Cross-Border Gathering of E-Evidence: Different Legal Frameworks in European Union and Council of Europe

PhD Silvia Signorato*

Abstract

In a world of borders, the Internet has no borders. This is one of the reasons why the need for cross-border gathering of e-evidence is increasingly frequent. The article is aimed at identifying the legal instruments for cross-border collecting of e-evidence. For this purpose, the main legal sources of the European Union and the Council of Europe are analysed. Furthermore, the article is aimed at providing the reader with a roadmap for orientation in this matter. In this perspective, the following hypotheses are analysed: 1) The collection of publicly available e-evidence or for which there is consent to the collection and the relationship of these investigations with Article 32 of the Budapest Convention; 2) The collection of e-evidence with direct request to service providers based on the Second Additional Protocol to the Budapest Convention on Cybercrime of the Council of Europe, and the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters; 3) The gathering of e-evidence on the basis of bilateral and/or multilateral agreements; 4) The gathering of e-evidence according to the European Investigation Order in criminal matters (EIO); and 5) The gathering of e-evidence in states where EIO does not apply.

Keywords: *cross-border collection of e-evidence; sources in matters of e-evidence in Europe; Second Additional Protocol to the Budapest Convention on Cybercrime; Regulation (EU) 2023/1543; Directive (EU) 2023/1544*

I. Introduction: a world of borders and collection of evidence across borders

In Europe, after many years of war, the peace of Westphalia was reached in 1648. This peace contributed to the identification of the concept of territory as circumscribed by borders. In particular, the border took on a double meaning: 'inclusive' for those who are within the border; 'exclusive' for those who are outside the border.

This distinction reverberates between the concepts of 'internal' and 'external' inherent in the collection of evidence in other countries. This distinction implies that the competent authorities can carry out investigations inside the territory of their state for the purposes of the prevention and repression of crime.

However, they cannot carry out investigations in the territory of other states. In fact, if it is necessary to gather evidence abroad, the judicial or police authority of the state must first of all verify whether its jurisdiction exists. If it exists, as a rule[1], it cannot

* Associate Professor in Criminal Procedure, University of Padua, Italy; lecturer in Criminal Procedure, University of Innsbruck, Austria. Contact: silvia.signorato@unipd.it.

gather evidence directly in another state, but will have to activate the judicial cooperation instruments in criminal matters[2].

At first glance, one might think that the member states of the European Union (later on, simply EU member states) could collect evidence in other States without activating the Police and judicial cooperation in criminal matters. This is because Article 3 of Consolidated versions of the Treaty on European Union provides for the creation of an area of freedom, security and justice without internal frontiers. However, this area is functional to the free movement of persons and has not yet been completed as regards the collection of evidence. As a result, since the borders between the member states still remain, it is necessary to resort to Police and judicial cooperation in criminal matters even if the collection of evidence has to take place in another EU member state.

II. E-evidence and data retention

Information and communications technology (ICT) is widespread and pervasive in every sector of human activity. Indeed, the distinction between online and offline now seems to tend to dissolve and be replaced by the 'OnLife dimension'[3].

An electronic evidence (or digital evidence), hereinafter simply e-evidence, is any probative information stored or transmitted in digital form. The growing pervasiveness of ICT implies that the need for cross-border collection of e-evidence often emerges as investigations are carried out[4].

In particular, it may happen that an e-evidence is located on a device located abroad; this is the case, for example, of photographs or digital documents stored on a computer located in another state.

More frequently, however, the e-evidence is found across the border not because the devices are abroad, but because the servers that people use to store information or to communicate through social networks are located abroad (this is the case of WhatsApp, Facebook, Mastodon, Telegram etc.). Consequently, even if the communication takes place between two people both located in the same state, the data are stored not only in the users' devices[5] but also in the foreign state in which the server is located.

