Gathering Electronic Evidence for Administrative Investigations

Exploring an Under-the-Radar Area

Stanisław Tosza *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

The intense debate over the past few years on access to data for criminal investigations has led to the adoption of the E-evidence package. Yet, electronic evidence is no less crucial for punitive administrative proceedings. One administrative investigation authority that could benefit from more extensive access to electronic evidence is OLAF, which, at this point, does not seem to have the power to request data from service providers. Such powers could be essential, however, for the detection and investigation of fraud or corruption. This article argues the need for a general and thorough reflection on access to electronic evidence from Internet Service Providers (ISPs) in administrative punitive proceedings. It also discusses the transfer of this type of evidence between administrative and criminal proceedings (in both directions) in order to more specifically justify an extension of OLAF's powers to be able to request such evidence.

AUTHOR

Stanisław Tosza

Associate Professor in Compliance and Law Enforcement
University of Luxembourg

CITE THIS ARTICLE

Tosza, S. (2023). Gathering Electronic Evidence for Administrative Investigations : Exploring an Under-the-Radar Area. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-018

Published in eucrim 2023, Vol. 18(2) pp 216 – 222

https://eucrim.eu

ISSN:

I. Introduction

With the ever-increasing digitalisation of almost every aspect of human activities, any type of infringement – be it criminal or administrative – leaves digital traces, which may become crucial as evidence in punitive proceedings. Yet, access to electronic evidence is far from straightforward, as it is often in the hands of foreign service providers. Outdated rules of territoriality thus hamper law enforcement efforts, because instruments of international cooperation, such as mutual legal assistance, must be used, which complicate the procedure and render it disproportionately lengthy.[1] This is linked with the fact that often the data has to be obtained from US service providers given their market share. However, US law in principle prohibits the transfer of content data to foreign law enforcement without a decision of a US judge.[2] Numerous other factors of a legal and practical nature add complexity to the problem, such as encryption,[3] rules on admissibility of evidence,[4] and limitations of enforcement capacity,[5] to name just a few.

Three major initiatives are intended to remedy this situation, although it is too early to assess their impact. First, the EU has just adopted the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, which aims at addressing the above-mentioned difficulties.[6] Most importantly, it will allow law enforcement authorities in one Member State to compel service providers in another Member State to produce data without engaging the authorities of the latter. Second, the EU is negotiating an agreement on e-evidence with the USA, which would broaden the possibilities of US service providers to transmit data to foreign law enforcement authorities without the decision of a US judge.[7] Third, the recently adopted Second Protocol to the Cybercrime Convention also provides for possibilities to directly request data cross-border from digital companies, even if this would apply only to limited types of data.[8]

All these initiatives open the door to direct cross-border cooperation between law enforcement authorities and service providers, which is not without controversy and creates different legal problems. Intense debate during the lengthy process of negotiating the E-evidence Regulation (and its accompanying Directive) concerned such issues as: its legal basis,[9] the future relationship between the European Production Order and the European Investigation Order,[10] the role of EU data protection law,[11] and the future relationship with the US legal framework.[12] The adoption of the E-evidence package will not end the debate, rather the contrary. One of the most important questions is how service providers can be gatekeepers and protectors of fundamental rights while retaining a private entity nature.[13]

Administrative law enforcement has been notably absent from these debates and initiatives. The European E-evidence Regulation will solely apply to criminal proceedings.[14] Also, the Second Protocol to the Cybercrime Convention is limited to criminal investigations only.[15] Yet, electronic evidence is no less crucial for punitive administrative proceedings. Although access to electronic evidence will arguably not be as broad as that for criminal investigations, due to privacy limitation concerns, it will be increasingly more difficult to miss the golden opportunity that access to evidence through service providers offers for effective investigations. Already non-content data offers insights that may be essential for providing proof of misconduct.[16]

An administrative investigation authority that could benefit from more extensive access to electronic evidence is the European Anti-Fraud Office (OLAF), which so far has no specific provisions on cooperation with Internet Service Providers (hereinafter: ISPs). The need to access new types of evidence is well exemplified by the recently added possibility for OLAF to request bank account information.[17] However, we may find possibilities to access electronic evidence in other administrative proceedings, e.g., in financial supervision and the Market Abuse Regulation.

https://doi.org/10.30709/eucrim-2023-018

This article aims to sketch out the problem of gathering of electronic evidence in the context of administrative punitive enforcement and the need for research in this area. A particular focus will be placed on OLAF, its need for electronic evidence, and the lack of legal basis to request data from service providers. The article will also briefly present a recently launched research initiative to further explore this issue.

