between which it is possible an exchange of impulses that transmit information. By "IT system" we mean any set of equipment intended to perform any function useful to man through the use of IT technologies. Communications between computer systems – which take the form of digital signals (binary data or bits) – take place along non-telephone lines, such as those used to connect, with the aid of special equipment (servers), various computer workstations (Local Area Network). In a telematic system, on the other hand, data transmission takes place along the telephone, television or satellite line. A similar differentiation is endorsed by the jurisprudence of legitimacy. Court of Cassation, Section V, Judgment of 8 January 2020, no. 4470, in *C.E.D.*, no. 277855.

[22] L. FILIPPI, *art. 266* bis, in A. GIARDA, G. SPANGHER (eds.), *Codice di procedura penale commentato,* Milan-Padua, 2023.

[23] On this point ECHR, Judgment of 4 December 2015, Application no. 47143/06, *Roman Zakharov v. Russia*.

Reasoning in this way, the server could be considered as a container on which communication flows pass to be paid attention to, not unlike a smartphone or computer.

In other words, one could go so far as to say that this capture represents an evolution of "traditional" telematic interception having as its object communication flows transiting on a new "computer system", i.e. the server, given that it is precisely that space that has to be "monitored" because the crime is committed (presumably) in the new virtual environment.

The approach is partially different in the case in which the investigators decide not to proceed with "live" captures of a communication flow in transit on computer systems but acquire pre-established data directly "at the source", through apprehension of the server as the body of the crime.

As clarified by the jurisprudence of legitimacy[24], messages stored in the memory of a mobile phone must be considered documents, pursuant to art. 234 Code of Criminal Procedure, given that the same "*do not fall within the concept of 'correspondence', as the latter implies a shipping activity in progress or in any case started by the sender by delivery to third parties for delivery (...) ; nor can it be considered that these are the results of an interception activity ' which foresees, by its nature, the capture of an ongoing flow of communications. (...) the data present in the telephone memory acquired ex post constitute mere documentation of said flows* "[25].

Consequently – according to the Court[26] – the acquisition of such texts cannot be subjected either to the rules applied for the seizure of correspondence (art. 254 Code of Criminal Procedure), nor to the provisions concerning telematic interceptions (artt. 266 bis Code of Criminal Procedure), but to the discipline referred to in art. 253 Code of Criminal Procedure, since they are electronic documents with a communicative content[27].

Following a similar reasoning, when messages stored on the server are acquired, the related activity cannot be subject to the regulation established for correspondence. In this case, in fact, the server is "freezed" as an information container to acquire *ex post* data stored in a macro container that documents communication flows that have already taken place. Hence, at least from a technical-operational point of view, the related activity could be included in the context of the probative seizure of computer data, according to the provisions of art. 253 Code of Criminal Procedure.

However, it must be emphasized that even this approach can be critical. Indeed, as known, the probative seizure decree must contain a specific motivation on the purpose pursued for the ascertainment of the facts[28] and must be aimed at apprehension only of what is actually useful for the purposes of the investigation[29], in full compliance with the principle of proportionality[30].

However, it should be highlighted that even this "rule" suffers from exceptions: in some rulings, in fact, the Court of legitimacy excludes the violation of the principle of

[24] Court of Cassation, Section VI, Judgment of 6 February 2020, no. 12975.
[25] Cassation, Section I, Judgment of 2 December 2020, no. 461.
[26] Court of Cassation, Section VI, Judgment of of 28 May 2019, no. 28269, cit.
[27] The IT document, *especially* the digital proof, is a non-paper document formed by the programs (software) of an electronic computer and, simultaneously, with its formation, recorded in a special space by the computer itself (hardware) or on instruments electronic or digital media. An IT document could therefore be defined as "*any file having a representative element expressed in a binary language*". So P. TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico,* in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (eds.), *Cybercrime, op. cit.*, p. 1308.
[28] Court of Cassation, Unified Sections., Judgment of 19 April 2018, no. 36072, in *Processo penale e giustizia,* 2019.
[29] M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale,* in *Diritto penale contemporaneo*, 18 June 2014.
[30]Court of Cassation, Section VI, Judgment of 22 September 2020, no. 34265.

proportionality where the seizure of the entire contents of a computer system is required by specific evidentiary requirements which they come into relief on the basis of the peculiarities of the crime for which the proceeding is taking place[31].