---

[1] Exceptions include the joint investigation teams provide by the Council Framework Decision of 13th of June 2002 on joint investigation teams (2002/465/JHA) and the regulations provided by Article 32 of the Convention of Budapest. See C. Rijken, G. Vermeulen G., (Eds.), *Joint Investigation Teams in the European Union. From Theory to Practice,* Springer, 2006, pp. 1-248.

[2] See W. Bogensberger, *Chapter 4. Judicial Cooperation in Criminal Matters*, in M. Kellerbauer, M. Klamert, J. Tomkin, (Eds.), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Oxford Academic, 2019.

[3] See L. Floridi, *The Onlife Manifesto*, in L. Floridi, (Ed.), *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Cham, 2015, pp. 7-13.

[4] The importance of this kind of evidence is destined to increase more and more. Furthermore, new investigative possibilities (but also new issues) are related to the use of artificial intelligence (AI) for the collection of evidence. Discussions on the application of AI in collection of evidence can be found in S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*. Springer, 2023; and in L. Stanila, *Living in the Future: New Actors in the Field of Criminal Law – Artificial Intelligence*, in *Legal Science: Functions, Significance and Future in Legal Systems II. The 7th International Scientific Conference of the Faculty of Law of the University of Latvia 16–18 October 2019*, Riga Collection of Research Papers, 2020, pp. 300-312.

[5] Moreover, only some data are stored in the users' devices.

Traffic data are considered so important for investigative purposes that states have specific data retention laws. Before introducing the concept of data retention, it is necessary to define the concept of traffic data; 'traffic data means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service'[6].

The law that disciplines the type of data, the methods and the period of their retention for the purposes of prevention and prosecution of criminal offenses is called 'data retention'[7]. In particular, data retention is a concept different from 'data preservation' (or 'quick freeze') disposed against a suspect[8]. This is also because the data retention discipline is not about processing data from a suspect but from every person instead. Data retention is an important instrument when a crime is committed. For example, think of the importance that the localization data of the cell to which a subject's mobile phone is connected can have in order to understand whether he/she is the perpetrator of a crime (e.g. a murder or a robbery).

Given the importance that these data can have, the states impose their retention to the providers of publicly available electronic communications services or of a public communication network. There is, however, a problem because each state has specific data retention rules which may differ from those of other states. In particular, the most significant difference concerns the data retention periods. These differences certainly do not facilitate the prosecution of crimes. However, all data retention laws of all EU member states are characterized by a fundamental common factor: No data revealing the content of the communication may be retained pursuant to data retention. In relation to this, it should be noted that the distinction between communicative contents and non-communicative contents is not always clear[9].

Finally, it should be noted that the terms 'collection of evidence' and 'gathering of evidence' are considered to be equivalent here.

III. A different legal framework in the Europe of the European Union and in the Council of Europe one

In a world of ever faster dynamics, investigations should also be characterized by the rapid collection of evidence, even in cases where such evidence must be collected abroad.

---

[6] See Article 1 of the Convention on Cybercrime of Council of Europe, 23.XI.2001.

[7] See H. Matsumi, D. Hallinan, D. Dimitrova, E. Kosta, P. de Hert, (Eds.), *Data protection and privacy: In transitional times.* Bloomsbury Publishing, 2023; S. Signorato, *Data retention, a balance between judicial requirements and the risk of illegality,* in Provincial Protector of Citizens-Ombudsman, Institute of Criminological and Sociological Research (Eds.), *Human Rights Protection "From Unlawfulness to legality"* (1), 2018, pp. 447- 456; S. Signorato, *Streamlining the Fight Against Child Sex Offenders Trough EU Regulation of IP address* in *Journal of Eastern-European Criminal Law* no. 1/2020, pp. 77-86; and S. Signorato, *Combating terrorism on the internet to protect the right to life. The regulation (EU) 2021/784 on addressing the dissemination of terrorist content online*, in Provincial Protector of Citizens, Ombudsman (Eds.), *Yearbook. Human rights protection. The right to life.* Vojvodina Provincial authorities Common Affairs Department Novi Sad, Republic of Serbia, 2021, pp. 403-408.