II. Need for Electronic Evidence

The distinctiveness of electronic evidence – contrary to more traditional sources of evidence – is that it can be obtained through a third party: the service provider. This feature is unique: even if access to written letters was possible as a criminal procedural measure, the traditional postal service neither had regular access to the content of the letters they delivered nor did they regularly gather metadata on these letters. In contrast, email service providers do both. Starting from the possibility to acquire data from telecommunication providers,[18] access to data from different kinds of ISPs has become crucial for successful investigations in recent years.

Data in possession of ISPs may be a treasure trove for enforcement authorities. The nature of cyberspace clashes with the limitations of enforcement, however, which hinder access to the data. While data can flow unhindered, at least in principle, law enforcement remains confined to national borders as prescribed in the seminal Lotus judgment.[19] In its conventional reading, the principle of territoriality mandates that if the data being sought is stored outside of the country of investigation, then instruments of cross-border cooperation need to be used, which renders access much more time-consuming, costly, and cumbersome.[20] This duality – attractiveness of electronic evidence gathered from third parties and inaptness of principles governing enforcement in cyberspace – characterises this field and has triggered a number of legislative and jurisprudential initiatives.

Over the past several years, the debate over access to electronic evidence gained prominence as regards access to data for criminal investigations. The laws of criminal procedure allowed the authorities to access this data, while providing the framework for protecting suspects' procedural safeguards. However, if the service provider was located in another country or the data was stored abroad, law enforcement was supposed to resort to instruments of cross-border cooperation: the European Investigation Order (EIO) within the EU's area of freedom, security and justice and mutual legal assistance (MLA) outside this area, in particular regarding content data from US companies.[21]

The necessary paperwork for MLA and the length of the procedure, compulsory even in purely local cases, garnered frustration on the part of law enforcement, leading to the use of voluntary cooperation with ISPs and to a reinterpretation of the principle of territoriality.[22] As to the latter, Belgium for instance decided to treat foreign providers actively targeting Belgian clients as if they were national providers. In two famous cases concerning Yahoo and Skype, these companies found themselves obliged to produce data according to a Belgian order, although the law of the place where they were headquartered (USA and Luxembourg, respectively) prohibited them from doing so.[23]

The ensuing discussion resulted in the adoption of the EU's E-evidence package (composed of a Regulation and a Directive), which offers a much faster way to gather electronic evidence in criminal proceedings. While the Regulation (hereinafter: EPOR) creates the new instruments of the European Production and Preservation Orders, the Directive is meant to ensure that there is at least one potential addressee for the newly created orders per each service provider entering the scope of the EPOR. The main premise of the Regulation is that competent authorities are entitled to issue binding requests to service providers offering services within the EU regardless of their place of establishment or the physical location of the data. Law enforcement authorities in one Member State will now be allowed to issue orders that are directly transmitted to private actors in

https://doi.org/10.30709/eucrim-2023-018

a different Member State and which have to be executed without any involvement of the authorities of that Member State (with a number of limited exceptions).[24]

III. Electronic Evidence in Administrative (Punitive) Investigations

It is a truism that the nature of administrative proceedings is different from that of criminal proceedings. Administrative decisions do not carry the stigma and moral reproach of criminal law punishments, and instruments of administrative law are less intrusive overall. They also serve different objectives and are not focused on prevention, retribution, or reparation in the same way as criminal enforcement; most of all, they are meant to ensure compliance with the regulatory legal framework.[25] However, punitive administrative proceedings may be sufficiently punitive to justify being treated as a "criminal charge" according to the *Engel* jurisprudence.[26]

In order to be effective, administrative authorities need to have efficient and modern tools at their disposal to gather evidence for these proceedings, with electronic evidence gathered from ISPs wielding increasing influence over enforcement in recent years. There are four ways in which administrative authorities may acquire this type of evidence from the service providers:

