1. SHEDDING LIGHT: ELECTRONIC EVIDENCE IN ADMINISTRATIVE INVESTIGATIONS

S. TOSZA, S. LANNIER and M. SICLARI

1. 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 be crucial as evidence in punitive proceedings. According to a study by the European Commission, around 85% of criminal investigations require electronic evidence to be obtained.[1] The peculiarity of electronic evidence – contrary to more traditional sources of evidence – lies in its potential to be obtained through a third party, most notably the service provider holding the data. This feature is unique. By way of illustration, although access to physical correspondence was, already in the past, possible as an investigation measure, traditional postal services did not retain access to the content of the communications they delivered, nor did they regularly gather metadata associated with those letters. To the contrary, email service providers normally do both. While the possibility to acquire data from telecommunication providers appeared earlier, in recent years it is the access to data from Online Service Providers (OSPs) that has become crucial for successful investigations.

Likewise, the rapid evolution of technology continues to reshape the behaviour and methods of perpetrators of fraud and irregularities affecting the EU budget. Too often, such irregularities hide behind perfect paper presentations. Artificial circumstances created to unlawfully obtain EU funding through practices such as collusion, under-valuation or other wrongdoing, can only be effectively detected and revealed through access to information held by OSPs. To name just few examples, investigations

[1] European Commission, *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*, Commission staff working document, SWD/2018/118 final, UE, 17/04/2018, p. 14.

increasingly rely on the availability of evidence sourced from social media platforms, while fraudsters seem to increasingly (ab)use the deep and dark web to facilitate illicit financial transactions, particularly involving cryptocurrencies. Ongoing studies into the application of blockchain technology in the context of EU funding and public procurement highlights the pressing need for legal framework to adapt to the evolving technological landscape.[2]

Although access to electronic evidence for the purpose of criminal investigation has been subject to extensive research efforts, there has been no systematic research to date in the field of administrative investigations as to the legal possibilities for requesting electronic evidence from OSPs. There has been 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 project 'Gathering electronic evidence for administrative investigations – comparative study of law and practice' – ELEVADMIN, co-financed by the Union Anti-fraud Programme (EUAF), of which this book is the outcome.[3]

2. ELECTRONIC EVIDENCE: FROM CRIMINAL TO PUNITIVE ADMINISTRATIVE PROCEEDINGS

2.1. Towards the E-evidence Regulation

Data that is in possession of OSPs may be a treasure trove for law enforcement authorities. However, accessing OSPs' data is hindered by the clash of the nature of cyberspace and the limitations of enforcement. While data flows unhindered – at least in certain countries – law enforcement is confined to the national borders as prescribed in the seminal Lotus judgment.[4] The principle of territoriality mandates, in its conventional reading, that if the data is stored outside of the country of investigation, then instruments of cross-border cooperation need to be used, which renders the access much more time-consuming, costly, and cumbersome. This duality – attractiveness

---

[2] European Commission, 'European Blockchain Pre-Commercial Procurement', 02/10/2021, online https://digital-strategy.ec.europa.eu/en/news/european-blockchain-pre-commercial-procurement.

[3] The preliminary reflection on the design of this research was published in Eucrim 2/2023: S. Tosza, 'Gathering Electronic Evidence for Administrative Investigations : Exploring an Under-the-Radar Area', *Eucrim*, 2023, no. 2, pp. 216-222, online https://eucrim.eu/articles/gathering-electronic-evidence-for-administrative-investigations/, DOI:10.30709/eucrim-2023-018. This chapter uses portions of that text.
The editors are very grateful for Flora Jung for her invaluable help in drafting the comparative chapter and finalising the formatting of all chapters.

[4] Permanent Court of International Justice, *SS Lotus*, 07.09.1927, Series A.-No. 70, pp. 18-19.

of electronic evidence gathered from third parties and inaptness of principles governing enforcement to cyberspace – characterises this field and has triggered a number of legislative and jurisprudential initiatives.