[8] See Article 16 of the Convention on Cybercrime, and European Commission (2011). *Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive* (Directive 2006/24/EC): 5.

[9] See L. Bachmaier Winter, *Criminal Investigation and Right of Privacy: The Case-law of the European Court of Human Rights and Its Limits*, in *Lex ET Scientia*, Juridical Series (II), 2009, p. 12.

Regarding this aspect, there are different attitudes in the various states. Some of them appear to be so xenophilic that, if the collection of evidence is requested by another state, they carry out this collection even more quickly than a collection relating to an investigation within the state. Conversely, other states tend to cooperate very little.

For this reason, Article 12.1 of the EIO provides that 'The decision on the recognition or execution shall be taken and the investigative measure shall be carried out with the same celerity and priority as for a similar domestic case and, in any case, within the time limits provided in this Article'.

The need for a fast collection of evidence emerges particularly in the case of e-evidence, given that such kind of evidence is easily alterable, perishable, and eliminated.

It is therefore necessary to verify whether, at a European level, there are sources that specifically regulate the cross-border collection of e-evidence.

In dealing with European sources, it must first be specified that, even if we often speak generically of Europe, it is instead necessary to distinguish between the European Union and the Council of Europe.

The European Union (EU) has legal personality and 27 states, named EU member states, belong to it. They are: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden. The EU has a complex structure. Specifically, there are four main decision-making institutions: the European Parliament; the European Council; the Council of the European Union; and the European Commission. There are also other institutions and bodies, which include the European Central Bank, and the European Court of Auditors. Finally, the EU's judicial body is the Court of Justice of the European Union.

There are many EU sources of law. Usually, they are distinguished either as primary legislation of the European Union or as secondary legislation of the European Union.

The following are part of the primary legislation of the EU: Treaty on European Union (TEU), Treaty on the Functioning of the European Union (TFEU), and their protocols; Charter of Fundamental Rights of the European Union[10]; Treaty Establishing the European Atomic Energy Community (Euratom), which is still in force as a separate treaty; international agreements; general principles of union law.

The following are part of the secondary legislation of the EU[11]: Regulations, Directives, Decisions, recommendations, and opinions. In particular, a regulation is a binding legislative act and must therefore be applied in all member states. Instead, a directive indicates the objectives to be achieved, and as a consequence member states must legislate in order to achieve those objectives.

The Council of Europe is a second European entity quite distinct from the EU. It is first of all essential to clarify that, beyond the lexical assonance, the Council of Europe and the Council of the EU are different organisations. In particular, the Council of the EU adopts EU laws and coordinates EU policies. Instead, the Council of Europe is an international organization which currently includes 46 European countries, namely: Albania; Andorra; Armenia; Austria; Azerbaijan; Belgium; Bosnia and Herzegovina;

---

[10] See J.A.E. Vervaele, *L'applicazione della Carta dei Diritti Fondamentali dell'Unione Europa (CDF) in materia di giustizia penale: valore aggiunto alla CEDU?*, in *Ius* no. 2/2015, pp. 131-164.

[11] See R.E. Kostoris, *Sources of Law* in R.E. Kostoris, (Ed.), *Handbook of European Criminal Procedure*, Springer, 2018, pp. 25-26.

Bulgaria; Croatia; Cyprus; Czech Republic; Denmark; Estonia; Finland; France; Georgia; Germany; Greece; Hungary; Iceland; Ireland; Italy; Latvia; Liechtenstein; Lithuania; Luxembourg; Malta; Republic of Moldova; Monaco; Montenegro; Netherlands; North Macedonia; Norway; Poland; Portugal; Romania; San Marino; Serbia; Slovakia; Slovenia; Spain; Sweden; Switzerland; Republic of Türkiye; Ukraine; and United Kingdom.