First, there may be a concrete legal basis allowing them to make such requests. For example, the Market Abuse Regulation (596/2014) provides that, under certain circumstances, competent authorities shall have the power to request existing data traffic records held by a telecommunications operator (Art. 23 (2) (h)). Particularly at the national level, however, such access may be controversial. For instance, the French legal framework regarding access to telecommunication data by administrative authorities has evolved dramatically during the last few years. Even though the case law of the European Court of Justice has been subject to criticism in France, the French Constitutional Council struck down several laws that did not take into consideration privacy and data protection, following the case law of the ECJ.[27] One interesting feature of the current legal framework is the creation of a new authority in charge of allowing these measures (*le contrôleur des demandes de données de connexion*).[28]

Secondly, data may be potentially requested from service providers by means of a more general legal basis concerning a request for information.[29] For instance, the European Central Bank may request data based on Art. 10 (1) (f) of SSM Regulation No 1024/2013. The Commission's Directorate General Competition may request information from third parties based on Art. 18 of Regulation 1/2003, which does not preclude using it to request information from ISPs. Competent national authorities may proceed similarly.

Thirdly, administrative enforcement authorities may simply request data from service providers on a voluntary basis. These requests are not binding for ISPs. This practice developed in criminal investigations due to the shortcomings of compelling ways of requesting data described above. It relies on the general willingness of ISPs to cooperate with law enforcement and allows the authorities to circumvent the problem of territoriality and the necessity of using cooperation instruments. However, such practice results in that the ISPs *de facto* take the responsibility to assess the legality and proportionality of the requests becoming guardians of the fundamental rights of their users instead of public authorities. Contrary to public authorities, however, the ISPs will perform such assessment in accordance with their business interest.[30]

Fourthly, electronic evidence may be transferred from other proceedings, be they administrative or criminal, if the law so permits. As established by the ECJ in *WebMindLicences*, in fact, EU law does not preclude administrative procedures from using evidence obtained in the context of a parallel criminal procedure that is still ongoing, provided that the rights guaranteed by EU law are observed.[31]

IV. OLAF and Gathering of Electronic Evidence

OLAF, at this point, does not appear to have the power to request data from service providers, which might be essential for the detection and investigation of fraud or corruption. OLAF needs to extend its powers in a way that reflects modern realities, as demonstrated by the addition of the possibility for OLAF to request bank account information.[32] In order to protect EU financial interests, in particular to combat fraud, corruption, and any other illegal activities affecting them, electronic evidence will become increasingly relevant.

OLAF has also a less advantageous position in this respect than the European Public Prosecutor's Office (EPPO). European Delegated Prosecutors (EDPs) will have different possibilities to request and receive data from service providers, even if the legal framework as regards issuing European Production Orders by EDPs presents some interpretative problems,[33] and the silence of the EPOR in this respect is not helpful.[34] In any case, national measures of criminal procedure may certainly be used to acquire electronic evidence and there will be a possibility to issue orders to non-participating Member States (including Ireland).

It is therefore necessary to provide a general and thorough reflection on access to electronic evidence from ISPs in administrative punitive proceedings and on the transfer of this type of evidence in administrative and criminal proceedings (in both directions), in order to more specifically justify the possibility for OLAF to extend its powers to be able to request such evidence. It is necessary to examine whether OLAF should have the power to request the ISPs to produce data and, if so, to what extent (which data, in which circumstances, etc). Despite entering into the remit of EPPO, OLAF remains crucial for protecting the EU's financial interests in several contexts: internal investigations,[35] countries that do not participate in the EPPO,[36] investigations involving third countries, [37] cases in which the EPPO decided not to open investigation,[38] and where OLAF's support has been requested.[39] In order to better protect the EU budget, OLAF needs to permanently increase the efficiency of its investigations. The newly acquired power to request bank statements is a good example of how it is venturing into waters traditionally associated with criminal investigations. Information held by ISPs is surely of great interest in OLAF investigations, for example enabling OLAF to identify perpetrators/accomplices in fraud and/or corruption investigations, which are typically characterised by hidden arrangements, or to demonstrate the organised nature of criminal groups targeting the EU budget (e.g., the same organisations are behind different email addresses used in custom fraud). At the same time, the gathering of data has to be done in ways that ensure protection of the right to privacy and safeguard the right to data protection.

