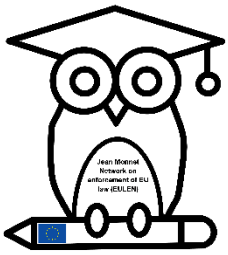

Co-funded by the
Erasmus+ Programme
of the European Union

Jean Monnet Network on EU Law Enforcement

# The gathering of e-evidence by the EPPO and the relevant admissibility issues

Sapfo Katsanaki[1]

Crimes affecting the financial interests of the Union, falling under the competence of the European Public Prosecutor's Office, are more and more often these days committed or facilitated using communication systems. These crimes leave traces in the form of electronic evidence, whose importance is paramount for their successful prosecution. However, the handling of e - evidence presents challenges because of its intangible, volatile and ephemeral nature. The EPPO's investigations involving e-evidence and especially the cross-border ones will encounter issues regarding the gathering and handling of e-evidence, which are only partially addressed by the provisions of the Regulation. It may be proven even harder to ensure the admissibility of such evidence, gathered either by the EPPO or by its close partner OLAF, especially when it has been gathered though special investigative and highly intrusive measures, as there is no harmonisation of evidential rules within the EU. Proposals for amendments of the relevant legislative framework and policy recommendations are put forward to address these issues.

Keywords:

EPPO, e-evidence, cross-border investigations, OLAF, special investigative measures, Budapest Convention on Cybercrime, admissibility, assessment of evidence

[1] Deputy Prosecutor at the Public Prosecutor's Office to the Athens Court of First Instance. Master of Laws (LLM) in Computer and Communications Law from Queen Mary, University of London and LLM in "Penal Law and Penal Procedure Law" from the Faculty of Law of the National and Kapodistrian University of Athens.

## I. Introduction

Nowadays, an increasing number of crimes affecting the financial interests of the Union are committed or facilitated using communication systems. These crimes leave traces in the form of electronic evidence, whose importance is paramount for their successful investigation and prosecution. Electronic evidence (hereafter e-evidence) is used in this article in its broad definition and encompasses "any data resulting from the output of an analogue device and/or a digital device of potential probative value that are generated by, processed by, stored on, or transmitted by any electronic device"[2]. Thus, the term e-evidence includes all kind of evidence regardless of its origin, namely both evidence originally born electronically as wells evidence of any form, either physical or analogue, that is then digitised and acquires a digital status[3].In that sense electronic evidence includes, but it is not limited to, digital evidence [4].

Inevitably, the European Public Prosecutor's Office (hereafter EPPO)[5] will conduct investigations involving e-evidence and most often this evidence will be collected through cross-border operations, even if the criminal activity has taken place within the jurisdiction of one Member State, because e-evidence, due to its particular nature and the development of modern technologies, may be stored or located anywhere in the world[6]. Thus, the EPPO, being established by way of enhanced cooperation[7], will be faced with different regulatory frameworks governing the collection of e-evidence, since investigation measures may have to be taken in the territory of a participating Member State, in that of a non-participating Member State or even in the territory of a third state.

The issues arising when e-evidence is collected by EPPO and its close partner OAF as well as the problems of admissibility and assessment of the e- evidence gathered are presented in the following chapters, while the policy recommendations put forward by institutional bodies and the proposed amendments of the relevant legislative framework are presented in the last chapter.

## II. EPPO's investigations involving e- evidence

### a) Special investigative measures under the EPPO Regulation

Although, nowadays, all investigative measures in criminal proceedings may generate e - evidence, the rising use of technology for investigative purposes has led to the emergence of new investigative techniques for the gathering of evidence, which the EPPO should also use for tis operations to be successful. Hence, the minimum list of investigative measures that must be made available by member states to European Delegated Prosecutors (hereafter EDPs) handling cases within their competence[8], includes the following special

---

[2]Definition used in the EVIDENCE Project—Deliverable 2.1—EVIDENCE Semantic Structure, 24 <http://www.evidenceproject.eu/the-activities/deliverables.html> accessed 17 May 2022. Under the same Project, digital evidence is defined as that electronic evidence which is generated or converted to a numerical format

[3] Ibid 24,25.

[4] Maria Angela Biasiotti, 'A proposed electronic evidence exchange across the European Union' (2017)14 Digital Evidence and Electronic Signature Law Review 1, 4.

[5] Established by the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') [2017] OJL283/1.

[6] E – evidence may have a cross-border nature either because of the location of the information provider recording the information, or because of the actual location where the digital information is stored or because the crime itself may have a cross-border nature, Jeanne Pia Mifsud Bonnici, Melania Tudorica, and Joseph A. Cannataci 'Chapter 11 The European Legal Framework on Electronic Evidence: Complex and in Need of Reform' in Jeanne Pia Mifsud Bonnici Melania Tudorica Joseph A. Cannataci and Fabrizio Turchi (eds) *Handling and exchanging electronic evidence across Europe* (Springer 2018) 219.

[7] Art 86(1) subpara 3 of the consolidated version of the Treaty on the Functioning of the European Union (2012) OJ C326/1. The EPPO Regulation was adopted with the consenting votes of 20 Member States and, following its adoption, two more states, Malta and the Netherlands also joined the enhanced cooperation in August 2018 in accordance with the procedure set out in art. 331 TFEU. For the consequences of the EPPO being established by enhanced cooperation see Hans-Holger Herrnfeld, Judith Herrnfeld 'The European Public Prosecutor's Office – where do we stand?' (2021) ERA forum 657.

[8] Article 30 para (1) of the EPPO Regulation.

investigative measures[9]: a) the production of stored computer data, encrypted or decrypted, either in their original form or in some other specified form, including banking account data and traffic data[10], b) the interception of electronic communications to and from the suspect or accused person, over any electronic communication means that the suspect or accused person is using[11] and c) the tracking and tracing of an object by technical means, including controlled deliveries of goods[12].

These investigative measures should be made available on the precondition that the offence subject to the investigation is punishable by a maximum penalty of at least 4 years of imprisonment and may be subject to restrictions provided by national law, regarding certain categories of persons or professionals, legally bound by an obligation of confidentiality[13]. However, because of their intrusive nature, they may also be subject to further conditions and limitations provided by national law[14] so long that they also apply for national cases and are not provided only for the EPPO investigations[15], whereas the interception of communication and the tracking and tracing of objects may as well be limited by Member-States to specific serious offences. Indeed, under the national legislations of Member States, access to such intrusive investigative techniques is limited to certain offences, however the 'seriousness' thresholds of the offences are not the same[16]. In any case, the Member States, intending to make use of such limitation must notify the EPPO, with the relevant list of serious offences[17].

b) The cross-border investigations involving e-evidence

As is usually the case with investigations involving e-evidence, its location could be outside the territory of the state where the EDP is conducting investigations. Indeed, the evidence needed could be located either in the territory of another Member State participating to the EPPO, or in the territory of a Member State not participating in the EPPO, or even in the territory of a third state.

i) The provisions of the Regulation

In case evidence is located in the territory of another Member State participating to the EPPO, the investigation will be conducted according to Article 31 of the EPPO Regulation. Thus, the EDP handling the case, may assign any investigative measure involving e – evidence[18], to the 'assisting' EDP located in the

[9] Article 30 para (1) (c), (e) and (f) of the EPPO Regulation

[10] With the exception of data specifically retained in accordance with national law pursuant to the second sentence of Article 15(1) of Directive 2002/58/EC of the European Parliament This exception, referring to traffic data retained by Member States under a national data retention regime, has been included since Directive 2006/240EC providing for the establishment of data retention regimes has been annulled by the ECJ in its ruling of the Digital Rights Ireland Case (C-293/12 και C-594/12 [2014] ECR -I, 238). Hence, Member States participating to the EPPO are not obliged, under the Regulation, to entitle EDPs to request the production of data retained under national mandatory retention regimes, but if national prosecutors have such power under national law, the EDPs should be granted it as well, according to para (4) of Article 30 (provided that these data retention regimes are not contrary to Union law).

[11] The interception refers to content data and traffic data being transmitted (live data), as opposed to stored traffic data to which art.30 para.1 (c) applies, Dominik Brodowski, in Herrnfeld/Brodowski/Burchard eds, European Public Prosecutor's Office: Article-by-Article Commentary, (Bloomsbury Publishing 2020) 276.

[12] This could include the tracking and tracing of mobile phones by an IMSI catcher or by identifying the radio cell where it is connected, or the tracking or tracing of cars by GPS, ibid 276.

[13] Article 30 para2 EPPO Regulation. Categories of persons legally bound by obligations of confidentiality are usually attorneys, public servants, members of Parliament and members of medical professions, ibid, 277.

[14] Article 30 para (3), EPPO Regulation.

[15] These conditions may refer to the exclusion of certain content, as highly personal data or to the exclusion of certain persons such as close relatives, Dominik Brodowski (n 11), 277.

[16] See examples of the differentiated thresholds for the use of special investigative measures in the Study about 'Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation', commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (2018) 24 www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)604977 accessed 17 May 2022.

[17] The relevant notifications to the EPPO can be found in the EPPO website in the following URL www.eppo.europa.eu/en/documents?search_api_fulltext=&f%5B0%5D=facet_media_document_category%3A16 accessed 17 May 2022.