Over the past 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 protecting suspects' procedural safeguards. However, when the OSP was located in another country or the data was stored abroad, law enforcement was supposed to resort to instruments of cross-border cooperation, such as the European Investigation Order[5] (EIO) within the Area of Freedom, Security and Justice, and mutual legal assistance (MLA) outside this area, in particular as regards content data from US companies.[6]

The paperwork of mutual legal assistance (MLA) and the length of the procedure, necessary even in purely local simple cases, garnered frustration of law enforcement and led to the use of voluntary cooperation with OSPs and to a reinterpretation of the principle of territoriality. As to the latter, Belgium for instance decided to treat foreign providers actively targeting Belgian clients in the same way as if they were national providers.[7] In two famous cases concerning Yahoo and Skype these companies found themselves obliged to produce data according to a Belgian order, while the law of the place where they were headquartered (United States and Luxembourg respectively) forbade them to do so.[8]

Three major initiatives aimed to remedy this situation, although it is too early to assess their impact. The European Union (EU) has recently adopted a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (the E-evidence Regulation),[9] which aims at addressing the above-mentioned difficulties. 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

---

[5] Directive 2014/41/EU of the European Parliament and of the Council of 03.04.2014 regarding the European Investigation Order in criminal matters.

[6] J. Daskal, 'Unpacking the CLOUD Act', *Eucrim*, 2018, no. 4, pp. 220-225, online https://eucrim.eu/articles/unpacking-cloud-act/, DOI:10.30709/eucrim-2018-022.

[7] V. Franssen, 'The Belgian Internet Investigatory Powers Act - A Model to Pursue at European Level Reports: Practitioner's Corner', *European Data Protection Law Review*, 2017, vol. 3, no. 4, pp. 534-542.

[8] P.D. Hert, M. Kopcheva, 'International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case', *Computer Law & Security Review*, 2011, vol. 27, no. 3, pp. 291-297.

[9] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12.07.2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings.

the latter.[10] This Regulation is also linked with the potential agreement with the United States, which would broaden the possibilities of US OSPs to produce data to foreign law enforcement.[11] Finally, the recently adopted Second Protocol to the Cybercrime Convention[12] also provides for possibilities of directly requesting data cross-border, even if it would apply only to limited types of data.

2.2. The gap around administrative law enforcement

Notably absent from these debates and initiatives is administrative law enforcement.[13] Yet, electronic evidence is no less crucial for both national and European punitive administrative proceedings. While, due to fundamental rights concerns, the access to electronic evidence will arguably not be as broad as for criminal investigations, it will be increasingly more difficult to miss the golden opportunity that access to evidence through OSPs offers for effective investigations, including within the administrative domain. Even non-content data can provide valuable insights, which may prove essential to

[10] V. Franssen, S. Tosza (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Matters*, Cambridge, United Kingdom, Cambridge University Press, 2025; S. Tosza, 'Mutual recognition by private actors in criminal justice? E-evidence regulation and service providers as the new guardians of fundamental rights', *Common Market Law Review*, 2024, vol. 61, no. 1, DOI:10.54648/cola2024005; S. Tosza, 'European Union · The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?', *European Data Protection Law Review*, 2023, vol. 9, no. 2, pp. 163-172, DOI:10.21552/edpl/2023/2/11; S. Tosza, 'Internet service providers as law enforcers and adjudicators. A public role of private actors', *Computer Law & Security Review*, 2021, vol. 43, p. 105614, DOI:10.1016/j.clsr.2021.105614; 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', *New Journal of European Criminal Law*, 2020, vol. 11, no. 2, pp. 161-183, DOI:10.1177/2032284420919802; S. Tosza, 'Cross-border gathering of electronic evidence: mutual legal assistance, its shortcomings and remedies', *in*: V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 269; S. Tosza, 'The European Commission's Proposal on Cross-Border Access to E-Evidence : Overview and Critical Remarks', *Eucrim*, 2018, no. 4, pp. 212-219, online https://eucrim.eu/articles/european-commissions-proposal-cross-border-access-e-evidence/, DOI:10.30709/eucrim-2018-021.

[11] United States Department of Justice, 'Joint US-EU Statement on Electronic Evidence Sharing Negotiations', 26.09.2019, online https://www.justice.gov/archives/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.