Furthermore, and given OLAF's role, it is necessary to establish the conditions under which evidence gathered in this way can be transferred to a criminal investigation (e.g., to the EPPO) or how it can be transferred from a criminal investigation to an administrative one. Transfer of evidence from OLAF to criminal investigations is currently governed by Art. 11(2) of the OLAF Regulation, according to which OLAF's final reports, together with all supporting evidence annexed to them, shall constitute admissible evidence in administrative or judicial proceedings of a criminal or non-criminal nature, before national courts or before the CJEU, according to the type of irregularity or fraud identified.[40]

OLAF must strive to make its investigations consistently more efficient and effective,[41] adapting to operating in a challenging, fast-paced environment. The nature of irregularities and fraud has changed significantly in recent years and keeps shifting in keeping with an exceedingly more digitised world. The trans-border dimension of fraud as well as rapid technical advances in the European Union and worldwide demand a response at the EU level.

The Internet of Things is ever accelerating and permeates all aspects of life, including the life of perpetrators of fraud and irregularities. Too often, irregularities and fraud are hidden behind perfect paperwork. Artificial

circumstances created to gain EU funding by collusion and under-evaluation or other wrongdoing[42] can only be detected and revealed through information held by ISPs. Cases that rely on the availability of social media evidence[43] are just one example, as fraudsters seem to increasingly (ab)use the deep or dark web for illicit financial transactions in cryptocurrencies. Ongoing studies on how blockchain technology can be used to procure EU funding and for public procurement only accentuate the need to cover this ground.[44] As a European centre for knowledge, intelligence, and competence in anti-fraud matters at the EU level, OLAF should be able to (and certainly cannot afford not to) address this development, also in its investigative activities.

One of the questions that remains to be answered is how to design OLAF's competence to request electronic evidence from ISPs. Should it be a system analogous to OLAF's access to bank accounts?[45] Another question is to what extent access to information by ISPs complies with,[46] or should be accompanied by, supplementary judicial control? Within OLAF's administrative investigative remit, such power could be equated with that of national investigators and, relying on conditions of national law, could possibly include assistance by national anti-fraud coordination services[47] and/or judicial review.

In cases in which OLAF assists a criminal investigation by the EPPO,[48] the Office would act, within its mandate, under the direction of the handling EDP. The latter would then be responsible for assessing the legality and regularity of his/her own request under EU and national law.

Access to data by OLAF should also respect principles of proportionality, necessity, and data protection. All OLAF's investigations need to be conducted objectively and impartially, in accordance with the principle of the presumption of innocence, and with respect to procedural guarantees.[49] The current legal framework, including internal guidelines, already provides a structure by which to control compliance with procedural guarantees and data protection rules. A request for access to information held by ISPs would arguably warrant at least the following:

- Assessment of the necessity and proportionality of the request;
- Authorisation by OLAF's Director-General, possibly after internal review;
- An independent monitoring and complaints mechanism which is handled by the Controller of Procedural Guarantees[50] and OLAF's Supervisory Committee.[51]

V. Need for Further Research

Although access to electronic evidence for the purpose of criminal investigation has been subject to extensive research efforts,[52] there has been no systematic research to date in the field of administrative investigations as to the legal possibilities for requesting electronic evidence from ISPs. There is no knowledge about the practice itself, in particular as regards the use of a general legal basis or voluntary cooperation. These matters are the subject of the recently started project "Gathering electronic evidence for administrative investigations – comparative study of law and practice" (ELEVADMIN) hosted by the University of Luxembourg and financed by OLAF.[53]

Its objective is to examine the already existing legal framework at the national (in nine selected Member States) and EU levels and especially to understand the practice of gathering electronic evidence from ISPs for administrative investigations. The study will cover the gathering of electronic evidence in administrative punitive proceedings in the following areas:

- Protection of the EU's financial interests (PIF);

- Customs enforcement;
- Tax enforcement as regards VAT;
- Punitive enforcement in the area of banking and financial markets;
- Competition law enforcement.