[18] Not only the investigative measures enumerated under Article 30, but also any other measure available under the national law, as provided by para 4 of article 31 of the EPPO Regulation.

Member State where the investigation needs to be carried out[19]. The justification and adoption of such measures shall be governed by the law of the Member States of the handling EDP[20], while the assisting EDP must simply undertake the measure or instruct the national authorities to do so, without having any competence to invoke any grounds of no recognition[21]. However, the investigative measures involving e - evidence and especially those of an intrusive nature, as interception and tracking and tracing of objects, are most likely to require a judicial authorisation[22] under national legislation. In that case, if the authorisation is required under the national law of the handling EDP, the authorization shall be obtained by the latter and submitted together with the assignment, whereas if authorization is required under the law of the assisting EDP, the latter shall obtain it in accordance with the national laws of his/her member state and if the authorization is denied the handling EDP will withdraw the assignment. If authorization is required by both member states, only one should be obtained, in line with the concept of the 'single judicial authorization', stemming from Recital 72, and it should also be obtained by the assisting EDP in whose Member State the investigation measure will be taken[23].The judge or Court in either case, will decide whether to authorise the assigned measures according to national law, as if the authorisation was required for a purely domestic case[24] and will not be called to merely recognise a foreign order for an investigation measure as is the case with the execution of a European Investigation Order[25]. Hence, it has been rightly criticised that the mechanism of the European Investigation Order is more favourable to the execution of an investigation measure than that provided under the EPPO Regulation at least when authorisation is required under the laws of the assisting EDP[26], whereas the opposite is true when such authorisation is only required by the national law of the handling EDP, as only the national law of the latter shall apply[27].

[19] The Regulation uses the terms 'handling' and 'assisting' with regard to EDPS when conducting cross - border investigations (see recital 72 and article 2 (5) and (6)), instead of the terms 'issuing' and 'executing' to emphasize that EPPO operates as a single European Office, according to Article 8 para 1 and does not rely on the principle of mutual recognition, Towards a European Public Prosecutor's Office Study for the LIBE Committee (2016) 31 www.europarl.europa.eu/RegData/etudes/STUD/2016/571399/IPOL_STU(2016)571399_EN.pdf accessed 17 May 2022. The use of the concept of mutual recognition in case of cross border investigations within the territory of the EPPO, was also rejected by most Member states as inconsistent with the concept of a single office, Hans – Hogel Herrnfeld in Herrnfeld/Brodowski/Burchard eds, European Public Prosecutor's Office: Article-by-Article Commentary, (Bloomsbury Publishing 2020) 286.

[20] Article 30 para 2 second sentence. According to Article 30 para (5), the grounds to be taken into account when ordering an investigative measure is the possibility of it providing information or evidence useful to the investigation, and the inexistence of a less intrusive measure available which could achieve the same objective.

[21] Whereas the execution of a European Investigation Order can be denied for several grounds listed under Art. 11 of the Directive 2014/41/EU regarding the European Investigation Order in criminal matters, Hans – Hogel Herrrnfeld (n 19) 287.

[22] The term refers to authorisation by a judge or a Court and encompasses both the decision of a judge or court approving the prosecutor's decision to order an investigation measure, as well as the decision of a court of judge to order a certain investigation measure, following a prosecutor's application, ibid 292, Dionisios Mouzakis, 'Cross – border investigations of the EPPO: progress or a step backwards in judicial cooperation in criminal matters' (2022) 1 Poinika Chronika 11, 13.

[23] Hans- Holger Herrnfeld (n 19) 287. However, according to the Guidelines of the College of the EPPO on the application of Article 31of the Regulation, in that case, no Court, neither that of the handling EDP nor that of the assisting EDP will have the opportunity to assess the substantive reasons of the measure, which is contrary to the EU Charter of fundamental rights and hence it can be concluded that an authorisation will have to be taken from the Member State of the handling EDP, see para 18, 20, 21 of the Decision of the College of the European Public Prosecutor's Office of 26.01.2022.

[24] The assignment of the investigation measure is subject to a double legal examination as the Judge/Court of the Member State where the investigation measure is assigned, is called to examine once again the preconditions of its assignment according to national law, Dionisios Mouzakis (n 22) 14.

[25] Hans- Holger Herrnfeld (n 19) 293.

[26] Lorena Bachmaier Winter, Cross- border Investigations under the EPPO proceedings and the quest for balance, in Lorena Bachmaier Winter (eds), *The European Public Prosecutor's Office, The Challenges ahead* Springer Volume 1 (Springer 2018) 129, Silvia Allegrezza and Anna Mosna, 'Cross-Border Criminal Evidence and the Future European Public Prosecutor. One Step Back on Mutual Recognition?' in Lorena Bachmaier Winter (ed), *The European Public Prosecutor's Office- The challenges ahead,* vol 1 (Springer 2018) 156.

[27] Dionisios Mouzakis (n 22) 16.

As the special investigative measures involving e- evidence and in particular productions orders or interceptions of communications, exist in all Member States to the EPPO[28], the consultation procedure and notification to be followed in case of a non – existence of the assigned measure[29], should never appear. However, a situation where the investigation measure would not be available in a similar domestic case under the laws of the assisting EDP's Member State, cannot be excluded since the threshold requirements for the authorisation of such investigation vary greatly in the legislation of the member states[30]. In this latter case, it could be substituted by another measure achieving the same results[31]. However, although one could hardly imagine which investigative measure would achieve the same results as interception of communications or access to computer data, in any case the time elapsed for the consultations between the EDPs and the Permanent Chamber's Decision, could be fatal for the preservation of the evidence in electronic form[32]. Furthermore, it is difficult to understand how the inexistence of the measure assigned, would be resolved by having recourse to legal instruments on mutual recognition, as provided by para (6) of the Regulation. Although its intention is to make clear that these instruments, such as the European Investigation Order, are supplement to the EPPO's assignment mechanism, it is hard to contemplate a case where an investigative measure involving e- evidence is not available on domestic cases but would be available through an EIO[33].

For the collection of evidence located in the territory of Member States non-participating to the EPPO, in the absence of a separate legal instrument on criminal cooperation between these states and the EPPO, those participating to the EPPO shall notify the EPPO as competent authority for the instruments adopted on criminal cooperation under Union law[34]. The most relevant to e-evidence instrument is undoubtedly the European Investigation Order and, if adopted, the Regulation on European Production and Preservation Orders for electronic evidence in Criminal matters[35]. However, under both instruments the issuing authority is a competent, under the members states national law, authority[36] and thus it is doubted whether the EPPO would constitute such an authority[37]. Moreover, although the non-participating Member States are not legally bound to accept such notification, they are expected to do so on the basis of sincere cooperation, a duty provided under Art.4 (3) TEU[38].

Regarding the cooperation with third countries, the EPPO is bound by international agreements concerning cooperation in criminal matters concluded by the Union[39]. Furthermore, the EPPO may be notified

[28] Member states to the Budapest Convention on Cybercrime are called, under Article 18, 20 and 21 to adopt production orders and necessary measures to empower the real – time collection of traffic data and the interception of communications. Since all member states to the EPPO have signed and ratified the Budapest Convention, those investigative measures should already exist under their national legislations.

[29] Article 30 para (4) (5) (6)

[30] Lorena Bachmaier Winter, Mutual Recognition and Cross-Border Interception of Communications: The Way Ahead for the European Investigation Order, in Chloé Brière and Anne Weyembergh (eds) *The Needed Balances in EU Criminal Law Past, Present and Future (*Hart Publishing 2018) 313,317.

[31] Article 31 (8) EPPO Regulation. A similar provision is provided in Article 10 para 5 of the Directive 2014/41/EU regarding the European Investigation Order in criminal matters.

[32] Lorena Bachmaier Winter (n 26)126.

[33] Ibid, 127.

[34] Article 105 para (3) The adoption of a separate legal instrument is favoured by the Regulation and the non- participating Member States as it provides legal certainty, Nicolas Franssen 'The Future judicial cooperation between the EPPO and non – participating member states' (2018) 9(3) New Journal of European Criminal Law 291, 294.

[35] Commission, 'Proposal for a Regulation of the European Parliament and the Council European Production and Preservation Orders for electronic evidence in Criminal matters' COM (2018) 225 final.

[36] Article 2 (c) and 33 para 1 (a) of the of the Directive 2014/41/EU regarding the European Investigation Order in criminal matters and art 4 para 1 and 2 and 22 para 1 of the Proposal for a Regulation of the European Parliament and the Council European Production and Preservation Orders for electronic evidence in Criminal matters.

[37] Nicolas Franssen (n 34) 296.

[38] Dominik Brodowski (n 11) 639.