[12] Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

[13] Tosza, (n. 3). See the exception of S. Mason, U. Rasmussen, *The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof. A comparative study and analysis*, CDCJ(2015)14 final, Strasbourg, European Committee on Legal Co-operation, Council of Europe, 2016.

substantiating evidence of misconduct.[14] So far, no comprehensive research has been done on the powers of administrative punitive authorities to gather electronic evidence from OSPs or about safeguards for affected persons on that context.

2.2.1. Gathering electronic evidence for administrative enforcement authorities

The possibilities of acquiring electronic evidence from third parties (in that case, OSPs) for evidentiary purposes are no less attractive or necessary in administrative proceedings than in criminal investigations. In this regard, we can already distinguish at least three different ways for administrative enforcement authorities to gather such evidence.

Firstly, there may be a concrete legal basis allowing them to make such requests. For instance, the Market Abuse Regulation[15] provides that under certain circumstances competent authorities shall have the power to request existing data traffic records held by a telecommunications operator.[16] However, in particular at the national level, such access may be controversial. For instance, the French legal framework regarding access to telecommunication data by administrative authorities evolved considerably during the last few years. Relying on the case law of the European Court of Justice (ECJ), the Constitutional Council struck down several laws that did not adequately address privacy and data protection considerations.[17] One interesting feature of the current legal framework is the creation of a new authority (*le contrôleur des demandes de données de connexion*) in charge of allowing these measures in some administrative sectors.[18]

Secondly, data may be potentially requested from OSPs by means of a more general legal basis of requests for information. For instance, at the EU level, the European Central Bank (ECB) may request data based on Article 10(1)(f) of the SSM Regulation no. 1024/2013.[19] Likewise, Directorate-General for Competition of the European Commission (DG COMP) may request information from third parties based on Article 18 of Regulation

---

[14] B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company, 2016.

[15] Regulation (EU) no. 596/2014 of the European Parliament and of the Council of 16.04.2014 on market abuse (Market Abuse Regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.

[16] Article 23 (2) (h) Market Abuse Regulation.

[17] Conseil Constitutionnel, 25.02.2022, no. 2021-976/977 QPC.

[18] Article L. 621-10-2 Code monétaire et financier.

[19] Council Regulation (EU) no. 1024/2013 of 15.10.2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions.

1/2003,[20] which does not preclude using it to request information from OSPs. Similarly, competent national authorities may proceed in a comparable manner, relying on general legal bases within their domestic legal framework.

Thirdly, administrative enforcement authorities may simply request data from service providers on a voluntary basis. Such a practice has emerged particularly in the context of criminal investigations, as a pragmatic response to the shortcomings of coercive mechanisms for obtaining such data, as outlined above. It relies on the general willingness of OSPs to cooperate with law enforcement and allows the authorities to avoid the problem of territoriality and the necessity to use cooperation instruments. At the same time, these requests are not binding for OSPs. Furthermore, OSPs may tend to check fundamental rights compliance of requests, which creates distorted dynamics between public and private authorities, with potentially detrimental results for persons concerned or interests of investigations at stake.[21]

A very particular case in that context is offered by OLAF: a body, with an objective to conduct investigations of misconduct, the results of which should transform into national criminal proceedings. The relevance of electronic evidence for those investigations is no less evident than for criminal proceedings. Yet, OLAF at this point does not seem to have the power to directly request such data from OSPs, which might be essential for detection or investigation of irregularities affecting the Union budget.

2.2.2. Regulating investigations in a world of interconnected law enforcement authorities

The need for electronic evidence arises in the punitive landscape in which the boundary between administrative and criminal enforcement within both national and European legal systems has become progressively blurred, especially in complex areas such as taxation and financial compliance. This raises important questions regarding the legal safeguards applicable to investigative powers, particularly in light of existing data protection standards.[22] As administrative authorities increasingly engage in fact-finding activities that mirror criminal investigations in both scope and intrusiveness, ensuring the appropriate calibration of procedural guarantees has become a critical issue for the legitimacy and accountability of hybrid enforcement regimes.

---

[20] Council Regulation (EC) no. 1/2003 of 16.12.2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.

[21] Tosza, 'Internet service providers as law enforcers and adjudicators', (n. 10).