The information gathered will be the subject of a comprehensive comparative analysis and in this way provide an extensive examination of the law and practice of gathering electronic evidence from ISPs in the context of punitive administrative enforcement. This analysis will also enable the formulation of policy goals for OLAF and for its potential extension of competencies.

VI. Conclusions

Despite the recent adoption of the E-evidence package, the electronic evidence question will remain a problematic issue in the years to come. Over the next three years, which are intended to have the necessary legislation for national rules to the EPOR adapted, numerous questions have to be answered, and the technical capacity for exchange of data must be provided.[54] The outcome of the negotiations with the USA on the agreement to allow unmediated cross-border exchange of electronic evidence between law enforcement and service providers will have a significant impact on how this evidence is gathered and will be crucial for the efficiency of the EPOR. Lastly, it remains to be seen how many countries will sign and ratify the Second Protocol to the Cybercrime Convention and what impact it will have on ensuing national legislation.

The increasing transfer of human activity to cyberspace, which will exacerbated even more by the entry into adult life of new generations of digital natives, will continue to put pressure on the rules of enforcement to adapt to this new reality. An area in which access to electronic evidence remains largely unaddressed is administrative punitive enforcement. In order to increase its efficiency and keep pace with technological developments, administrative investigations, such as the ones undertaken by OLAF, will have to be equipped with the possibility to acquire electronic evidence through cooperation with Internet service providers. A simple "transplant" of rules developed in the field of criminal investigation is not a viable possibility, given the nature and objectives of administrative law and the potential intrusiveness of gathering of personal data. Thus, a thorough reflection is needed on the needs and limits of gathering electronic evidence for administrative investigations. Such a reflection could be part of a broader discussion on the role of technology in enforcement and on challenges created by constant technological developments, including the gathering and examining of evidence by means of Internet of Things and Artificial Intelligence. OLAF and the EPPO should not lag behind in such developments, and the interaction between the two enforcement bodies in electronic evidence gathering will be of key importance in the field of the protection of the EU's financial interests.

---

1. D. J. B. Svantesson, *Solving the Internet Jurisdiction Puzzle*, 2017; J. Daskal, "The Un-Territoriality of Data", (2015) *The Yale Law Journal*, 326; S. Tosza, "All evidence is equal, but electronic evidence is more equal than any other. The relationship between the European Investigation Order and the European Production Order", (2020) *New Journal of European Criminal Law*, 161.↩
2. J. Daskal, "Unpacking the CLOUD Act", (2018) *eucrim*, 220.↩
3. O. S. Kerr and B. Schneier, "Encryption Workarounds", (2018) *Georgetown Law Journal*, 989.↩
4. See European Law Institute, "ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings", 2023, available at: <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf>. For this proposal, see the article by L. Bachmaier in this issue.↩
5. S. Tosza, "Cross-Border Gathering of Electronic Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies", in: D. Flore and V. Franssen (eds.), *Société numérique et droit penal*, 2019, p. 269.↩