[39] Article 104 para 3. Such international agreements concerning crime areas for which the EPPO is competent or may be competent for inextricably linked offences are ie the United Nations Convention against Transnational Organised Crime, the United Nations Convention against Corruption, the Council of Europe Convention on the Prevention of Terrorism and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation on the Proceeds from Crime. It has been argued, that although the Union is theoretically allowed to designate the EPPO as a central Authority competent to issue and execute requests for legal assistance (at least under the UNTOC and Warsaw Convention), this could impede

by Member States as a competent authority to issue requests for legal assistance in the context of multilateral or bilateral agreements on legal assistance in criminal matters concluded by them with third countries, subject to the latter's acceptance[40]. So far 16 Member States have declared EPPO as a competent authority for the purposes of the European Convention on Mutual Assistance in criminal matters[41]. No such declarations have been made under the Budapest Convention on Cybercrime, which has specific provisions on mutual legal assistance for the collection of evidence in electronic form[42]. This is probably because the Budapest Convention does not create a separate regime for mutual assistance but rather provides as a general principle that assistance should be carried out through the application of the existing relevant treaties and international agreements between the parties[43]. Consequently, the parties to the European Convention on Mutual Assistance in Criminal Matters will continue to provide assistance to each other pursuant to its provisions and those that have concluded bilateral agreements on mutual assistance, will continue to apply their terms[44]. Hence the EPPO shall rely on these agreements and arrangements for the preservation and gathering of e- evidence through the mechanisms provided under the Budapest Convention[45]. The framework of the EPPO investigations involving e-evidence, will be further strengthened if the Member States to the Budapest Convention ratify the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence**,** opened for signature on the 12th of May 2022**,** which provides common rules for enhanced co-operation and the disclosure of electronic evidence[46].

Finally, in case the EPPO is not notified as competent authority, then the handling EDPs may have recourse to the powers of a national prosecutor and can rely on the international agreements concluded by their Member States to require legal assistance from third countries, as if they were handling a purely domestic case, provided they inform the requested state and they obtain its consent that the evidence collected will be used by the EPPO[47].

ii) Alternative mechanisms for gathering e-evidence

Although the Regulation, as explained above, provides for a wide range of mechanisms to request evidence in cross-border investigations, it should be borne in mind that e – evidence, particularly traffic and

effective cooperation due to the EPPO's institutional design and its limited competence to execute requests for legal assistance, Dominik Brodowski (n 11) 627.

[40] Art 104 para 4. However, this provision raises also legal issues, as the EPPO is not an authority of the Contracting party but a supranational body, ibid, 629.

[41] Austria, Belgium, Bulgaria, Czech Republic, Finland, France, Germany, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Romania, Slovak Republic, and Slovenia. See these declarations at www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=030&codeNature=0 accessed 17 May 2022.

[42] Chapter III of the Budapest Convention on Cybercrime contains specific provisions for mutual assistance regarding provisional measures, such as the expedited preservation of stored computer data and the expedited disclosure of preserved traffic data (Art. 29 and 30) and provisions for investigative powers such as access to stored computer data, the real time- collection of traffic data and interception of content data (Art 31,33 and 34). It also provides for the establishment of a 24/7 Network, under Art. 35, which obliges each party to designate a point of contact available 24 hours per day, 7 days per week to ensure immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

[43] See art 23 of the Budapest Convention and the Explanation Report to the Convention on Cybercrime under art 27 p 46 https://rm.coe.int/16800cce5b accessed 17 May 2022.

[44] Explanatory Report to the Convention on Cybercrime Art 27 p47.

[45] Provided that the parties to the Budapest Convention have already established a legal basis to enable the carrying out of the forms of co-operation in computer related criminal matters under Articles 29-35, Explanatory report to the Convention on Cybercrime under Art 25 p44.

[46] The Protocol contains specific provisions for the disclosure of domain name registration information (Art.6) and for direct co-operation with service providers regarding subscriber information (Art.7) and it also establishes procedures enhancing international cooperation for the expedited production of subscriber information and traffic data and for the disclosure of stored computer data (Section 3) https://rm.coe.int/1680a49dab accessed 17 May 2022.

[47] Consent should be given to ensure the admissibility of the evidence and the EPPO's ability to make full use of it through its proceedings, even if the case is reallocated according to the provisions of the EPPO Regulation (Art 26 (5), 36 (3)), Dominik Brodowski, (n 11) 631.

subscriber data[48], is very often requested directly from service providers who cooperate voluntarily with the Law Enforcement Authorities (hereafter LEAs)[49]. The gathering and access to e - evidence on the grounds of voluntary cooperation between the Law Enforcement Agencies and the service providers has become a common investigative practice in Europe, thus instigating the Commission's legislative proposal for the European Production and Preservation Orders[50] and the Directive on imposing obligation on service providers to appoint legal representatives acting as points of contact or Production and Preservation Orders addressed by LEAs[51]. The Regulation has not been adopted yet, since the Commission's proposal has raised controversial reactions and received severe criticism by stakeholders, European associations, and European bodies, questioning the Proposal's necessity and added value[52].

Consequently, until a binding legal instrument is adopted, EDPs may collect e-evidence located in any Member State, either participating to the EPPO or not, or even evidence located in a third state, such as the US where the major Service providers are located[53], through these schemes of «voluntary cooperation» with the service providers[54]. This direct cooperation with the private sector remains undoubtedly the fastest and easiest mechanism for transborder access to e-evidence than any other mechanism of mutual legal assistance[55].

---

[48] Definitions of traffic data are given under art 2 (b) of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and under art 1 (d) of the Budapest Convention on Cybercrime and relates to any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service. A definition of subscriber data is given under art 18 para 3 of the Budapest Convention and refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data. It is argued that this data is less sensitive and thus easier to hand over, Paul de Hert, Cihan Parlar Johannes Thumfart, 'Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland' (2018) 9 (3) New Journal of European Criminal Law 326, 329.

[49] Indeed, the majority of the requests for access to data within the European Union and beyond refer to non -content than content data. See the relevant data at the 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT' accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters' and 'Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD(2018) 118 final, p.14

[50] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters', COM (2018) 225 final. For a more thorough analysis of the Commission's proposal see, Marco Stefan and Gloria González Fuster, 'Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters State of the art and latest developments in the EU and the US' November 2018 (updated in May 2019) ,*27* Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters – CEPS accessed 17 May 2022, also, Ángel Tinoco-Pastrana, 'The Proposal on Electronic Evidence in the European Union;, eucrim, issue 1/2020 46-50.

[51]Commission, 'Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' COM (2018) 118 final.

[52] Sergio Carrera and Marco Stefan, 'Access to Electronic Data for Criminal Investigations Purposes in the EU' (February 2020) 31 https://www.ceps.eu/download/publication/?id=26544&pdf=LSE20120-01_JUD-IT_Electronic-Data-for-Criminal-Investigations-Purposes.pdf> accessed 17 May 2022.

[53] Like Microsoft and Google. See the statistics of these companies for the increasing demands of LEAS to gain access to data in Gertjan Boulet and Nicholas Hernanz, 'Cross-border law enforcement access to data on the Internet and rule of law challenges in the EU' 2013, SAPIENT Deliverable 6.6, issue SAPIENT Policy Brief 6.6, 4, https://www.academia.edu/4959180/Cross_border_law_enforcement_access_to_data_on_the_Internet_and_rule_of_law_challenges_in_the_EU> accessed 17 May 2022. It is indicative that in 2015, European countries sent more than 130,000 requests—mostly for subscriber information—directly to major US service providers and the latter responded positively in about 60% of the cases on average, Alexander Seger, 'e-evidence and access to data in the cloud, results of the cloud evidence group of the cybercrime Convention Committee' in Maria Angela Biasiotti, Jeanne Pia Mifsud Bonnici, Joe Cannataci, Fabrizio Turchi (eds), *Handling and Exchanging Electronic Evidence Across Europe* Volume 38 (Springer 2018) 35, 37.

[54] As this mechanism of cooperation is called in Gertjan Boulet and Nicholas Hernanz, ibid 7.

[55] However, this option is not without problems, especially since no regulatory framework exists for theses mechanisms of cooperation. For the challenges posed to privacy and data protection see Gertjan Boulet and Nicholas Hernanz, ibid 13.

Finally, it should be highlighted that e-evidence located outside the jurisdiction where the investigation is taking place, may also be collected without consent and without recourse to any mechanism of mutual legal assistance. Indeed, since the remote search of computers is technologically feasible, data located extraterritorially may be accessed unilaterally by LEAS[56]. However, these extraterritorial searches and collection of evidence without consent, with which the EPPO will undoubtedly be faced when investigations involve cross -border e -evidence, may raise issues of jurisdiction and particularly of jurisdiction to enforce[57]. The views on these issues differ from jurisdiction to jurisdiction[58], and several approaches have been identified, such as that no jurisdiction or sovereignty of states is violated[59] or that a violation is taking place only if these searches resulted in material damage to the cyber infrastructure of the relevant state[60]. But even if state sovereignty may be encroached, there is no legal sanctioning system for the offence suffered by states or individuals[61]. It is also argued that especially in a case of an ongoing investigation, where the LEAS are following trails on real time, the investigation should continue with no territorial concerns, even if the suspect or the information sought has moved or shifted to a server outside their territorial jurisdiction[62]. A similar approach has been followed by the Directive on the European Investigation Order with regard to the interception of telecommunications that has to be carried out in the territory of another member state, where the subject of the interception has moved. Under Article 31, the interception will continue and, if no technical assistance is required, the intercepting state shall merely notify the relevant member state of the interception taking place[63].