Consequently, there would be no impediments to the acquisition of a server (and its contents) when the decree ordering the measure contains the precise indication of the reasons justifying the extension of the apprehension, in such a way as to allow a posthumous check on the proportionality of the constraint placed on the IT data.

4.2. Investigations on Servers Located in EU Countries

The second hypothesis to consider pertains to the case in which the server is located in a member state of the European Union; hypothesis, indeed, much better known in judicial practice and addressed on several occasions by national courts[32].

The undisputed reference point of EU investigations is represented by the EIO which, for some time now, has overwhelmed traditional forms of cooperation when the investigation is relegated to the borders of the European Union[33].

With the establishment of the EIO, the executive procedure of cross-border interceptions is regulated, even if carried out electronically, to be carried out when the device (or system) to be controlled is located in a Member State[34].

In fact, both Directive 2014/41/EU[35] and Legislative Decree 108/2017[36] devote particular attention to the institution in question, referring, in particular, to "*telecommunications interceptions*" [37], here to be understood as tapping of conversations or communication flows that make use of the aid of technical tools, such as the telephone or the computer .

In this sense, even the capture of communication flows in transit on servers located abroad can be assumed in the context of telecommunications interceptions and, therefore, can be carried out through recourse to the EIO

If, however, the investigative operation is not assigned to the request for testing telematic interceptions abroad but is aimed at the acquisition of "pre-established" information, i.e. evidence that represents the result of investigative activities carried out in other countries, the procedure is partially different.

Following the reasoning already conducted with reference to the acquisitions on servers located in Italy[38], the activity of capturing messages archived on encrypted

[31] Court of Cassation, Unified Sections, Judgment of 20 July 2017, no. 40963..
[32] This is the case dealt with by the jurisprudence of legitimacy. Cfr. para. 3.
[33] A. CABIALE, *I limiti alla prova nella procedura penale europea*, Milan-Padova, 2019, p. 250.
[34] With reference to cross-border wiretapping, Recital no. 31 of Directive 2014/41/EU, establishes that "*(If) more than one Member State is able to provide the necessary technical assistance, the EIO should be sent only to one of them and priority should be given to the Member State where the person concerned is located. The Member States where the person subject to interception is located, and whose technical assistance is not needed to carry out the interception, should be notified in accordance with this Directive. However, although technical assistance cannot be received by a single Member State, the EIO can be sent to several executing States*".
[35] The directive addresses the issue of interceptions both in Recitals nos. 30-31, which, especially in Chapter V, in arts. 30 and 31, entitled "*Interception of telecommunications*".
[36] More precisely, in arts. 23-25 the rules are inherent to the passive procedure, while in arts. 43-45 they are dedicated to the active procedure.
[37] As stated, in Recital no. 30 of Directive 2014/41/EU states that "*the possibilities to cooperate in accordance with this Directive on telecommunications interception should not be limited to the content of telecommunications, but should also concern the collection of traffic data and associated with such telecommunications, so that competent authorities can issue an EIO to obtain less intrusive telecommunications data (...)*".
[38]Cfr. para. 4.1.

platforms cannot be subjected to the discipline of interceptions (lacking the contextual nature of the communication).

From this point of view, the EIO is functional in collecting the results of investigative measures already carried out in the territory of the foreign State, according to the provisions of art. 234 bis Code of Criminal Procedure, because they are documents with a communicative content.

4.3. Investigations on Servers Located in non-EU Countries

The last case to be examined pertains to the hypothesis – anything but far-fetched – in which the server is located in non-EU countries.

