Renata Marcinauskaitė

Electronic Evidence in Criminal Proceedings

General Remarks

The problems of proof-taking activities and proof in criminal proceedings are complex. To address these issues, it is important to identify the various aspects of the proof-taking process, define what constitutes evidence in criminal proceedings, and outline their requirements. This analysis should be seen as a starting point for unravelling the concept of electronic evidence and its peculiarities, as well as aspects of its evaluation and requirements for substantiating its reliability.

The emergence of electronic evidence in criminal proceedings is linked to the commission of cybercrime. Cyberspace is defined as "the indefinite place where individuals transact and communicate" (Britz 2009, p.3). As cyberspace activities have expanded, some activities that are considered as traditional criminal offenses (e.g., fraud, forgery of documents) have moved to cyberspace alongside the introduction of cyberspace-specific offenses (e.g., unauthorized access to an information system, unauthorized modification of electronic data). Investigating and proving these offenses is complicated by the specificity of cyberspace: "the intangible nature of computer interaction and subsequent criminality poses significant questions for investigative agents" (Britz 2009, p.6). It is also relevant that in cybercrime cases, usually "eyewitness statements and other traditional types of evidence are not available or scarce because of the digital nature of the offences" (Riekkinen 2019, p.6).

The chosen directions of analysis also underline the need for a coherent approach to this type of evidence in criminal proceedings. The legal framework should not give priority to evidence based on its form, i.e., whether it is tangible (physical) or intangible (without physical parameters). The consistency of such practice would also meet the requirements of the principle of technological neutrality. It should also be mentioned that the proper process of obtaining and managing electronic evidence is crucial for the quality of proof-taking activities and can contribute to the cost-effectiveness and speed of criminal proceedings.

The need for a coherent approach to electronic evidence is becoming an issue not only at the national but also at the international (European Union) level. This aspect is underlined by the specific cross-border nature of cybercrime. Successful cybercrime investigations often depend on cooperation between jurisdictions to facilitate access to electronic evidence while ensuring high

standards of human rights protection. Obtaining access to electronic evidence in another country is complicated and burdensome for judicial authorities because of the lengthy and complex procedures that need to be followed. Legal instruments have been adopted at both the European Union and international level to address these issues. Directive (EU) 2023/1544 of the European Parliament and of the Council of July 12, 2023 laying down harmonized rules on the designation of establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (hereafter – Directive 2023/1544) and Regulation (EU) 2023/1543 of the European Parliament and of the Council of July 12, 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 (hereafter – Regulation 2023/1543) have been adopted to ensure that authorities have easier and faster access to electronic evidence. At the international level, the Council of Europe Convention on Cybercrime (hereafter – Convention on Cybercrime, 2001) and its Additional Protocols, in particular the Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (hereafter – Second Additional Protocol, 2022), should also be mentioned.

The Concept of Proof-Taking Activity and the Assessment of Evidence in Criminal Proceedings

Establishing the existence (or otherwise) of a criminal offense and other circumstances relevant to the fair disposition of a criminal case is inseparable from the proof-taking process in criminal proceedings. Proof-taking activity is the activity of the relevant entities specified in the law (suspect, defense counsel, prosecutor, court, etc.) which continues throughout all criminal proceedings and is related to obtaining, presenting, verifying, and assessing data important to the investigation of the criminal offense committed (Goda *et al.* 2005, p.171). The purpose of proof-taking activities is to clarify the circumstances relevant to the criminal case and, ultimately, to establish the truth in the criminal case. In this respect, it should be noted that "collection, verification and evaluation of evidence is a whole unit of cognitive activity, but with different intermediate tasks" (Ablamskyi and Vasko 2022, p.14).

One of the provisions of the right to a fair trial, that "everyone charged with a criminal offense shall be presumed innocent until proved guilty according to law" (European Convention for the Protection of Human Rights and Fundamental Freedoms 1950, Article 6(2)), is often reflected in the constitutional provisions

of states and in legislation on criminal proceedings. Recognizing that the presumption of innocence is regarded as a guarantee to protect "accused persons from wrongful conviction" (Tadros and Tierney 2004, p.402), the Constitution of the Republic of Lithuania, for example, states that "a person shall be presumed innocent until proved guilty according to the procedure established by law and declared guilty by an effective court judgment" (Article 31(1)). These provisions have also influenced the understanding of the purpose of criminal proceedings. For example, Article 1(1) of the Criminal Procedure Code of the Republic of Lithuania states that the aim of criminal proceedings is, among other objectives, to ensure the full disclosure of a criminal offense and the proper application of the law "in order to ensure that any person who has committed a criminal act is given a fair punishment and that no one who is innocent is convicted" (Criminal Procedure Code of the Republic of Lithuania 2002, Article 1(1)). Accordingly, the discovery of the offense committed, fair punishment, and thus the determination of the truth in a criminal case is directly related to various issues of proof-taking actions and evidence.