The Council of Europe promotes democracy, human rights and the rule of law. It aims to facilitate the creation and dissemination of common and democratic principles based on the European Convention on Human Rights and other acts on the protection of individuals, such as the European Social Charter; the European Convention on the Suppression of Terrorism[12]; the Budapest Convention on cybercrime. The jurisdictional body is the European Court of Human Rights, which judges on the violation or non-violation of the articles of the European Convention on Human Rights.

Having clarified the distinction between the EU and the Council of Europe, it should be emphasized that, in the two corresponding European scenarios, the reference sources regarding the cross-border collection of e-evidence are different.

IV. Sources of e-evidence collection: European Union

Despite the need of e-evidence collection abroad, for a long time there were no specific instruments of police and judicial cooperation in e-evidence matters. There were only principles to comply with and rules on data retention whose history is very troubled.

In fact, the matter of data retention was governed by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (the so-called Data Retention Directive). This directive amended Directive 2002/58/EC. However, on 8 April 2014 the Court of Justice[13] declared the Data Retention Directive to be invalid due to the violation of the principle of proportionality, and also due to its failure to provide adequate safeguards.

Consequently, Directive 2002/58/EC of 12 July 2002 returned to being the reference source on data retention. However, this directive, which concerns the processing of personal data and the protection of privacy in the electronic communications sector (the so-called Directive on privacy and electronic communications), currently is partially obsolete.

In the absence of specific rules for the collection of e-evidence, its gathering takes place in accordance with the same rules envisaged for the cross-border collection of other types of evidence. Specifically, the reference discipline is the Directive 2014/41/EU of 3 April 2014 regarding the EIO[14].

---

[12] See I.C. Paşca, *Is Terrorism an International Crime?* In *Journal of Eastern-European Criminal Law* no. 1/2020, p. 177.

[13] Court of Justice, 8 April 2014, Joined Cases C-293/12 and C-594/12.

[14] A discussion on the OEI can be found in M. Daniele, *Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles,* in *New Journal of European Criminal Law*, 2014, p. 179ss.; S. Ruggeri, (Ed.), *Transnational Evidence and Multicultural Inquiries in Europe. Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Springer, 2014; L. Scomparin, A. Cabiale, *The Proportionality Test in Directive 2014/41/EU: Present and Future of a Fundamental Principle*, in *Eurojus* no. 2/2022, pp. 72-86.

It was only on 17 April 2018 that the Commission submitted two proposals: A Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters[15]; and a Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings[16].

On the one hand, the Regulation establishes that the judicial authorities can directly request e-evidence from service providers of other States and that the service providers must transmit the evidence within 10 days, or within a shorter time limit in emergency cases. Furthermore, the regulation provides that the judicial authorities can issue a preservation order aimed at imposing that foreign service providers not delete the data, so that they can also request it later. On the other hand, the Directive provides that the service providers that offer their services in the EU must appoint a legal representative or designate an establishment which must be physically present in the EU. This designation will allow the judicial authorities to send the e-evidence orders precisely to the designated subjects.

The Council of the EU adopted such a regulation and a directive on 27 June 2023. They are the Regulation (EU) 2023/1543[17] and the Directive (EU) 2023/1544[18] respectively. However, they are still not actually applicable. This is because such a directive enters into force on the twentieth day following that of its publication in the Official Journal of the European Union, but it must be implemented by legislations of the member states. Moreover, the Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union but it shall apply from 18 August 2026[19].

V. Sources of e-evidence collection: Council of Europe

As far as the Council of Europe is concerned, the reference rules on the matter are firstly those of the European Convention on Human Rights (ECHR).

In the investigative field, Article 8 of the ECHR is of particular importance. This provision generically refers to investigations that cause interference with the Right to respect for private and family life, without distinguishing between collection of evidence and collection of e-evidence. Specifically, Article 8 ECHR provides that such interference is lawful if it satisfies three requirements. First, it must be 'in accordance with the law'.