Until today, the exception to territorial jurisdiction and only legal basis for the unilateral transborder access to data stored in another jurisdiction is provided by Article 32 of the Budapest Convention on Cybercrime, which allows access to extraterritorially located data without the authorisation of another Party if it is publicly available (open source) or if the data is located in another Party and the accessing 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. But transborder access is limited to open-source data, whereas more often the data sought for criminal investigation purposes will not be publicly available and legal issues also arise regarding the meaning of consent[64] and the determination of the person having lawful authority to disclose the data[65]. Moreover, no harmonisation of the regulatory framework regarding unilateral transborder access to data has been achieved, since in some members states, LEAS can access data located abroad, from devices in

[56] Unilateral or transborder access refers to access to data stored in another jurisdiction, without previous requesting specifically mutual assistance, and is usually conducted from domestically located devices, Anna-Maria Osula 'Transborder access and territorial sovereignty' (2015) 31 Computer Law and Security Review 720.

[57] Jurisdiction το enforce should be exercised within a state's territory, whereas jurisdiction to prescribe, meaning the state's ability to legislate, may encompass subjects or offences taking place abroad, Paul de Hert, Cihan Parlar Johannes Thumfart (n 48) 330. Jurisdiction is closely tied to sovereignty, whereas territorial sovereignty refers to a state's authority to exercise supreme authority over all persons, Anna-Maria Osula, ibid 721.

[58] According to a UN study, around two-thirds of countries in all regions of the world perceived foreign law enforcement's access to other States' computer systems or data as impermissible, even if it may occur in practice either with or without the knowledge of investigators, Anna-Maria Osula, ibid 725.

[59] According to this view no consent is required for remote searches since these acts are virtual and not material but, even if some states see a state -sovereignty endangerment, the judicial authorities do not always realise that these searches are conducted extraterritorially Paul de Hert, Cihan Parlar Johannes Thumfart (n 48) 333,334.

[60] Anna-Maria Osula (n 56) 726.

[61] Paul de Hert, Cihan Parlar Johannes Thumfart (n 48) 334.

[62] Jeanne Pia Mifsud Bonnici, Melania Tudorica, and Joseph A. Cannataci (n 6) 204.

[63] Lorena Bachmaier Winter argues that the notifications made should not aim to the obtaining of authorisation but to the establishment of good relationships between Member States and to the enhancement of the exchange of information, otherwise they would simply be skipped by the intercepting authorities, Lorena Bachmaier Winter (n 30), 333.

[64] Indeed, the legal meaning of consent is not the same in various jurisdictions, Council of Europe, 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY' (Cybercrime Convention Committee (T-CY)) Adopted by the 12th Plenary of the T-CY (2–3 December 2014) 19, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e accessed 17 May 2022.

[65] Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under art 32, Council of Europe, 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY', ibid, 20.

their jurisdictions, while in others, this would be possible only if the preconditions foreseen under Article 32 of the Budapest Convention are met[66].

Finally, the rapid development of technology and the emergence of new infrastructures for storing data, such as the cloud[67], has given rise to situations know as 'loss of location', where the location of the data sought cannot be identified[68]. In these situations, it has been argued that the unilateral collection of data breaches no territorial jurisdiction since the state to which a mutual legal assistance request could be addressed, is unknown[69]. No solution is given by art32 of the Budapest Convention on Cybercrime, since it presupposes that the location of the data is known. However, the drafters of the Convention advise the Parties in situations of loss of location to 'evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations'[70]. Finally, some states have even enacted legislation to address the issue of loss of location[71], but no common legal framework exists.

The EPPO acting as a single office[72] will not have issues of territorial jurisdiction when unilateral remote searches and ongoing investigations are carried out in the territory of the participating Member States. In these cases, there will most likely take place only a simple communication between the EDPs about the investigation actions being caried out. However, the situation is different if these investigative measures are conducted in the territory of the non- participating Member States or even of third states, where especially if third states are involved, issues of international comity may arise[73].

c) E-evidence gathered by OLAF

OLAF is the European Union's body responsible for conducting administrative investigations concerning any illegal activity affecting the EU's financial interests [74]. EPPO's relationship with OLAF has been an issue of discussion, since they both operate in the same field, even if on different levels, and there was a risk of duplication of investigations[75]. There were even thoughts that OLAF might not be needed anymore, since tis competence in protecting the financial interest of the Union overlapped with those of the EPPO[76].

---

[66] Cybercrime Convention Committee (T-CY) 'Transborder Access and Jurisdiction: What Are the Options?', 2012 29 https://rm.coe.int/16802e79e8 accessed 17 May 2022.

[67] For an analysis of cloud computing services, see Marcin Rojszczak, Cloud act agreement form an EU perspective (2020)38 Computer Law & Security Review, 3 https://www.sciencedirect.com/science/article/pii/S0267364920300479 accessed 17 May 2022.

[68] Anna - Maria Osula, *Remote search and seizure of extraterritorial data* (University of Tartu Press 2017), 7 especially footnote 6.

[69] Anna - Maria Osula ibid, p.30, 43.

[70] Council of Europe, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32)'Cybercrime Convention Committee (T-CY)) Adopted by the 12th Plenary of the T-CY (2–3 December 2014', 6 https://www.ccdcoe.org/uploads/2019/09/CoE-141203-Guidance-Note-on-Transbprder-access-to-data.pdf accessed 17 May 2022.

[71] For example, Belgium and the Netherlands, see Anna - Maria Osula (n 68) 44.

[72] The notion of a 'single office' used to indicate that EPPO's transborder investigations should be made easier and not rely on traditional forms of mutual legal assistance, replaced the notion of a 'single legal area' proposed by the Commission, in which the EPPO would conduct investigations and prosecutions, Hans – Hogel Herrnfeld (n 19) 286.

[73] International comity, a concept much used in public and private international law, can be defined as 'courtesy, reciprocity, moral obligation, or respect for foreign sovereignty', Lorena Bachmaier Winter (n 30) 330 especially footnote 27.

[74] OLAF was established in 1999 to replace UCLAF ('Unite´ de Coordination de la Lutte Anti-Fraude'). See more on how the latter was replaced by OLAF in Anne Weyembergh Chloé Brière, 'The future cooperation between OLAF and the European Public Prosecutor's Office' 2018, Vol. 9(1) 62, 65. OLAF's investigative powers are mainly defined in Regulation 883/2013 of the Parliament and of the Council of 11 September 2013 in conjunction with the provisions of the Regulations 2185/9640 and 2988/95. Its powers include the possibility of conducting on-the-spot checks and inspections. Two kinds of investigations are foreseen, the internal investigations conducted in the EU's institutions, bodies, agencies, and offices (Art 4 Regulation 883/ 2013) and the external ones conducted on the premises of economic operators in the Member States, in third countries and on the premises of international organisations (Article 3).

[75] Andrea Venegoni, 'The new frontier of PFI investigations, The EPPO and its relationship with OLAF' (2017) 4 eucrim 193, 195.

[76] Petr Klement, 'OLAF at the gates of Criminal Law' (2017) 4 eucrim, p.196.

However, OLAF maintains its competence for minor financial cases and for transnational VAT cases, under the threshold of €10 million[77] and will keep its exclusive powers in the field of internal investigations, as well as in the Member States not participating to the EPPO[78]. So long as OLAF continues to operate, it should establish and maintain an effective and close cooperation with the EPPO, given the convergence of their objectives and the complementarity and interconnection of their mandates[79]. In the framework of this cooperation OLAF shall provide support to the EPPO's activities by providing information, analyses (including forensic analyses), expertise and operational support and by conducting administrative investigations[80].

Following the adoption of the EPPO Regulation, OLAF's legislative framework of investigations was further amended and strengthened to ensure that the effectiveness of its investigations will not be hindered by any unclarity thereof and that its administrative investigations will complement the EPPO's criminal proceedings, without changing its mandate[81]. Indeed, as far as external investigations are concerned OLAF had no autonomous investigative powers on an EU level to obtain evidence and specifically e-evidence but was much dependent on national law[82]. Furthermore, its legislative framework of external investigations was rather complex and ambiguous regarding the collection of e-evidence, such as computer data since it was not clear from its provisions whether it could conduct digital forensic operations[83]. Under the new rules, OLAF has extensive powers to gather evidence, including e-evidence, irrespective of the type of medium on which the latter is stored[84], both in the course of external and internal investigations, even if data is stored on privately owned devices, when latter are used for work purposes[85]. However, the exercise of such power is not completely independent from the national legislations since the inspection of such devises, during external investigations, is subject to the same conditions and to the same extent that national control authorities are allowed to investigate privately owned devices[86].

The Office has also drafted guidelines on Digital Forensic Procedures, which are rules to be followed by OLAF staff with respect to the identification, acquisition, imaging, collection, analysis and preservation of e-evidence, to ensure the integrity and authenticity of the evidence gathered during the Office's investigation[87]. The guidelines also contain specific provisions for access to data stored remotely or held by Cloud Service

[77] Art 22 para 1 EPPO Regulation.