[22] K. Ligeti, S. Tosza, 'Challenges and Trends in Enforcing Economic and Financial Crime: Criminal Law and Alternatives in Europe and the US', *in*: K. Ligeti, S. Tosza (eds.), *White collar crime: a comparative perspective*, Oxford, Hart publishing, Hart studies in European criminal law vol. 7, 2019, pp. 1-34.

In the contemporary legal landscape, where national and supranational law enforcement authorities increasingly operate in a coordinated manner, the regulation of investigative procedures must adapt to a reality characterised by legal hybridity and institutional interdependence. Irregularities may fall within the realm of either administrative or criminal law, and thus the choice of investigative framework may reveal strategic.

Administrative proceedings are generally perceived as more flexible, with fewer procedural constraints and lower thresholds for initiating inquiries. However, whenever new evidence emerges, such proceedings – initially framed as administrative – may be requalified as criminal, thereby triggering the application of enhanced procedural safeguards, in line with Article 6 of the European Convention on Human Rights (ECHR).

This fluidity between procedural frameworks is further illustrated by the transfer and mutual admissibility of evidence across domains, a phenomenon sometimes referred to as '*vases communicants'*.[23] For instance, electronic evidence gathered in an administrative context may be reused in a parallel or subsequent criminal proceeding, provided that the applicable legal framework allows such transfer. This interconnection is particularly visible in the operational relationship between OLAF and the EPPO. While OLAF conducts administrative investigations into fraud affecting the financial interests of the European Union, its findings – including electronic evidence – may be transmitted to the EPPO to support criminal prosecution. In turn, EPPO may rely on OLAF's investigative outputs to launch or complement criminal investigations under its competence. This institutional synergy, while promoting efficiency and coherence, also raises important questions regarding procedural guarantees, the scope of admissible evidence, and the potential risk of circumventing criminal procedural safeguards through administrative corridors.[24]

---

[23] S. Lannier, 'Obtention par l'ACD de données auprès d'opérateurs ou de fournisseurs de services de télécommunication. Une étude à la lumière du règlement sur les preuves électroniques en matière pénale', *Cahiers de fiscalité luxembourgeoise et européenne*, 2024, vol. 2024/2, pp. 23-50. This dynamic was thematised already in the seminal study on the penal provisions for the protection of European finances: M. Delmas-Marty, J. Vervaele (eds.), *The Implementation of the Corpus Juris in the Member States: Penal Provisions for the Protection of European Finances*, Antwerpen, Intersentia, 2000, vols. 1-4.

[24] S. Allegrezza, I. Rodopoulos, 'Interactions Between Administrative and Criminal Law in the Context of the Enforcement of Bank Prudential Regulations', *Oxford Business Law Blog*, 2016, online https://blogs.law.ox.ac.uk/business-law-blog/blog/2016/06/interactions-between-administrative-and-criminal-law-context.

2.3. Perspective from the Council of Europe and the European Court of Human Rights

Administrative authorities often impose sanctions that, while formally labelled as non-criminal, may produce punitive consequences comparable to those of criminal penalties. The European Court of Human Rights (ECtHR) has consistently held that where administrative penalties have a punitive and deterrent effect, they may fall within the scope of Article 6 of the ECHR, thereby triggering the application of criminal procedural guarantees.[25]

In its seminal judgment *Engel and Others v. The Netherland*[26], the ECtHR established a set of criteria – commonly referred to as the *Engel* criteria – for determining whether a given procedure, although formally administrative, should be regarded as 'criminal' in nature for the purpose of the Convention. These include: (1) the legal classification of the offence under domestic law, (2) the nature of the offence, and (3) the severity of the penalty. The Court has emphasised that the latter two carry greater weight in determining the autonomous meaning of 'criminal charge' under the Convention. In assessing this, the Court has taken into account a range of factors, including: the general applicability of the legal rule, whether the procedure is initiated by a public authority exercising statutory enforcement powers, whether the rule pursues a punitive or deterrent objective, whether the rule aims to protect general societal interests in a manner comparable to criminal law, whether the imposition of a sanction depends on a finding of guilt, and the classification of similar procedures in other member states of the Council of Europe.