The adoption of an evidence-based final judgment depends, *inter alia*, on the quality of the proof-taking process and the quality of obtaining, presenting, verifying, and evaluating data relevant to the investigation of the criminal offense committed. The proof-taking activity and its quality is not confined to a single stage of the criminal proceedings (e.g., trial), but is continuous, starting with the initial recording of certain data and ending with their use in the final judicial decision. For example, the case-law of the European Court of Human Rights notes that "the investigation stage may be of particular importance for the preparation of the criminal proceedings: the evidence obtained during this stage often determines the framework in which the offence charged will be considered at the trial […]" (*Ibrahim and Others v. United Kingdom* 2016). Thus, fair trial guarantees apply to the entire criminal proceedings process, both at the pre-trial and trial stages (*Vera Fernandez-Huidobro v. Spain* 2010), and breaches of these guarantees can significantly undermine the fairness of a trial.

An important part of the proof-taking process is the examination of the evidence during the trial, its admission as evidence, and its assessment in order to arrive at a lawful and reasoned final judgment. It should be noted that, according to the case law of the European Court of Human Rights (hereinafter – ECtHR), "as a general rule, it is for the national courts to assess the evidence before them, while it is for the Court to ascertain that the proceedings considered as a whole were fair, which in case of criminal proceedings includes the observance of the presumption of innocence" (*Telfner v. Austria* 2001). According to the above-mentioned ECtHR case law, the principle of the presumption of innocence

requires, *inter alia*, that "when carrying out their duties, the members of a court should not start with the preconceived idea that the accused has committed the offense charged; the burden of proof is on the prosecution, and any doubt should benefit the accused" (*Telfner v. Austria* 2001). Thus, regardless of the type of evidence, it is the prerogative of the court that renders the final judgment to assess it and draw conclusions in a criminal case. It is for the court to decide which evidence contained in the case has probative value and whether it is sufficient to establish that a person's conduct constitutes all the elements of a particular criminal offense.

It is also mentioned that evidence must be evaluated in accordance with the law. This requirement means that the court's conclusions cannot be based on data that do not meet the legal requirements. An infringement should also be established in cases where data that met the legal requirements were not admitted as evidence.

Thus, when deciding whether to accept data as evidence, the court must determine whether the data are relevant to the case, whether they were obtained in accordance with the procedure laid down by the law and were gathered by lawful means, as well as whether the reliability of the data has been verified by lawful actions of the criminal procedure.

Although the assessment of evidence is a matter for the national court, it must be consistent with, *inter alia*, the requirements of fair proceedings. The establishment and practical implementation of the latter requirements ensure coherence between international obligations and national legal regulation. Such compatibility is also a guarantee of the rights of the persons involved in criminal proceedings, including in the proof-taking process. Since one of the objectives of the proof-taking process is the establishment of facts relevant to a criminal case, the issue of evidence and its requirements become crucial. In this respect, there is also a need for a coherent approach to the evaluation of electronic evidence, especially since "evidence records vary in forms and types" (Raghavan and Raghavan 2009, p.1).