[78] Lothar Kuhl, 'The European Public Prosecutor's Office – More Effective, Equivalent and Independent Criminal Prosecution against fraud?', (2017) 3 eucrim 135, 140, Petr Klement (n 76)197.

[79] Recital (103) and Art. 101 para (1) EPPO Regulation. The specific and detailed provision regarding the EPPO's cooperation with OLAF was inserted after it became clear that the EPPO would be established through enhanced cooperation and thus OLAF would be the key partner in respect of the non – participating Member States, Anne Weyembergh Chloé Brière (n 74) 71.

[80] Articles 101 para 3 of the EPPO Regulation and Article 12 (e) and (f) of Regulation (EU, EURATOM) No 883/213 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (consolidated version).

[81] Recital (15) Regulation (EU, Euratom) 2020/223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations [2020] OJ L 437/49.

[82] For a more extensive analysis of OLAF investigative powers see M. Scholten & M. Simonato 'EU Report' in Michieli Luchtman & John Vervaele (eds) *Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with the other EU Law Enforcement Authorities (ECN/ESMA/ECB)* (2017) 9, 27ff. file:///C:/Users/User/Downloads/olaf.pdf accessed 17 May 2022, a study carried out under the Hercule III program (Regulation (EU) 250/2014 of the European Parliament and of the Council establishing a programme to promote activities in the field of the protection of the financial interests of the European Union (Hercule III programme) and repealing Decision (EC) 804/2004 [2014]OJ L 84). For an analysis of the finding of the study, see Kouen Bovend' Eerdt, 'Learning lessons – Reflecting on Regulation 883/2013 through Comparative Analysis' (2017) 4 eucrim 188.

[83] Michiel Luchtman & John Vervaele,'Comparison of the legal frameworks' ibid 293.

[84] In order to reflect the evolving technological progress, Recital (28) Regulation (EU, Euratom) 2020/223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013.

[85] Arts 3 para 5 and 4 para 2 (a) Regulation 883/2013 (consolidated version).

[86] Art 3para 5 Regulation 883/2013 (consolidated version).

[87] Guidelines on Digital Forensic Procedures for OLAF Staff (15 February 2016)https://ec.europa.eu/anti-fraud/investigations/digital-forensics_en accessed 17 May 2022.

Providers[88], as well as procedures to be followed in case it is claimed that the devices found on spot are exclusively personal or contain data of legally privileged nature[89]. However, although the guidelines are following the main technical reference standards, they have been criticised as lacking the technical precision and accuracy in several steps, since they don't mention how the specialised in digital forensics OLAF's staff[90] will proceed in practice, nor which programs will be used[91].

Nevertheless, the EPPO could avail itself of the OLAF's expertise and knowhow, when the investigations, falling under its competence, are likely to involve e-evidence and thus require specific forensic procedures to be followed. To this view EPPO and OLAF have already concluded a working arrangement, which contains specific terms concerning OLAF's support to EPPO, such as the conducting of operational analysis, including forensic activities of documents or data in any format acquired by the EPPO or OLAF and the provision of operational support of any kind, included the participation of OLAF staff in the EPPO investigation as expert[92].

## III. Admissibility issues of e-evidence gathered by EPPO

### i) The issue of admissibility of e-evidence

The EPPO Regulation has not harmonised the rules in the field of investigation and collection of evidence[93]. On the contrary, it stems from its provisions that EPPO's conducting of investigation will basically rely on national law[94]. Hence, it comes with no surprise that the relevant issues of the admissibility of evidence gathered by the EPPO is also left to be resolved by the national criminal procedure laws[95]. However, diversities are encountered regarding the admissibility of cross - border evidence as some countries accept such evidence if it has been collected in accordance with the lex fori, others if the lex loci has been complied with and there are even countries that admit the admissibility of the evidence collected abroad without any other check of the

[88] Art 7 of the Guidelines.
[89] Art 5.4 and 6.3 of the Guidelines
[90] The Digital Evidence Specialist as named in the Guidelines under art 1.4.
[91] Raffaella Brighi, Michele Ferrazzano, 'Digital Forensics: Best practices and perspective' in Michele Caianiello and Albrto Camon (eds) *Digital Forensic Evidence - Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (2021) 13,28.
[92]The working arrangement signed on the 5th July 2021, is available online https://www.eppo.europa.eu/sites/default/files/2021-07/Working_arrangement_EPPO_OLAF.pdf accessed 17 May 2022. For an analysis of the working arrangement see Julia Echanove Gonzalez de Anleo, Nadnine Colloczek, 'The European Antifraud Office and the European Public Prosecutor's Office: A work in progress' (2021) 3 eucrim, 187.
[93] The Regulation only contains basic rules of procedures concerning initiation and conducting of investigations (Art.26-40) and sets a minimum of investigative measures to be made available to EDPs for significant offences, Hans-Holger Herrnfeld, Judith Herrnfeld (n 7) 661.
[94] Article 5 para 3 of the EPPO Regulation provides that national law 'shall apply to the extent that a matter is not regulated by this Regulation'. Hence the provisions of the Regulation will only complement the national procedures and specifically those of criminal procedure. It has been argued that the Regulation establishes a system of full recourse to the national legal systems regarding the procedural mechanisms and the competencies of the judicial mechanisms for the conducting of investigations as is concluded from the wording of Art 28 para 1 of the EPPO Regulation, which specifically refers to national law, as opposed to that of Art 18 of the Commission's proposal, Dimitrios Zimianitis, 'The European Public Prosecutor's Office: Establishment, structure and procedural imprint in the national criminal procedural law' Poinika Chronika (2022) 1, 6.
[95] Christoph Burchard in Herrnfeld/Brodowski/Burchard eds (n11) 349. The unification of rules applied to gathering of evidence would create a more consistent procedural framework for the EPPO and would ensure its admissibility before Court, Katalin Ligeti and Michele Simonato, The European Public Prosecutor's Office: Towards a truly European Prosecution Service?' (2013)4 New Journal of European Criminal Law 7, 18ff. However, unification of rules of evidence would entail a codification of criminal procedure law at EU level, which was considered, according to the Commission's Green Paper on Criminal Law Protection of the Financial Interests of the European Community and the Establishment of a European Prosecutor, disproportionate to the objective pursued with the creation of an EPP, Ladislav Hamran and Eva Szabova, 'European Public Prosecutor's Office: – CUI BONO?' (2013)4 New Journal of European Criminal Law 40, 54ff. Apart from that, any effort of adopting common rules in the field of criminal procedure law would be undermined by the reluctance of member states, still perceiving the Union's intervention in this field as threat to nation-state sovereignty, Katalin Ligeti and Michele Simonato, ibid 19. See also, Frédéric Baab, 'Le parquet européen : un projet entre audace et réalisme politique' (2021) 1 eucrim 45.

process of gathering followed[96]. The Regulation contains no admissibility criteria for the evidence presented before Courts by the prosecutors of EPPO, but rather introduces a simple non-discrimination clause under Article 37, which provides that such evidence shall not be denied admission on the mere ground that it was gathered in another Member State[97]. Thus, this provision gives great discretion to national Courts to deny the admissibility of evidence collected if other grounds exist, besides its foreign origin[98], invoking a broad range of fundamental principles, especially if this provision is read in conjunction with Recital 80, which suggests that the admission of evidence should respect the fairness of the procedure and the suspect or accused person's rights of defence under the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms[99]. National courts may be even more resistant to accept the admissibility of cross-border e-evidence, since the latter is most often collected through special investigative techniques, where there is great divergence between the national laws of the Member States[100]. The risk of non – admission of cross – border evidence is only partially eliminated by the provision of Article 32, which stipulates that the formalities and procedures indicated by the handling EDP shall be observed when enforcing a cross-border investigative measure. The reasons for this are that the assigned measures are basically conducted under the provisions of the Regulation and the national law of the state where they are enforced[101] and because an exception of order public clause is stipulated, allowing the member states of the EDP to not comply with the formalities indicated if they are contrary to the fundamental principles of its law[102].

The issue of admissibility is equally problematic regarding e-evidence, as there is no uniform legal framework within the European Union's Member States regarding its collection, storage, and exchange, although legal instruments have been implemented at European level relevant to the collection of e-evidence[103]. Thus, the collection of e-evidence not only heavily relies on national laws, but these laws may be outdated or, even if they are adapted to recent technological developments, not all member states have kept the same pace and some even still rely on traditional criminal procedure laws, hence resulting in an even bigger fragmentation of the procedures of investigations involving e-evidence[104]. Furthermore, although investigations in communications systems are very likely to entail casual findings, meaning evidence related to another crime, than the one investigated, there are no harmonised rules on the treatment and admissibility of such findings[105].