This jurisprudence has had far-reaching implications, particularly in areas of hybrid enforcement where administrative proceedings may entail punitive elements, necessitating the application of criminal procedural safeguards to ensure compliance with the ECHR fair trial guarantees. In particular, Article 6 of the ECHR enshrines a number of defence rights and procedural guarantees that must be implemented in the face of criminal charges, including the presumption of innocence and the right to an independent and impartial tribunal established by law.

This jurisprudential framework is particularly relevant in the context of electronic evidence, where the intrusiveness of investigative measures may resemble those of criminal proceedings. As administrative authorities increasingly rely on data held by private actors, the ECtHR's case law

---

[25] D. Ohana, 'Regulatory Offenses and Administrative Sanctions: Between Criminal and Administrative Law', *in*: M.D. Dubber, T. Hörnle (eds.), *The Oxford Handbook of Criminal Law*, Oxford University Press, 2014.

[26] ECtHR, *Engel and Others v. the Netherlands*, 08.06.1976, nos. 48272/17, 57479/17, 510/18, 7936/18, 27115/18.

provides a crucial benchmark for assessing the legitimacy and proportionality of such practices, thereby anchoring the book's exploration of electronic evidence within a broader human rights paradigm.

3. METHODOLOGY OF THIS RESEARCH

In view of the above considerations and given the exponential increase of significance of electronic evidence, this research aimed at shedding the light on this under-the-radar problem, which is gathering electronic evidence in administrative investigations. This book presents the outcome of this research, which examined the existing legal framework and practice at the national and EU level, compared it critically and formulated recommendations as to the legal framework of gathering electronic evidence in that context. The research followed tailored-made methodology consisting of examining five legal areas at the EU level and across nine legal systems.

3.1. Selected areas of enforcement

The comparative analysis examined five areas of punitive enforcement, namely customs, Value Added Tax, competition law and General Data Protection Regulation (GDPR) enforcement, as well as punitive enforcement in the area of banking and financial markets. These areas were examined to establish legal possibilities to request electronic evidence from OSPs or to transfer such evidence from another proceeding (criminal or administrative). While PIF was the main targeted area for policy recommendations formulated in the last chapter of this book, the four other areas were chosen for comparison due to their thematic and policy proximity and interaction between criminal and administrative enforcement. At the same time each of them offers a different perspective and a different set of experience and challenges.

As to the domain of financial supervision, it was chosen since the Market Abuse Regulation already provides for a possibility to request records held by a telecommunications operator. While market abuse has a strong EU component, this is less prominent for enforcement in customs. Customs duties represent a traditional own source for the EU budget, with 75% of the customs duties collected by EU Member States going to the EU budget.[27] The revenue from customs duties is estimated to be about 10% of the total revenues of the EU budget.[28]

---

[27] Council Decision (EU, Euratom) 2020/2053 of 14.12.2020 on the system of own resources of the European Union and repealing Decision 2014/335/EU, Euratom.

[28] G. D'Angelo, *Aspects of customs control in selected EU Member States*, Bologna University Press, 2023.

As to competition law, the enforcement of EU competition law plays a crucial role in maintaining fair market conditions, preventing anti-competitive practices and safeguarding consumer interests. As markets become more integrated and globalised, the complexity of enforcing competition rules has increased, particularly with regard to cross-border mergers, cartels and other anti-competitive agreements, with a prominent role played by DG Competition at the EU level. Finally, as data processing and digitalisation continue to accelerate, ensuring compliance with GDPR has become increasingly complex. The regulation mandates strict controls on data collection, storage, and processing, with severe penalties for non-compliance. The enforcement of GDPR thus requires effective collaboration between national data protection authorities, particularly for cross-border data flows.

While all areas were given equal attention in the research, they shed light on OLAF's investigatory powers, resulting in policy recommendations as to the possibilities for OLAF to extend its powers to gather electronic evidence from OSPs and the parameters for such powers. Furthermore, the study explored to what extent access to information held by OSPs complies with or should be accompanied by supplementary judicial control. The research explored to what extent a system analogous to OLAF's access to bank accounts could be set-up. Within OLAF's administrative investigative remit, such power could be equated to those of national investigators, and rely under conditions of national law, possibly including assistance by the national anti-fraud coordination services and/or judicial review.