---

[15] COM/2018/225 final – 2018/0108 (COD).

[16] COM/2018/226 final – 2018/0107 (COD).

[17] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings.

[18] Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.

[19] See Article 34 of the Regulation (EU) 2023/1543, which provides that: '1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. 2. It shall apply from 18 August 2026. However, the obligation for competent authorities and service providers to use the decentralised IT system established in Article 19 for written communication under this Regulation shall apply from one year after the adoption of the implementing acts referred to in Article 25. This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties'.

Secondly, the interference must be 'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'. Thirdly, in accordance with a requirement elaborated by the European Court of Human Rights (ECtHR), the interference must respect the principle of proportionality[20].

In addition to the ECHR, the Convention on Cybercrime (or Budapest Convention)[21] plays an important role in the field of digital investigations. This Convention of the Council of Europe is open to signature also by states which are not parties of said Council.

It is the first international treaty on crimes committed via the Internet and other computer networks, and also provides investigative tools, such as the search of computer networks and interception. Currently, the 68 States that are signed up to the Convention on Cybercrime are the following: Albania; Andorra; Argentina; Armenia; Australia; Austria; Azerbaijan; Belgium; Bosnia and Herzegovina; Brazil; Bulgaria; Cabo Verde; Canada; Chile; Colombia; Costa Rica; Croatia; Cyprus; Czech Republic; Denmark; Dominican Republic; Estonia; Finland; France; Georgia; Germany; Ghana; Greece; Hungary; Iceland; Israel; Italy; Japan; Latvia; Liechtenstein; Lithuania; Luxembourg; Malta; Mauritius; Monaco; Montenegro; Morocco; Netherlands; Nigeria; North Macedonia; Norway; Panama; Paraguay; Peru; Philippines; Poland; Portugal; Republic of Moldova; Romania; San Marino; Senegal; Serbia; Slovakia; Slovenia; Spain; Sri Lanka; Sweden; Switzerland; Tonga; Republic of Turkey; Ukraine; United Kingdom; and United States of America[22].

Finally, at the level of the Council of Europe, the need for enhanced cooperation and disclosure of electronic evidence between states was felt. For this reason, negotiations took place from September 2017 to May 2021, which led to the formal approval on 17 November 2021 of the Second Additional Protocol to the Budapest Convention on Cybercrime.

VI. Focussing on the second additional protocol to the Budapest Convention on Cybercrime of the Council of Europe

There is no doubt that server providers now play a fundamental role also in the legal field. Not only do they allow communications, the exchange of messaging, video calls etc., but they also process information that can become evidence in a criminal trial.

The fact that service providers have such information at their disposal implies the need for their collaboration for investigative purposes. Consequently, the importance of co-operation between States and the private sector emerges. Indeed, not infrequently the private sector becomes essential for investigative purposes.

---

[20] See T. Tridimas, *2438 The Principle of Proportionality*, in R. Schütze, T. Tridimas, T. (Eds), *Oxford Principles Of European Union Law: The European Union Legal Order: Volume I.* Oxford, 2018, pp. 243–264.

[21] Budapest, 23.XI.2001.

[22] The following states are not yet parties of the Convention on Cybercrime, but are signatories and invited to accede to it: Benin; Burkina Faso; Cameroon; Côte d'Ivoire; Ecuador; Fiji; Guatemala; Ireland; Kazakhstan; Kiribati; Korea; Mexico; New Zealand; Niger; Sierra Leone; South Africa; Timor-Leste; Trinidad and Tobago; Tunisia; Uruguay; and Vanuatu.

However, this co-operation is also characterized by problematic aspects, if only because the service providers operate according to business logic with secondary importance given to justice, which, of course, is instead the purpose of the investigations. Technology poses new opportunities, but also new challenges because it is always necessary to verify the compatibility of the collection of evidence with procedural safeguards[23].