Generally, when it is necessary to carry out an investigative activity in a State which does not fall within the "competence" of the European Union, the form of international cooperation to be used is the rogatory letter, according to the provisions of article 727 Code of Criminal Procedure. It is an instrument of judicial assistance that can be invoked – at least in the abstract – whenever the interception has as its object utilities located in part or wholly in a non-EU State.

In order to verify its compatibility with the "live" acquisition of communications in transit on encrypted platforms, it is first of all necessary to dwell on the physiognomy that the institution of the rogatory has assumed in recent years.

Generically, the rogatory has become a form of "residual" cooperation to be used only to pick up conversations and communications "foreign to foreign" not passing through Italian nodes, or carried out without the aid of the so-called telephone bridges[39]. On the contrary, when the telephone traffic is picked up from Italy (regardless of where the user is located), the conditions of the rogatory are not outlined but of the so-called routing[40].

This investigative technique allows the perception of communications that depart from Italy and are directed to a specific foreign user, or to a bundle of users belonging to a geographical district which includes a city located abroad, with the possibility of simultaneous use of telematic flows in different places and countries and evident trespassing in the perception of the communicative contents of subjects outside the national jurisdiction.

In these cases, as clarified by the jurisprudence of legitimacy[41], it is not necessary to resort to international cooperation techniques since the investigation must be qualified as internal and not managed by the foreign State.

Therefore, what is relevant for the purposes of predicting forms of legal assistance is not the place of collection but of acquisition of the results learned through interception: thus, if the evidence is found abroad but, thanks to technology, it becomes possible to learn them in Italy, the investigation must be classified as "internal".

Although the perimeter of the institute – at least in its traditional guise – has found an almost stable sedimentation in doctrine and in jurisprudence, the question is not easy to solve when, in the experiment of cross-border investigations, the investigators make use of new tools or new investigation techniques.

In these cases, it is not at all easy to identify the distinction between rogatory and routing, posing interpretative difficulties both with reference to verifying the need to

[39] On the subject, extensively, S. ALLEGREZZA, F. NICOLICCHIA, *L'acquisizione della prova all'estero e i profili transnazionali,* in G. CANZIO, L.D. CERQUA, L. LUPARIA (eds.), *Diritto penale delle società*, Padua, 2014, p. 1275.

[40] Very critical of the use of the routing technique, F. RUGGIERI, *Le intercettazioni "per instradamento" sul canale internazionale: un mezzo di ricerca della prova illegittimo,* in *Cassazione penale,* 2000, p. 1062.

[41] Court of Cassation, Section III, Judgment of 3 March 2016, no. 25833.

resort to forms of international cooperation, and with regard to the type of assistance to be requested.

This criticality seems to have been recently overcome by the jurisprudence of legitimacy: even if with reference to the interceptions carried out through the computer interceptor, the Court specifies that "*the environmental interception by means of a computer virus installed in Italy on a telephone connected to a national operator , does not require the activation of an international rogatory for the mere fact that the conversations are partially carried out abroad, and temporarily recorded via local wifi, (...) given that the tapping originated and was in any case carried out in Italy, through the reception centers at the Public Prosecutor's Office*"[42].

The reason for such an approach derives, according to the Court, from the awareness of the slowness of the rogatory procedure which, evidently, does not reconcile with the speed of computer investigations.

A similar approach could also find use in the case of "live" investigations carried out on encrypted platforms : in these circumstances, in fact, it seems possible to resort to the routing technique, since the rogatory procedure does not have to be activated, given that the recording of data allocated abroad represents only a segment of a more impressive investigation activity which, in fact, takes place on the territory of the State. The decryption of communications following the "storage" of the data represents, in fact, the final phase of the more complex executive process of the interception activity which, evidently, is carried out in Italy at the servers of the Public Prosecutor's Office.

Conversely, a similar conclusion cannot be reached if the investigation has as its object the acquisition of data stored on servers located in non-EU countries: in these cases – when the acquisition does not concern communication flows in transit – the apprehension of the information useful for ascertaining the facts in a criminal trial established in Italy must take place through the international letter rogatory[43].