6. 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, *O.J.* L 191, 28.7.2023, 118-180; 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, *O.J.* L 191, 28.7.2023, 181-190.↩
7. Directorate-General for Justice and Consumers, Statement of 2 March 2023, "EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations", <https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en>, accessed 2 November 2023.↩
8. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).↩
9. V. Mitsilegas, "The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence," (2018) *Maastricht Journal of European and Comparative Law,* 263; K. Ligeti and G. Robinson, "Transnational Enforcement of Production Orders for Electronic Evidence. Beyond Mutual Recognition?", in: R. Kert and A. Lehner (eds), *Vielfalt des Strafrechts im internationalen Kontext: Festschrift für Frank Höpfel zum 65. Geburtstag*, 2018, 625–644.↩
10. S. Tosza, (2020) *New Journal of European Criminal Law, op. cit.* (n. 1).↩
11. F. Fabbrini and E. Celeste and J. Quinn (eds.), *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty*, 2021.↩
12. J. Daskal, (2018) *eucrim, op. cit.* (n. 2), 220.↩
13. S. Tosza, "Internet service providers as law enforcers and adjudicators. A public role of private actors", (2021) *Computer Law & Security Review,* 1-17.↩
14. The future agreement with the USA will also most probably be limited to criminal investigations only, cf. U.S. Department of Justice, White Paper, April 2019, <https://www.justice.gov/opa/press-release/file/1153446/download> accessed 2 November 2023.↩
15. Art. 2 of the Second Additional Protocol to the Convention on Cybercrime.↩
16. B. Schneier, *Data and Goliath*, 2015, p. 26.↩
17. Art. 7 (3a) Regulation 883/2013 as amended by Regulation 2020/2223 (OLAF Regulation). For an overview of the 2020 reform of the OLAF Regulation see M. Bellacosa and M. De Bellis, "The protection of the EU financial interests between administrative and criminal tools: OLAF and EPPO", (2023) *Common Market Law Review*, 15-50.↩
18. See for instance R. Kert and A. Lehner, "Austria"; in: K. Ligeti, *Toward a Prosecutor for the European Union. Volume 1*, 2013, p. 29; J. Tricot, "France", in: K. Ligeti, *ibid*, p. 238 -240; T. Weigend, "Germany" in: K. Ligeti, *ibid*, 278-279; see also C. Larsson, "Telecom Companies as Crime Investigators", (2004) *Scandinavian studies in law*, 421–450; Council Resolution of 17 January 1995 on the lawful interception of telecommunications, *O.J.* C 329, 4.11.1996.↩
19. Permanent Court of International Justice on 7 September 1927 in the case of SS Lotus, Publications of the Permanent Court of International Justice, Series A.-No. 70, 18–19.↩
20. U. Sieber and C. Neubert, "Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty", (2017) 20th *Max Planck Yearbook of United Nations Law Online,* 239.↩
21. J. Daskal, (2018) *eucrim, op. cit.* (n. 2), 222.↩
22. K. Ligeti and G. Robinson, "Sword, Shield and Cloud: Toward a European System of Public–Private Orders for Electronic Evidence in Criminal Matters?" in: V. Mitsilegas and N. Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives*, 2021, p. 27; S. Tosza, (2020) *New Journal of European Criminal Law*, *op. cit.* (n. 1).↩
23. V. Franssen, "The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?", (2017) *European Data Protection Law Review*, 534, 538 ff.↩
24. See S. Tosza, "European Union, The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?", (2023) *European Data Protection Law Review*, 163.↩
25. C. Harlow and G. Cananea and P. Leino, "Introduction: European administrative law – a thematic approach" in: C. Harlow (ed.), *Research handbook on EU administrative law*, 2017, p. 2.↩
26. ECtHR, 8 June 1976, *Engel and Others v. The Netherlands*, Appl nos 5100/71; 5101/71; 5102/71; 5354/72; 5370/72.↩
27. Conseil Constitutionnel n° 2021-976/977 QPC du 25 février 2022.↩
28. Art. L. 621-10-2 Code monétaire et financier.↩
29. M. Luchtman and J. Vervaele (eds.), *Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with other EU law enforcement* authorities *(ECN/ESMA/ECB)*, 2017, available at <https://dspace.library.uu.nl/handle/1874/352061> accessed 2 November 2023.↩
30. For more details on this argument see: S. Tosza, (2021) *Computer Law & Security Review, op. cit.* (n. 13), 10.↩
31. CJEU, 15 September 2022, Case C-419/14 (*WebMindLicences*); see also F. Giuffrida and K. Ligeti (eds.), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, 2019.↩
32. See supra note 17.↩
33. A. Frunza-Nicolescu, "Electronic Evidence Collection in Cases of the European Public Prosecutor's Office", in this issue.↩
34. It is unclear how to interpret Art. 31 of the EPPO Regulation in this context; in particular, Art. 31(6) seems to be inapplicable as its first condition is in contradiction with the last condition of Art. 5(2) of EPOR.↩
35. Art. 4 OLAF Regulation.↩
36. See in this regard, A. Weyembergh and C. Brière, *The future cooperation between OLAF and the EPPO*, In-depth Analysis for the CONT Committee, 2017.↩
37. Art. 14 OLAF Regulation.↩
38. Art. 101(4) EPPO Regulation.↩
39. Art. 101(3) EPPO Regulation and Art. 12e OLAF Regulation.↩