Admissibility issues also arise with evidence collected by LEAS from private sector through voluntary cooperation, a common practice nowadays as mentioned above, since there is not yet a uniform European framework of rules and procedures of compliance when accessing such data. Furthermore, as the regulatory framework of unilateral transborder access to data varies widely among members states, the rules of admissibility of the data thus gathered also vary. In some countries the evidence obtained through unilateral transborder access can be used in criminal proceedings, even if the procedure is not based on a specific permission under international law such as article 32b of the Budapest Convention on Cybercrime, while in others this depends on the specific circumstances[106]. Finally, some countries have enacted specific legislation allowing their investigation authorities to extend searches to computer systems located abroad, if they are

[96] The principle of non - inquiry, see Lorena Bachmaier Winter (n 30) 324.
[97] Silvia Allegrezza and Anna Mosna, (n 26)159.
[98] Ibid 159.
[99] Case Law on the admissibility of evidence has been mostly developed by the European Court of Human Rights and much less by the European Court of Justice, Elise Martin-Vignerte, 'Procedural safeguards in EPPO cross-border investigations' (2020 ERA FORUM) 507.
[100] Compared to other investigation measures where some convergence has already been succeeded such as pre -trial interrogation of witnesses, Katalin Ligeti, 'The European Public Prosecutor's Office: How should the rules applicable to its procedure be determined?' (2011) 1 EuCLRev 123, 146, 147 esp. footnote 128
[101] The article introduces a combination of forum regit actum and locus regit actum rule.
[102] Christoph Burchard (n 93) 302.
[103] Maria Angela Biasiotti, 'Present and Future of the Exchange of Electronic Evidence in Europe', in Maria Angela Biasiotti, Jeanne Pia Mifsud Bonnici, Joe Cannataci, Fabrizio Turchi (eds), *Handling and Exchanging Electronic Evidence Across Europe* Volume 38 (Springer 2018),14.
[104] Jeanne Pia Mifsud Bonnici, Melania Tudorica, and Joseph A. Cannataci (n 6) 211.
[105] Lorena Bachmaier Winter (n 26) 130.
[106] Cybercrime Convention Committee (T-CY) 'Transborder Access and Jurisdiction: What Are the Options?', 2012 29 https://rm.coe.int/16802e79e8 accessed 17 May 2022. For the admissibility of evidence gathered through the interception of telecommunications, without technical assistance, in case the Member State where the interception was conducted was not notified see Lorena Bachmaier Winter (n 30) 334.

accessible from devices located in their jurisdiction, under specific preconditions and hence no admissibility issues arise for the e-evidence thus collected[107] at least in the domestic jurisdiction, but such issues could arise if the evidence was to be used in a different jurisdiction.

It is apparent that the EPPO, gathering e-evidence in different jurisdictions, with no consistent regulatory framework for the mechanisms described above will be faced with admissibility issues, which are only partially, if not at all, resolved by Article 37 of the Regulation.

OLAF's investigative powers are also dependent on national law both for the scope and enforceability of its competence[108]. The situation is not different regarding the collection of e-evidence. As mentioned above, the Office, when conducting investigations has access to any data, irrespective of the medium, where the latter is stored. The Office may as well subject privately owned devices to inspection, when used for work purposes, but, during an external investigation it may do so only under the same conditions and to the same extent that national control authorities are allowed to investigate privately owned devices, while during an internal investigation under the conditions set in the decisions adopted by the relevant institution, body, office, or agency[109]. Even when drafting the report with the conclusions of an investigation conducted and the recommendations of further measures to be taken, the provisions of the national law of the member state concerned, should be taken into account[110]. This is because the material of OLAF's investigation may then be used in national proceedings especially criminal ones. To enhance the admissibility of such material procedural safeguards have been introduced in the OLAF Regulation, which have been further strengthened through its amendment, by the creation of a controller of procedural guarantees and the introduction of a complaint's mechanism[111]. Furthermore, an assimilation rule was introduced under Article 11 of the Regulation according to which, OLAF final reports shall constitute admissible evidence in administrative or judicial proceedings of the Member States and shall be treated in the same way as national administrative reports drawn up by administrative inspectors. However, this rule was criticised as insufficient by academics, Eu bodies and OLAF itself, since it presupposes the existence of an administrative authority with a mandate and powers that can be considered 'equivalent' to those of OLAF[112]. Furthermore, since there is no harmonisation of rules and practices on the admissibility of administrative reports in criminal proceedings across Member States, in many cases duplication of investigation activities, already conducted by OLAF was not avoided[113]. To address the shortcomings of the assimilation rule, the European Parliament in April 2019 suggested that OLAF reports should 'constitute admissible evidence in judicial proceedings', including criminal ones, upon simple verification of their authenticity[114]. This suggestion was not followed, and the assimilation clause was eliminated only for reports to be used in the context of judicial proceedings of a non-criminal nature and in administrative proceedings, whereas it has been maintained for reports used in criminal proceedings[115].

If the EPPO decides to use for its prosecutions e - evidence acquired and analysed by OLAF, in the framework of their operational cooperation, it will have to address the same admissibility issues concerning evidence gathered by an administrative authority and used in the framework of criminal proceedings, even if

[107] For example, Belgium and Portugal, Council of Europe, 'Transborder Access and Jurisdiction: What Are the Options?' ibid, 32. See an analysis of the relevant provisions in Anna-Maria Osula (n 56)729, 730

[108] Mirka Janda, Romana Panait 'The OLAF Regulation, evaluation and future steps' (2017) 4 eucrim 182, 185. Koen Bovend' Eerdt (n 82) 189.

[109] Arts 3 para 5 and 4 para 2 (a) Regulation 883/2013, consolidated version.

[110] Art 11 para 2 Regulation 883/2013 (consolidated version).

[111] Articles 9a and 9b Regulation 883/2013, inserted by Article 1 para 9 of Regulation 2020/223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013.

[112] M. Luchtman, A. karagianni, K. Bovend' Eerdt, 'EU administrative investigations and the use of their results as evidence in national punitive proceedings' in Fabio Giuffrida and Katalin Ligeti (eds.) *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings* (University of Luxembourg June 2019) 44 esp. footnote 167.

[113] F. Giuffrida and K. Ligeti, 'Introduction', ibid 12.

[114] European Parliament, 'Legislative resolution of 16 April 2019 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 883/2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) as regards cooperation with the European Public Prosecutor's Office and the effectiveness of OLAF investigations (COM (2018)0338 2021/C 158/32)', amendment 85.

[115] Article 11 para 2 (a) (b) and (c) Regulation 883/2013, consolidated version. However, due to the lack of harmonisation of rules on national criminal proceedings, it doesn't seem probable that even this amendment would have provided an adequate answer to the admissibility issues raised, F. Giuffrida and K. Ligeti (n 112) 3.

the latter are to take place in the Member State where the evidence was gathered. The issue will be more complex if the evidence collected is to be used in criminal proceedings in a different Member State, especially if its collection had implications on the rights of privacy, for which differentiated national procedural safeguards exist[116]. OLAF's inspections of privately owned devices, even if they are used for work purposes, interfere with privacy rights, but the impact of the interference depends on the national law of the state where the investigations are taking place. Even if procedural guarantees are partially harmonised within the OLAF's framework of investigation and on – the - spot checks, the procedural frameworks concerning the interference with privacy rights, vary among the member states. Consequently, there is no guarantee that the results of such inspections, conducted according to national rules and conditions of a given Member State, will be admitted as evidence in a different Member State, where prosecutions are to be ordered. The issue becomes more complicated when investigatory measures of an intrusive nature, such as interception of communications or seizure of e-evidence which are usually only available for criminal investigations, are to be used in administrative investigations[117]. The relevant national provisions on highly intrusive investigatory measures, such as interception of communications, are differentiated reflecting the national sensitivities on the privacy rights infringed[118]. OLAF's forensic operations, during on-the-spot checks, to acquire digital evidence are conducted in close cooperation with the competent authorities of the Member State concerned and according to the legal provisions of that Member State[119]. Thus, the use of highly intrusive measures, during these operations may be permissible in one Member State and impermissible in another and consequently issues of inadmissibility of the relevant e-evidence collected are raised.

To address the issues of admissibility, OLAF is called, in close cooperation with the EPPO to observe the applicable procedural safeguards of the EPPO Regulation, concerning the rights of the suspects and accused persons and judicial review, when it performs, within its mandate, supporting measures requested by the EPPO[120]. However, it is much doubted whether this provision protects the admissibility of evidence, as intended, let alone, since the reports to be drawn up by OLAF, after the conclusion of a complementary investigation requested by EPPO[121], will also be subject to the assimilation rule and thus its admissibility will depend on the national procedural laws and practices of the 22 member - states participating to the EPPO.

ii) The issue of assessment of e-evidence

The assessment of evidence refers to the evaluation of whether a certain piece of evidence has any probative value and which[122]. The EPPO Regulation does not affect, according to Article 37 para (2),the power of the trial Court to freely assess the evidence presented either by the defendants or the prosecutors of the EPPO. Thus, the relevant national rules of criminal procedure on the assessment of evidence shall be fully applicable to evidence presented not only to the trial Court but also to all national courts that become involved in the EPPO proceedings[123].

The assessment of evidence in electronic form is a rather delicate issue since e-evidence is by nature volatile and thus subject to be altered or manipulated[124]. Because of these special features safeguarding the authenticity and integrity of e-evidence is crucial for the assessment of its probative value[125]. And although

[116] F. Giuffrida and K. Ligeti (n 112) 12.