The only exception to the rule occurs in the event that the data owner spontaneously transfers the data obtained through an internal investigation: as also clarified by the legitimacy jurisprudence, "*(...) the information and documents transmitted autonomously by the judicial authority of a State foreign countries are usable in criminal proceedings, since, in such cases, the special discipline envisaged by art. 729, paragraph 1, Code of Criminal Procedure for letters rogatory from abroad*"[44].

5. Investigative Usefulness *vs* Fundamental Rights

Finally, the research focuses on the implications deriving from the use of new investigative techniques in the investigative reality.

Is it conceivable that the world of law and, more particularly, that of investigations closes its doors to the avant-garde technological reality?

On this point of view, it does not seem conceivable an "intermediate" solution: in fact, one must choose between the alternative of denying the entry of new scientific and technical discoveries into the criminal trial, or admitting their use even at the cost of sacrificing fundamental rights.

Faced with such a radical choice, the jurist is called to come to terms with the contingent reality, having to acknowledge that, while determining an interference with the enjoyment of the individual prerogatives recognized and protected by the

[42] Court of Cassation, Section II, Judgment of 22 July 2020, no. 29362.
[43] Court Cassation, Section VI, Judgment of 20 April 2021, no. 18907.
[44] Court of Cassation, Section I, Judgment of 16 June 2022, no. 354.

Fundamental Charter, the results obtainable through the tools offered by the technology are very effective in repressing the most advanced types of crime, so it is unthinkable that the penal system should remain completely free of them.

On the other hand, the use of modern collection techniques responds to the need to contain criminal phenomena, protecting the more general need for individual and collective security[45], as a constitutional asset "*inextricably linked to life, physical safety, well-being of the man and to the quality of his existence, as well as to the dignity of the person*"[46].

In this sense, it seems that the enigma can find a solution through the recognition of the value that must be considered "primary": there are those who believe that the need for security and the repression of crime represents the fundamental legal asset, whose protection legitimizes "*a clear restriction or* [...] *the complete cancellation of the guarantees of the subjects involved*"[47] and who, conversely, deems it essential to consider the existence of a nucleus of inviolable rights which, regardless of the context, cannot be subjected to compression[48].

In reality, neither of the two prerogatives seems to be able to pose as pre-eminent over the other: freedom and security do not represent conflicting values but two sides of the same coin, equally worthy of protection for the established order[49].

Therefore, since it does not seem possible to operate on the basis of a "hierarchical" criterion, the modern jurist finds himself having to operate a complex balance between the two rights. Consequently, the jurist's objective is to find the delicate balance between the need to repress crimes, facilitated by the frequent use of new investigative tools, and the protection of inviolable individual rights.

Consequently, the point of reference is the principle of proportion of the measure with respect to the purpose, in the sense that any restriction of fundamental rights cannot be excessive with respect to the seriousness of the reasons justifying it[50].

The scrutiny of reasonableness and proportionality therefore requires verifying that the balancing of constitutionally relevant interests has not been achieved in such a way as to determine the sacrifice or compression of one of them to an excessive extent and therefore incompatible with the constitutional provision.

Indeed, in this renewed system which imposes the centrality of inviolable rights, it seems that the canon of proportionality increasingly represents the central moment of verification in which the complex judgment of legitimacy of national provisions limiting

---

[45] Doctrine, especially constitutional law, has long questioned the definition of "security" and its constitutional foundation. For G. CERRINA FERONI, G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi costituzionali*, no. 1, 2018, p. 1 ff., "security is not only a constitutional right, but '*a super-primary value*'". For P. ZANON, *Un diritto fondamentale alla sicurezza?*, in *Diritto penale e processo*, 2019, p. 1555, "*security is also a full-fledged personal and primary right, perfectly in line with the rule of law*".

[46] G. CERRINA FERONI, G. MORBIDELLI, *La sicurezza: un valore superprimario*, cit., p. 3 ff.

[47] A.M. DERSHOWITZ, *Why Terrorism Works. Understanding the Threat, Responding to the Challenge*, Yale, 2002.