The Concept of Evidence: The Identification of Electronic Evidence

The proof-taking process, as discussed earlier, is directly concerned with obtaining, presenting, verifying, and assessing data to be admitted as evidence in criminal proceedings. The emergence of evidence in criminal proceedings and its ability to substantiate (or refute) facts relevant to the fair disposition of a criminal case is linked to the laws of cognitive theory (gnoseology). The latter laws reveal

an object's defining feature: when objects interact, they can reflect the traces of the criminal offense committed. Precisely because of their interaction, the traces of all criminal acts remain as a reflection, which allows the event that occurred in the past to be identified. Accordingly, irrespective of the type of trace – material or ideal (formed in the human memory) – it must be obtained, presented, verified, and assessed by the subjects of the proof-taking process. These traces, objectively visualized, are presented in the criminal case and are verified and evaluated in the criminal proceedings in accordance with the requirements established by the law. Taking these aspects into account, both the scientific and the legal concept of evidence is formulated. From this perspective, it should also be mentioned that, in line with the dual concept of evidence, two non-identical categories are used in criminal proceedings: "data relevant to the investigation and examination of a criminal offence" and "evidence" (Juozapavičius and Leonaitė 2021, p.86). This distinction is linked to the requirements of the adversarial principle, where data become evidence only after they have been examined in the court. Hereinafter, these terms will be used interchangeably depending on the context.

According to the scientific concept of evidence, evidence is "data obtained in accordance with the law, which confirm or deny at least one circumstance that is relevant to the fair disposition of a case" (Matulienė, n.d.). The legal concept of evidence is established or derived from a systematic analysis of statutory provisions. It is the latter concept that is also used, for example, in Lithuanian case law, which states that evidence in criminal proceedings is data obtained, verified, assessed at trial and accepted by the court in accordance with the procedure established by law, on the basis of which the court draws conclusions as to the existence (or absence) of a criminal offense, the guilt (or innocence) of the person who has committed the offense and other circumstances relevant to the fair disposition of the case (Ruling of the Supreme Court of Lithuania of July 14, 2020 in criminal case No. 2K-141-303/2020). According to the legal concept of evidence, the main features of evidence are usually revealed by analyzing the specific norms establishing the requirements for data collection, presentation, verification, its admission as evidence and the assessment of evidence in criminal proceedings.

There are different classifications of evidence that complement each other. For example, evidence is divided: into personal evidence (where the information is preserved in people's minds and transmitted orally or in writing) and physical evidence (where the information is reflected and transmitted through material objects); according to the primacy of the source of the information – i.e., primary and derivative evidence; according to the relationship to the circumstances to be proved – i.e., direct and indirect evidence; and according to the relationship

of the evidence to the version of the accusation – i.e., incriminating and justifying evidence (Matulienė, n.d.). The following categories of evidence do not directly mention electronic evidence. On the other hand, as far as the concept of the proof-taking process or the general concept of evidence is concerned, the exclusion of electronic evidence is not necessary, as these concepts do not change regarding the possible form of evidence (whether it is evidence with physical parameters or without such parameters – i.e., electronic evidence). However, it should be noted that the exclusion of electronic evidence is relevant in the context of justifying its admissibility in criminal proceedings, as well as in deciding on the requirements for its collection, presentation, verification, and assessment, and, accordingly, on how to ensure that it complies with the requirements of the law. The analysis of electronic evidence also provides for a better understanding of such kinds of evidence. After all, "in a digital investigation, investigators deal with acquiring digital data for examination" (Raghavan and Raghavan 2009, p.1).

As an example, Western European Codes of Criminal Procedure do not usually differentiate between physical and electronic data which may later be admitted as evidence in criminal proceedings. However, the presence of electronic evidence in the proceedings is determined by the development of technology and the possibilities it offers, as well as by the nature of the criminal offense. In this context, the view that "criminal law must respond adequately and enable the use of evidence obtained by new technologies such as satellites, GPS, GLONASS, dashcams, vehicle software, communication technologies, location, etc." is supported (Vasko and Klimek 2023, p.176). At this point, it should also be mentioned that a rather generalized approach which does not exclude electronic evidence into a separate type is also followed in foreign countries. For example, as stated in the scientific literature, there is no specific exception for computer-generated evidence in the USA; the Federal Rules of Evidence apply the same rules to electronic records as they apply to ordinary documents (Sethia 2016, p.235). On the other hand, the absence of an official concept of electronic evidence in national legislation may lead to difficulties in defining this type of evidence and identifying its characteristics.