3.2. A comparative analysis

The analysis of those five areas was performed at EU and national level. At the national level, it has been conducted using a standard questionnaire[29] in the following Member States: Belgium, Finland, France, Germany, Italy, Ireland, Luxembourg, the Netherlands, and Poland. In parallel, a similar analysis into the EU law in the same domains was performed.

At the national level, authorities competent in these selected areas were examined, such as national competitions authorities (*Autorité de la concurrence* in France, UOKiK in Poland), financial supervision authorities (e.g., BAFIN in Germany, CSSF in Luxembourg), and custom and tax investigation authorities (e.g. FIOD: Fiscal Information and Investigation Service in the Netherlands or the General Administration of Customs and Excise in Belgium). Some of these authorities perform tasks in criminal and administrative enforcement. The consequences of that feature for gathering electronic evidence were also examined. Similar investigations were

[29] See Annex I at the end of this book.

undertaken at the EU level concerning powers of relevant authorities, such as DG COMP, the ECB or European Securities and Markets Authority (ESMA).

The information thus gathered was subject to a comprehensive comparative analysis. ELEVADMIN established to what extent punitive administrative authorities are granted powers by legislators to request data from OSPs, to which extent they use those powers, and to what extent they need to look for creative solutions to gather data they need for their enforcement activities. This investigation provides sufficient material to understand patterns and tendencies as well as needs of examined authorities. We also examined the findings from the perspective of the fundamental rights standard of protection of privacy.

3.3. A 'law in action' analysis

Another key objective of ELEVADMIN was to understand the practice of gathering electronic evidence from OSPs in the context of administrative investigations. To this end, the project adopted a law in action approach, which contrasts with the traditional 'law in the books' methodology. While the latter centres on formal legal provisions, a law in action methodology seeks to understand how legal norms are implemented in practice, with particular attention to enforcement practices, administrative behaviour, and the interaction between legal frameworks and technological realities.[30]

As a result, an integral and highly important part of that research was the examination of the practice of using the identified legal frameworks, as well as in general of gathering electronic evidence from OSPs. This required conducting interviews with representatives of the relevant authorities, stakeholders from the private sector and practitioners.

4. THE STRUCTURE OF THE BOOK

The structure of this book is designed to provide a comprehensive analysis of the legal possibilities of gathering electronic evidence from OSPs in administrative punitive proceedings, combining theoretical, practical and comparative perspectives. Chapter 2 provides an in-depth analysis of the European Union setting, exploring the current legal framework for gathering electronic evidence from third parties in punitive enforcement proceedings in the selected areas at the EU level, with a particular focus on proceedings conducted by DG COMP, the ECB and ESMA. The third chapter specifically addresses the protection of the financial interests of the EU, detailing existing provisions that enable OLAF to collect data from private actors not involved

[30] R. Pound, 'Law in Books and Law in Action', *American Law Review*, 1910, vol. 44, no. 1, pp. 12-36.

in the context of both its internal and external investigations, as well as the procedural guarantees and the available remedies in place to safeguard the rights of those involved. Chapters 4 through 11 offer country-specific examinations, analysing the legal frameworks and practices in 9 different Member States: Belgium (Chapter 4), Finland (Chapter 5), France (Chapter 6), Germany (Chapter 7), Ireland (Chapter 8), Italy (Chapter 9), Luxembourg (Chapter 10), the Netherlands (Chapter 11), and Poland (Chapter 12). Notably, each chapter presents an extensive examination of national provisions and practices for each punitive administrative enforcement area. A comprehensive comparative analysis is then provided in Chapter 13, which identifies similarities and differences in legal provisions governing administrative proceedings and investigative powers, particularly with regard to the possibility to gather electronic evidence from OSPs across different jurisdictions. The book concludes with Policy Recommendations (Chapter 14), which result from this research as regards both national and European administrative authorities, with a particular attention to OLAF. They focus on the possibilities of using current legal framework to gather electronic evidence in punitive administrative proceedings and examine the question of extending those powers.