[48] R. ORLANDI, *Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali*, in *La giustizia penale preventiva. Ricordando Giovanni Conso*, Milan, 2016, p. 17 ff.

[49] A. MARANDOLA, *Sicurezza e diritti fondamentali: aspetti processuali*, in *Processo penale e giustizia*, 2019, n. 11, p. 1553 ff.

[50] Cfr., E. COTTU, *Giudizio di ragionevolezza e vaglio di proporzionalità della pena: verso il superamento del modello triadico?*, in *Diritto penale e processo*, 2017, p. 473 ff.; A. MACCHIA, *Il controllo costituzionale di proporzionalità e ragionevolezza*, in *Cassazione penale*, 2020, p. 19 ff.; V. MANES, V. NAPOLEONI, *La legge penale illegittima*, Turin, 2019, p. 362 ff.; D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Rivista italiana diritto e procedura penale*, 2020, n. 1, p. 3 ff.

individual prerogatives is articulated. And this decision must take place precisely through weightings relating to the proportionality of the means chosen by the legislator in its unquestionable discretion with respect to the objective needs to be met or the purposes it intends to pursue, taking into account the circumstances and limitations that actually exist.

6. Possible Scenarios

In the light of the foregoing, considerations of a systemic nature can be drawn which offer new insights for the jurist.

From a more strictly procedural point of view, it is considered essential to introduce a discipline capable of regulating the new forms of investigation with high technological potential, taking into account the balance between the various interests that may come into conflict.

Precisely, since it is not conceivable to leave the choice of indiscriminate recourse to new investigation techniques to the availability of the investigators and not even to legitimize their use in jurisprudential terms through extensive interpretations in a matter governed by a rigid principle of mandatory nature, the need is felt for a intervention of the legislator, called to typify the complex of activities that can be carried out through new digital investigative techniques, in such a way as to make the limitations on individual prerogatives "tolerable" in a democratic society.

In this case, one could lean towards the introduction of a new means of researching evidence (access and acquisition of big data on computer or telematic systems, it could be called) to regulate access, observation and acquisition of data and information found on the new virtual spaces: in these cases, the instrument with which to carry out computer investigations would not be typified but rather the rules to be applied whenever one proceeds with covert and continuous remote surveillance activities, arranging the fundamental guarantees that must always be recognized to the suspect and to third parties occasionally involved, regardless of the investigative technique used.

In other words, the objective could be to introduce a new category of evidence, with which the "cases" and "ways" of interference in the private sphere of individuals would be identified, so as to consider the sacrifice of inviolable rights as absolutely respectful of the principle of strict legality and the principle of proportion.

Furthermore, from a supranational perspective, the preparation of a uniform regulation on the circulation of digital data would be desirable.

More concretely, in the context of the Proposal for a regulation of the European Parliament and of the Council relating to European orders for the production and conservation of electronic evidence in criminal matters (so-called E-Evidence Regulation)[51], it could be envisaged the introduction of a procedure aimed at facilitating the exchange of information acquired abroad (in EU countries) through investigations carried out using new investigation techniques and, at the same time, prepare a standard built on the model of the dictates referred to in art. 270 of the Italian Code of Criminal Procedure, identifying limits and common prospects for acquiring the results of water collection in States other than those for which they were authorised.

[51] This is the Proposal for a Regulation of the European Parliament and of the Council, *on European orders for the production and conservation of electronic evidence in criminal matters*, of 17 April 2018, COM (2018) 225 final.

ABSTRACT

Investigations on the encrypted platforms are one of the main challenges for environmental law enforcement. The technical difficulties – being platforms equipped with important degrees of encryption, with servers often located in different countries of the world – are accompanied by critical issues of a legal nature in relation to the correct legal classification. The objective of the research is to verify the compatibility of the investigations carried out on encrypted platforms with the already existing evidentiary categories, in order to ascertain the existence of a regulatory coverage suitable for guaranteeing the constitutional and legal integrity of the evidence thus collected.

KEYWORDS

Cooperation, Evidence, Investigation, Interception, Surveillance.