The scientific literature defines electronic evidence as "evidence derived from data contained in or produced by any device the functioning of which depends on a software program or from data stored on or communicated over a computer system or network" (Mason, 2016, p.22). Electronic evidence can also be defined as "data (comprising the output of analogue devices or data in digital format) that is manipulated, stored, or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less

probable than it would have been without the evidence" (Trigkas 2017, p.21). Accordingly, evidence may be considered e-evidence if it is stored (or transmitted) in a communication system and (or) if it was created by that system. As electronic evidence usually retains an electronic form, it is suitable for processing in an information system. Such data may be stored in the system or transmitted using communication technology. Although the concept of electronic evidence is quite clear, it is worth noting a few aspects relevant to its use in the proof-taking process:

1) The need for the collection of electronic data to prove (or disprove) at least one circumstance relevant to the fair disposition of the case should not be limited solely to the commission of criminal offenses against the security of electronic data and information systems (as understood in Chapter II, Section 1(1) of the Convention on Cybercrime). The latter offenses constitute the definition of cybercrime in the narrowest sense. It is relevant that the appearance of electronic data admissible as evidence in criminal proceedings is possible in all cases where the commission of criminal offense involves the use of information technology. In this context, various electronic evidence issues can also be addressed in cases where the use of information technology has changed the traditional criminal offense. The latter offenses fall within the category of cybercrime as defined in its broadest sense. Some of these variations are referred to, for example, in Chapter II, Section 1, Title 2 to 4 of the Convention on Cybercrime: Computer-related forgery, Computer-related fraud, Offenses related to child pornography, Offenses related to infringements of copyright and related rights. Offenses of this nature are also included in the Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) and covering offenses of racist or xenophobic propaganda. It should be noted that the list of traditional offenses modified using information technology should not be considered exhaustive: "in fact, digital evidence has been utilized in cases ranging from homicide to software piracy" (Britz 2009, p.267).
2) It is proposed that the concept of electronic evidence in criminal proceedings should be as broad as possible; therefore, the terms used in the concept of electronic evidence that refer to technology (e.g., information system) should be interpreted in accordance with the requirements of the principle of technological neutrality. This principle is usually invoked to deal with the evolution of information and communication technologies and, in the most general sense, refers to the prohibition of prioritizing one technology

over another if such differentiation is not necessary (Ohm 2010). Thus "[…] legislation must be generic enough to encompass advances in technology, assuring that application to tomorrow's technology is possible" (Britz 2009, p.350). It has been stated that evidence can be considered electronic if it is stored in (or transmitted by) an information system, or it has been created by that system. Accordingly, the interpretation of what constitutes an information system should focus on its functions, i.e., the processing of data, rather than on the specific technologies that perform these functions. For example, the Convention on Cybercrime provides a technology-neutral definition of a computer system: "computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data" (Chapter I Article 1(a)). It is also relevant that the reference to the information system should not only include information technology, but also communication technologies that allow the transmission of information between various devices.

3) Expertise is important for the investigation of some types of electronic evidence. In such cases, the expert must carry out the expert examination in accordance with their competence, using scientifically validated, generally accepted and reliable or accredited methods of examination. On the other hand, an expert's report is only one piece of evidence which the court must assess after a complete and impartial examination of all the circumstances of the case. The evaluation of an expert's report as evidence is subject to the requirements laid down by law. It is therefore for the court to decide in each case whether the data (including electronic data) obtained constitute evidence.

Examples of electronic evidence may include text, video, audio, photographs, network traffic captures, Random Access Memory (RAM) data, event logs, mobile device artefacts, metadata, hash values, encrypted data, malware, and many others. This data can be processed by information systems with different functions (computers, mobile phones, servers, GPS devices, cloud technologies, etc.). One example is metadata, which is defined as "structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource" (National Information Standards Organization 2004, p.1). Metadata is commonly defined as "data about data" (Butterfield 2001, p.24). Metadata can reveal, for example, the origin of electronic data, relevant dates and times (creation, modification, transmission, etc.), and details of the device that generated the electronic data, and can provide the necessary context for evaluating other electronic evidence. As

metadata is an integral part of electronic evidence, it is necessary to bear in mind its evidentiary value.