[117] For the issues arising from the coexistence of 'criminal' and 'administrative' types of investigative measures see M. Luchtman, A. karagianni, K. Bovend' Eerdt (n 112)12.

[118] Inés Armad, 'The European Investigation Order and the lack of European Standards for gathering evidence - Is a Fundamental Rights-Based Refusal the Solution?' (2015) 6, New Journal of European Criminal Law 8, 10. Interceptions of communications are in general considered exceptional measures, admitted only in relation to serious crimes, the definition of which varies per country, and are subject to legal procedures (e.g. judicial warrant), Jeanne Pia Mifsud Bonnici, Melania Tudorica, and Joseph A. Cannataci (n 6) 216.

[119] Art. 6 para (1) and (2) of Guidelines on Digital Forensic Procedures for OLAF Staff (15 February 2016).

[120] Art 12e para 3 OLAF Regulation 883/2013 (consolidated version).

[121] Art 101 para (3) EPPO Regulation and arts 6.2, 6.2.8 of the working arrangement between EPPO and OLAF.

[122] Christoph Burchard (n 11) 351.

[123] Even Courts deciding for pretrial detention, given the Regulation's option of not affecting at all national applicable laws on the assessment of evidence, ibid 351 para 14.

[124] Hong Wu Guan Zheng, 'Electronic evidence in the blockchain era: New rules on authenticity and integrity' (2020) 36 Computer Law & Security Review 1.

[125] Integrity refers to the physical device where data is stored and means that 'the device and data sought to be introduced as evidence is the same as that which was originally discovered and subsequently taken into custody', while authenticity

national legal systems do not have explicit regulations on the assessment of the probative value of e - evidence[126], international guidelines and best practices have been provided for the handling of e-evidence, such as the Handbooks[127] and Guides[128] drafted by the European Union Agency for Network and Information Security (ENISA) and the Electronic Evidence Guide (EEG)[129], developed by the Council of Europe. Whereas it is true that none of the rules and procedures contained therein is legally binding, it is generally recognised as very important to duly document the data acquisition procedure, according to the chain of custody[130]. However, most Courts will not be able to interpret the conclusions drawn from the forensic findings and assess the procedures followed for safeguarding the probative value of e-evidence. For this reason, in most countries forensic experts are called upon to analyse and give expert opinions on the assessment and evaluation of e-evidence, although Courts may usually make different decisions, if the latter are motivated[131].

As a conclusion, once e-evidence presented by EPPO is admitted by national Courts, the issue of its assessment may differ, depending on applicable national rules, but at least common practices exist to ensure its probative value.

## IV. Conclusions

The collection and admissibility of e-evidence gathered by the EPPO are paramount for a successful prosecution and hence for the accomplishment of its objectives. However, it has been demonstrated that there is no common European legal framework for the collection, use and exchange of e-evidence and no such framework is provided by the EPPO Regulation[132]. One step towards the harmonisation of rules concerning the collection e-evidence has been made by the ratification of the Budapest Convention by all member states and another step forward would be the ratification of the Second Protocol to the Convention on Cybercrime, containing further rules on the collection of evidence from providers and entities located abroad[133]. Moreover, the framework of accessing data held by the private sector, will be further harmonised in the future, if the Regulation on European Production and Preservation Orders for electronic evidence in Criminal matters is adopted. Nonetheless, since investigations involving e-evidence may entail highly intrusive measures, such as interceptions, remote and computer assisted searches, specific legal provisions should be implemented union wide, accompanied by adequate safeguards for the privacy rights affected[134]. The issues raised concerning e-

---

refers to the stored data residing on the device and means that 'the digital information obtained from the device is a true and accurate representation of the original data contained on the device', 'UNDOC Comprehensive study on cybercrime (Draft February 2013)' 158 www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf accessed 17 May 2022.

[126] OLAF's Guidelines on Digital Forensic Procedures contain specific provisions, under Article 4 for the conducting of forensic operations to ensure the chain of custody.

[127] Identification and handling of electronic evidence Handbook, Document for teachers September 2013 and the Digital Forensic Handbook. Document for Teacher, September 2013, Mobile Threats Incident Handling (Part II) Handbook, Document for teachers, September 2015 and Introduction to Network Forensics FINAL VERSION 1.1 AUGUST 2019, accessible at the ENISA website, www.enisa.europa.eu accessed 17 May 2022.

[128] Electronic evidence - a basic guide for First Responders, Good practice material for CERT first responders file:///C:/Users/User/Downloads/Good%20practice%20material%20for%20first%20responders%20(3).pdf accessed 17 May 2022.

[129] Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges version 1.0, Strasbourg, France, 18 March 2013 https://rm.coe.int/0900001680a22757 accessed 17 May 2022.

[130] This is defined as the documentation that details how digital evidence was handled from the moment it was identified as evidence until its presentation to judge in the trial phase, Maria Angela Biasiotti, Joseph A. Cannataci, Jeanne Pia Mifsud Bonnici, and Fabrizio Turchi, 'Introduction: Opportunities and Challenges for Electronic Evidence' (n 6) 5.

[131] Jeanne Pia Mifsud Bonnici, Melania Tudorica, and Joseph A. Cannataci 'Chapter 11 The European Legal Framework on Electronic Evidence: Complex and in Need of Reform' (n 6) 218.

[132] Apart from a partial harmonisation under Article 30, providing for specific investigation measures involving e-evidence to be adopted by member states under the preconditions set therein, Dominik Brodowski (n 11) 272.

[133] On the 5th of April 2022, the Council adopted a decision authorising Member States to sign, in the interest of the EU, the second additional protocol to the convention on cybercrime of the Council of Europe (Budapest convention) www.consilium.europa.eu/en/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/ accessed 17 May 2022.

[134] Maria Angela Biasiotti, Joseph A. Cannataci, Jeanne Pia Mifsud Bonnici, and Melania Tudorica 'The Way Forward: A Roadmap for the European Union' (n 6) 394 ff.

evidence stored or located in the cloud also require specific rules, not limited by territorial boundaries, and oriented by a 'universal jurisdiction' approach in the investigation of serious crimes[135]. The existing guidelines and best practices for the collection of e-evidence should also be further developed and become common knowledge of LEAs across the European Union, while constant training of both the LEAs and the judiciary is necessary to ensure that the knowledge acquired does not fall behind the rapid technological change[136].

However, since the EPPO Regulation only contains an assimilation clause and leaves great discretion to national Courts to reject evidence gathered by EDPs as inadmissible, the issues of the admissibility of the e-evidence will continue to jeopardise the success of the prosecutions to be ordered, unless a coherent and harmonised legal framework is adopted[137]. It has been suggested that the issue of admissibility of cross border evidence, could be addressed by the adoption of a European legal instrument, under Article 82 para2 TFEU, providing for the mutual recognition of evidence collected by the judicial authorities of another Member State and thus establishing an inclusion rule of evidence, accompanied by an exclusionary rule based on the existing jurisprudence of the ECHR concerning human rights infringed within the process of evidence gathering[138]. In any case specific rules should be considered for e-evidence. So long as no such legislation is put in place and no uniform EPPO procedures exist, it has been argued that recourse to the EIO, already transposed in all Member States and used by their competent authorities, could provide for a more coherent scheme for the EPPO's investigations and enhance the recognition of the relevant evidence gathered[139]. Furthermore, since OLAF seems to become the EPPO's 'right hand' and its investigations, within the regime of Art. 101 of the EPPO Regulation, will increasingly involve e-evidence, the legislative framework of its investigative powers should be more coherent and less dependent on national laws. If a clear set of autonomous investigative powers was given to OLAF[140], which would be exercised in the same way in all Member States of the Union and would be subject to the same procedural safeguards provided under the EPPO Regulation, then the admissibility issues arising from different national thresholds and guarantees for the conduct of investigations are significantly limited.

As conclusion, it is observed that the EPPO, being established by enhanced cooperation and conducting investigations in a widely fragmented legislative framework, will largely depend on the policies and legislative initiatives, concerning e-evidence, taken both on national, European, and international level, to ensure that such evidence is lawfully acquired and then admitted before national Courts.

[135]Jeanne Pia Mifsud Bonnici, Melania Tudorica, and Joseph A. Cannataci 'Chapter 11 The European Legal Framework on Electronic Evidence: Complex and in Need of Reform' (n 6) 230.

[136] See further propositions on best practices and training in Maria Angela Biasiotti, Joseph A. Cannataci, Jeanne Pia Mifsud Bonnici, and Melania Tudorica, 'The Way Forward: A Roadmap for the European Union' (n 6) 386, 408, 411 ff.

[137] Neither the Directive 2014/41/EU regarding the European Investigation Order in criminal matters, nor the Proposal for a Regulation of the European Parliament and the Council European Production and Preservation Orders for electronic evidence in Criminal matters contain rules on the admissibility of evidence, Katalin Ligeti, Balázs Garamvölgyi , Anna Ondrejová, Margarete von Galen, 'Admissibility of Evidence in Criminal Proceedings in the EU', (2020)3 eucrim 201, 205.

[138] Ibid, 206.