40. M. Simonato, M. Luchtman and J. Vervaele (eds.), *Exchange of information with EU and national enforcement authorities: Improving OLAF legislative framework through a comparison with other EU authorities (ECN/ESMA/ECB)*, 2018, available at: <https://dspace.library.uu.nl/handle/1874/364049> accessed 2 November 2023.↩
41. See, e.g., ECA Special Report 01/2019 on fighting fraud.↩
42. See, e.g., OLAF Report 2021.↩
43. See e.g., P. Mathiessen et al. "Misuse of EU-funds: Messerschmidt's foundations investigated for fraud", *European Press Prize*, <https://www.europeanpressprize.com/article/misuse-eu-funds-messerschmidts-foundations-investigated-fraud/> accessed 2 November 2023.↩
44. See European Commission, News Article of 2 October 2021, "European Blockchain Pre-Commercial Procurement", <https://digital-strategy.ec.europa.eu/en/news/european-blockchain-pre-commercial-procurement> accessed 2 November 2023.↩
45. Art. 7 OLAF Regulation.↩
46. While the CJEU has consistently considered OLAF's investigative measures to be preparatory measures, because they do not bring about a distinct change in the legal position of the person concerned, and thus regarded them as non-reviewable under Art. 263 TFEU, the Court could be called on to indirectly review such acts in the context of an action against the final measure adopted by the Commission (See CJEU, 19 December 2012, C-314/11 P, *Planet v Commission*) or alternatively through a preliminary question of validity under Art. 267 TFEU, when and if a decision is adopted by a national authority (but it requires that national courts refer questions to the Court, and there seems to be no references so far, which would call into question the legality of OLAF's investigative acts). See K. Bovend'Eerdt, *The Protection of Fundamental Rights in OLAF Composite Enforcement Procedures*, 2024 (forthcoming); M. De Bellis, "Multi-level Administration, Inspections and Fundamental Rights: Is Judicial Protection Full and Effective?", (2021) *German Law Journal*, 416-440. See also J. Inghelram, "Judicial review of investigative acts of the European Anti-Fraud Office (OLAF): A search for a balance", (2012) *Common Market Law Review (CMLR)*, 601.↩
47. Art. 12a OLAF Regulation.↩
48. See Art. 101(3) EPPO Regulation.↩
49. Art. 9 OLAF Regulation.↩
50. See Art. 9a OLAF Regulation.↩
51. Art. 15 OLAF Regulation.↩
52. A significant body of knowledge was assembled in number of projects as regards the gathering of electronic evidence, including exploring national law in many EU and third countries, e.g., JUD-IT (Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU) conducted by the Centre for European Policy Studies (CEPS) (cf. S. Carrera and M. Stefan, *Access to Electronic Data for Criminal Investigations Purposes in the EU*, 2020, Centre for European Policy Studies (CEPS), <https://www.ceps.eu/wp-content/uploads/2020/02/LSE20120-01_JUD-IT_Electronic-Data-for-Criminal-Investigations-Purposes.pdf> accessed 2 November 2023); DEVICES project (Digital forensic Evidence: towards Common European Standards in antifraud administrative and criminal investigations) conducted by the University of Bologna (cf. M. Caianiello and A. Camon (eds.), *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, 2020.), and the project "Co-operation of service providers in criminal investigations" (ICTCOOP) conducted by the University of Liège. The results of this last project will be published in the Cambridge Handbook of Digital Evidence in Criminal Matters edited by V. Franssen and S. Tosza, 2024 (forthcoming).↩
53. Gathering electronic evidence for administrative investigations. Comparative study of law and practice (ELEVADMIN), financed by the Union Anti-fraud Programme (EUAF), Project: 101101776 — 2022-LU-ELEVADMIN. The author is the Coordinator and Principal Investigator of this project.↩
54. See, in detail, S. Tosza, (2023) *European Data Protection Law Review*, *op. cit.* (n. 24).↩

Author statement

The article was prepared within the framework of the project "Gathering electronic evidence for administrative investigations. Comparative study of law and practice (ELEVADMIN)", co-financed by the EU/Union Anti-Fraud Programme (EUAF), Project 101101776 — 2022-LU-ELEVADMIN. The views and opinions expressed are those of the author only and do not necessarily reflect those of the European Union or the European Commission.

ABOUT EUCRIM

eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.

Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.

All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.

The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union