It is important to underline that the co-operation of service providers is sometimes not only important, but fundamental. For this reason, there was the formal approval of the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. In accordance with Article 1, 'The purpose of this Protocol is to supplement: a) the Convention as between the Parties to this Protocol; and b) the First Protocol as between the Parties to this Protocol that are also Parties to the First Protocol'.

This additional protocol provides that a competent authority, for the purposes of specific criminal investigations or proceedings, can make 'a request to an entity providing domain name registration services in the territory of another Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name'24. Moreover, the authority can request the disclosure of subscriber information25, and traffic data26. For its part, an entity that receives a request from an authority must transmit the requested information. It is also provided that an expedited disclosure of stored computer data be made available if an emergency occurs[27].

These are very important provisions which, at least in part, recall the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. However, we must not forget that, on the one hand, only the Regulation is binding in its entirety and directly applicable in all member states and that, on the other hand, the two legal instruments (regulation and additional protocol) have different application areas. This is because the Regulation applies in member states, while the Second Additional Protocol applies in states which are parties to it and which, as stated above, can also be non-member states. Finally, in the member states which are parties to the Second Additional Protocol, both the provisions of the Regulation and those of this additional protocol must be observed, with the clarification that they are characterized by a different cogency.

VII. Conclusions

In general, when in an EU country it is necessary to proceed with the cross-border collection of e-evidence (in another member state or in a non-member state), various scenarios may occur, including the following ones:

Case 1. E-evidence is publicly available or else there is consent to the gathering of evidence. The hypothesis in which it is necessary to carry out the collection of e-evidence

[23] C. Cesari, Editorial: *O impacto das novas tecnologias sobre a justiça penal – um horizonte denso de incógnitas* in *Revista Brasileira De Direito Processual Penal*, no. 5(3)/2019, pp. 1167-1188.

[24] See Article 6 of the Second Additional Protocol to the Convention on Cybercrime.

[25] See Article 7 of the Second Additional Protocol to the Convention on Cybercrime.

[26] See Article 8 of the Second Additional Protocol to the Convention on Cybercrime.

[27] See Article 9 of the Second Additional Protocol to the Convention on Cybercrime. Such an additional protocol also provides specific rules about video conferencing.

in a state which is a party to the Convention of Budapest and where this e-evidence is publicly available or there is consent to gathering evidence is one of the easiest situations. Specifically, this hypothesis is governed by Article 32 of the Convention of cybercrime, which provides that 'A Party may, without the authorisation of another Party: a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system'.

Case 2: E-evidence to be requested from service providers. If the e-evidence is to be requested directly from service providers located in a state party to the Council of Europe, the Second Additional Protocol to the Budapest Convention on Cybercrime of the Council of Europe applies. In addition, if in the near future this request will be addressed to a service provider located in an EU member state, the Regulation (EU) 2023/1543 will also apply, i.e. the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, which will apply from 18 August 2026.

Case 3: Bilateral and/or multilateral agreements. If there are bilateral and/or multilateral agreements, the collection of e-evidence is carried out in accordance with the rules set out in these agreements.

Case 4: Collection of e-evidence in light of the European Investigation Order in criminal matters (EIO). This situation occurs if an EU member state should collect evidence in another EU member state that transposed the Directive 2014/41/EU regarding the EIO[28] into national law[29].

Case 5. Collection of e-evidence when EIO does not apply. If an EU member state has to collect evidence in a state where the EIO does not apply and in the absence of bilateral and/or multilateral agreements, the collection of evidence can only take place following a letter rogatory, which is based on the principle of mutual assistance.

Finally, it should be emphasized that hybrid situations can also occur. For example, it could happen that the collection of a certain type of evidence is governed by bilateral agreements, but both member states involved transposed the EIO into national law. In these cases, it is necessary from time to time to verify which instrument for transnational collection of evidence is to be used on the basis of the criteria established by international and EU law.