[139] András Csúri, 'Chapter 9 Towards an Inconsistent European Regime of Cross-Border Evidence: The EPPO and the European Investigation Order' in Willem Geelhoed, Leendert H. Erkelens, Arjen W.H. Meij (eds) *Shifting Perspectives on the European Public Prosecutor's Office*, (Springer 2018) 141, 150.

[140] Giving an autonomous mandate of investigations to OLAF was one of the propositions put forward in the Report 'Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with other EU law enforcement authorities (ECN/ESMA/ECB)' Michiel Luchtman & John Vervaele, 'Summary of main findings and overall conclusions' (n 82) 328.

References

Allegrezza S., Mosna A., 'Cross-Border Criminal Evidence and the Future European Public Prosecutor. One Step Back on Mutual Recognition?' in Lorena Bachmaier Winter (ed), *The European Public Prosecutor's Office- The challenges ahead,* vol 1 (Springer 2018).
Armad I., 'The European Investigation Order and the lack of European Standards for gathering evidence - Is a Fundamental Rights-Based Refusal the Solution?' (2015) 6, New Journal of European Criminal Law 8.
Baab F., 'Le parquet européen : un projet entre audace et réalisme politique' (2021) 1 eucrim 45.
Bachmaier Winter L., Cross- border Investigations under the EPPO proceedings and the quest for balance, in Lorena Bachmaier Winter (eds), *The European Public Prosecutor's Office, The Challenges ahead* Springer Volume 1 (Springer 2018).
Bachmaier Winter L., Mutual Recognition and Cross-Border Interception of Communications: The Way Ahead for the European Investigation Order, in Chloé Brière and Anne Weyembergh (eds) *The Needed Balances in EU Criminal Law Past, Present and Future (*Hart Publishing 2018).
Biasiotti M.A., 'A proposed electronic evidence exchange across the European Union'(2017)14 Digital Evidence and Electronic Signature Law Review 1.
Biasiotti M.A., 'Present and Future of the Exchange of Electronic Evidence in Europe', in Maria Angela Biasiotti, Jeanne Pia Mifsud Bonnici, Joe Cannataci, Fabrizio Turchi (eds), *Handling and Exchanging Electronic Evidence Across Europe* Volume 38 (Springer 2018).
Biasiotti M.A., Cannataci J.A., Mifsud Bonnici J.P., Turchi F., 'Introduction: Opportunities and Challenges for Electronic Evidence' in Maria Angela Biasiotti, Jeanne Pia Mifsud Bonnici, Joe Cannataci, Fabrizio Turchi (eds), *Handling and Exchanging Electronic Evidence Across Europe* Volume 38 (Springer 2018).
Biasiotti M.A., Cannataci J.A., Mifsud Bonnici J.P., Tudorica M. 'The Way Forward: A Roadmap for the European Union' in Maria Angela Biasiotti, Jeanne Pia Mifsud Bonnici, Joe Cannataci, Fabrizio Turchi (eds), *Handling and Exchanging Electronic Evidence Across Europe* Volume 38 (Springer 2018).
Boulet G., Hernanz N., 'Cross-border law enforcement access to data on the Internet and rule of law challenges in the EU' 2013, SAPIENT Deliverable 6.6, issue SAPIENT Policy Brief 6.6 https://www.academia.edu/4959180/Cross_border_law_enforcement_access_to_data_on_the_Internet_and_rule_of_law_challenges_in_the_EU.
Bovend' Eerdt K., 'Learning lessons – Reflecting on Regulation 883/2013 through Comparative Analysis' (2017) 4 eucrim 188.
Brighi R., Ferrazzano M., 'Digital Forensics: Best practices and perspective' in Michele Caianiello and Albrto Camon (eds) *Digital Forensic Evidence - Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (2021).
Brodowski D., in Herrnfeld/Brodowski/Burchard eds, European Public Prosecutor's Office: Article-by-Article Commentary, (Bloomsbury Publishing 2020).
Burchard C. in Herrnfeld/Brodowski/Burchard eds, European Public Prosecutor's Office: Article-by-Article Commentary, (Bloomsbury Publishing 2020).
Csúri A., 'Chapter 9 Towards an Inconsistent European Regime of Cross-Border Evidence: The EPPO and the European Investigation Order' in Willem Geelhoed, Leendert H. Erkelens, Arjen W.H. Meij (eds) *Shifting Perspectives on the European Public Prosecutor's Office,* (Springer 2018).
De Hert P., Parlar C. Thumfart J., 'Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland' (2018) 9 (3) New Journal of European Criminal Law 326.
Franssen N., 'The Future judicial cooperation between the EPPO and non – participating member states' (2018) 9(3) New Journal of European Criminal Law 291.
Giuffrida F., Ligeti K., 'Introduction' in Fabio Giuffrida and Katalin Ligeti (eds.) *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings* (University of Luxembourg June 2019).
Gonzalez de Anleo J H., Colloczek N., 'The European Antifraud Office and the European Public Prosecutor's Office: A work in progress'(2021) 3 eucrim, 187.
Hamran L. Szabova E., 'European Public Prosecutor's Office: – CUI BONO?' (2013) 4 New Journal of European Criminal Law 40.
Herrnfeld Hans-Holger, Herrnfeld Judith 'The European Public Prosecutor's Office – where do we stand?' (2021) ERA forum 657.
Herrnfeld H.-H. in Herrnfeld/Brodowski/Burchard eds, European Public Prosecutor's Office: Article-by-Article Commentary, (Bloomsbury Publishing 2020).

Janda M. Panait R., 'The OLAF Regulation, evaluation and future steps' (2017) 4 eucrim 182.
Klement P., 'OLAF at the gates of Criminal Law' (2017) 4 eucrim, p.196.
Kuhl L., 'The European Public Prosecutor's Office – More Effective, Equivalent and Independent Criminal Prosecution against fraud?', (2017) 3 eucrim 135.
Ligeti K., 'The European Public Prosecutor's Office: How should the rules applicable to its procedure be determined?' (2011) 1 EuCLRev 123.
Ligeti K. Simonato M., The European Public Prosecutor's Office: Towards a truly European Prosecution Service?' (2013)4 New Journal of European Criminal Law 7.
Luchtman M. & Vervaele J., 'Comparison of the legal frameworks' in Michieli Luchtman & John Vervaele (eds) *Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with the other EU Law Enforcement Authorities (ECN/ESMA/ECB)* (2017).
Luchtman & John Vervaele, 'Summary of main findings and overall conclusions' in Michieli Luchtman & John Vervaele (eds) *Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with the other EU Law Enforcement Authorities (ECN/ESMA/ECB)* (2017).
Luchtman M., karagianni A., Bovend' Eerdt K., 'EU administrative investigations and the use of their results as evidence in national punitive proceedings' in Fabio Giuffrida and Katalin Ligeti (eds.) *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings* (University of Luxembourg June 2019).
Martin-Vignerte E., 'Procedural safeguards in EPPO cross-border investigations' (2020 ERA FORUM).
Mifsud Bonnici Jeanne Pia, Melania Tudorica, and Joseph A. Cannataci 'Chapter 11 The European Legal Framework on Electronic Evidence: Complex and in Need of Reform' in Jeanne Pia Mifsud Bonnici Melania Tudorica Joseph A. Cannataci and Fabrizio Turchi (eds) *Handling and exchanging electronic evidence across Europe* (Springer 2018) 219.
Mouzakis D., 'Cross – border investigations of the EPPO: progress or a step backwards in judicial cooperation in criminal matters' (2022) 1 Poinika Chronika 11.
Osula M.A., 'Transborder access and territorial sovereignty' (2015) 31 Computer Law and Security Review 720.
Osula M.A., *Remote search and seizure of extraterritorial data* (University of Tartu Press 2017).
Rojszczak M., Cloud act agreement form an EU perspective (2020)38 Computer Law & Security Review, 3.
Scholten M. & M. Simonato 'EU Report' in Michieli Luchtman & John Vervaele (eds) *Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with the other EU Law Enforcement Authorities (ECN/ESMA/ECB)* (2017).
Seger A, 'e-evidence and access to data in the cloud, results of the cloud evidence group of the cybercrime Convention Committee' in Maria Angela Biasiotti, Jeanne Pia Mifsud Bonnici, Joe Cannataci, Fabrizio Turchi (eds), *Handling and Exchanging Electronic Evidence Across Europe* Volume 38 (Springer 2018).
Stefan M., González Fuster G., 'Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters State of the art and latest developments in the EU and the US', 27 https://www.ceps.eu/download/publication/?id=10797&pdf=MSGGF_JudicialCooperationInCriminalMatters-2.pdf
Tinoco-Pastrana A., 'The Proposal on Electronic Evidence in the European Union', eucrim, issue 1/2020 46-50.
Venegoni A., 'The new frontier of PFI investigations, The EPPO and its relationship with OLAF' (2017) 4 eucrim 193.
Weyembergh A. Brière C., 'The future cooperation between OLAF and the European Public Prosecutor's Office' 2018, Vol. 9(1) 62.
Zimianitis D., 'The European Public Prosecutor's Office: Establishment, structure and procedural imprint in the national criminal procedural law' Poinika Chronika (2022) 1.