References

1. Bachmaier Winter, L. (2009). Criminal Investigation and right of privacy: the case-law of the European Court of Human Rights and its limits. *Lex ET Scientia*, Juridical Series (II),.

2. Bogensberger, W. (2019). Chapter 4 Judicial Cooperation in Criminal Matters. In Kellerbauer, M., Klamert, M., Tomkin, J. (Eds). *The EU Treaties and the Charter of Fundamental Rights: A Commentary*. Oxford Academic.

[28] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014. This Directive was transposed into nation law of all EU member states, with the exception of Ireland and Denmark.

[29] For a discussion on Directive 2014/41/EU, see M. Daniele, *Evidence Gathering*, in R.E. Kostoris, (Ed.), *Handbook of European Criminal Procedure,* Springer, 2018, pp. 364-369.

3. Cesari, C. (2019). Editorial: O impacto das novas tecnologias sobre a justiça penal – um horizonte denso de incógnitas. *Revista Brasileira De Direito Processual Penal* 5(3).

4. Daniele, M. (2014). Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles. *New Journal of European Criminal Law*.

5. Daniele, M. (2018). Evidence Gathering. In Kostoris, R.E. (Ed.), *Handbook of European Criminal Procedure*. Springer.

6. European Commission (2011). *Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC).*

7. Floridi, L. (2015). The Onlife Manifesto. In Florifi, L. (Ed.), *The Onlife Manifesto: Being Human in a Hyperconnected Era*. Cham.

8. Kostoris, R.E. (2018). Sources of Law. In Kostoris, R.E. (Ed.), *Handbook of European Criminal Procedure.* Springer.

9. Matsumi, H., Hallinan, D., Dimitrova, D., Kosta, E.,de Hert, P. (Eds) (2023). *Data protection and privacy: In transitional times.* Bloomsbury Publishing.

10. Paşca, I.C. (2020). Is Terrorism an International Crime? *Journal of Eastern-European Criminal Law* (1).

11. Quattrocolo, S. (2023), *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*. Springer.

12. Rijken, C. – Vermeulen G. (2006) (Eds). *Joint Investigation Teams in the European Union. From Theory to Practice.Springer.*

13. Ruggeri S. (2014) (Ed.). *Transnational Evidence and Multicultural Inquiries in Europe. Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*. Springer.

14. Scomparin, L., Cabiale, A. (2022). The Proportionality Test in Directive 2014/41/EU: Present and Future of a Fundamental Principle. *Eurojus* (2).

15. Signorato, S. (2018), Data retention, a balance between judicial requirements and the risk of illegality. In Provincial Protector of Citizens-Ombudsman, Institute of Criminological and Sociological Research (Eds), *Human Rights Protection "From Unlawfulness to legality"* (1).

16. Signorato, S. (2020). Streamlining the Fight Against Child Sex Offenders Trough EU Regulation of IP address. *Journal of Eastern-European Criminal Law* (1), 77-86.

17. Signorato, S. (2021). Combating terrorism on the internet to protect the right to life. The regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. In Provincial Protector of Citizens, Ombudsman (Eds), *Yearbook. Human rights protection. The right to life*. Vojvodina Provincial authorities Common Affairs Department Novi Sad, Republic of Serbia.

18. Stanila, L. (2020). Living in the Future: New Actors in the Field of Criminal Law – Artificial Intelligence. *Legal Science: Functions, Significance and Future in Legal Systems II. The 7th International Scientific Conference of the Faculty of Law of the University of Latvia 16–18 October 2019, Riga Collection of Research Papers*.

19. Tridimas, T. (2018). 2438 The Principle of Proportionality. In Schütze, R. – Tridimas, T. (Eds), *Oxford Principles Of European Union Law: The European Union Legal Order: Volume I.* Oxford.

20. Vervaele, J.A.E. (2015). L'applicazione della Carta dei Diritti Fondamentali dell'Unione Europa (CDF) in materia di giustizia penale: valore aggiunto alla CEDU? *Ius* (2).