In the context of the analysis of electronic evidence, attention should be drawn to the need for coherence in the national legal frameworks relating to the admissibility of evidence in criminal proceedings. Firstly, the established legal framework should not reject or give priority to evidence depending on its form, whether physical or electronic. This objective can be achieved through a technology-neutral approach. According to it, electronic data, irrespective of the technology that created or processed them, should be admissible as evidence in criminal proceedings if they fulfil the purpose of evidence, its function in criminal proceedings and other requirements applicable to evidence. Secondly, it is relevant that in criminal proceedings it should be possible to present electronic evidence in its original electronic form. This would also help to ensure the economy and speed of criminal proceedings. Thirdly, the need for regulatory coherence is also linked to the transnational aspect of cybercrime. This aspect means that "evidence of […] criminal offence is increasingly stored in electronic form on computer systems in foreign, multiple or unknown jurisdictions" (Second Additional Protocol 2022, Preamble). Accordingly, an effective criminal justice response will determine whether the States that have signed up to cooperation commitments have a coherent, harmonized approach to the collection, presentation, verification, and assessment of electronic data crucial to the fair disposition of a criminal case. The latter aspect is particularly evident in the ratification of the 2001 Convention on Cybercrime, the provisions of which also address the current issues of obtaining electronic evidence in relation to the Expedited preservation of stored computer data (Section 2 Title 2), Production order (Section 2 Title 3), the Search and seizure of stored computer data (Section 2 Title 4), and the Real-time collection of computer data (Section 2 Title 5). To achieve more effective cooperation across jurisdictional boundaries, the Second Additional Protocol was adopted in 2022. This Protocol sets out various Procedures enhancing direct co-operation with providers and entities (Section 2), Procedures enhancing international co-operation between authorities for the disclosure of stored computer data (Section 3), Procedures pertaining to emergency mutual assistance (Section 4), Procedures pertaining to international co-operation in the absence of applicable international agreements (Section 5), as well as personal data protection safeguards (Chapter III Article 14). A coherent approach at the European Union level is also important in the application of Regulation 2023/1543 related to European production and preservation orders for electronic evidence in criminal matters, and in the implementation of the provisions of Directive 2023/1544 on the appointment of legal representatives

for the purposes of gathering evidence in criminal proceedings. In addition, these provisions, *inter alia*, can be seen as steps toward the harmonization of national approaches to electronic evidence.

The Requirements Applicable to Evidence

Evidence in criminal proceedings is data obtained in accordance with the law which confirm or disprove at least one circumstance that is relevant for the fair disposition of the case. Thus, data shall be considered as evidence if they meet certain requirements: 1) they prove (or disprove) at least one circumstance relevant for the fair disposition of the case; and 2) they are obtained by lawful means and may be verified by the procedural actions laid down in law. Irrespective of the form in which the data are produced (electronic or physical), they may be admitted as evidence if the prerequisites for such admission are met: the data fulfil the requirements of correlation, admissibility, and reliability.

One of the requirements for the admission of data as evidence – their correlation – is understood as a link to a fact to be proved in a criminal case. In this context, only data from which the court determines the factual circumstances of the act under investigation and other circumstances may be considered evidence. In all criminal cases, the circumstances of the act under investigation must be proven: the time, place, manner, tools and means, the type and scope of damage caused, the person who committed the act, their personal characteristics, the victim etc. It is not necessary that these circumstances be proven by direct evidence alone; they may also be substantiated by indirect evidence. According to this approach, both electronic data which are directly relevant to the matter of proof and electronic data that initially substantiate the existence of an intermediate fact – and, through that fact, the circumstances to be proved – are relevant. In such cases, it is essential that all evidence, both electronic and physical, is obtained and evaluated in accordance with the requirements laid down by law.

Another requirement for the acceptance of data as evidence is their admissibility. This means that only data obtained by lawful means and verified by actions provided by law can constitute evidence. Consequently, in deciding whether to accept the examined data as evidence, the court must verify that the way in which they were obtained does not contravene the requirements of the law and that they have been verified by actions prescribed by law. Where violations in the data obtaining procedure raise doubts and these doubts cannot be eliminated, such data shall not be admitted as evidence. Conversely, if the violations of the data collecting procedure did not affect the reliability of the data obtained, and the collection of the data did not deprive (or substantially restrict) the accused's

rights guaranteed by the law, the data are usually admitted as evidence (Ruling of the Supreme Court of Lithuania of July 17, 2020 in criminal case No. 2K-164-458/2020). The requirement to comply with the law in the process of obtaining evidence is particularly important, otherwise the fairness of the criminal proceedings would not be guaranteed (Ruling of the Supreme Court of Lithuania of April 9, 2020 in criminal case No. 2K-81-895/2020). In this respect, it is also relevant that "EU and international legislation does not provide any rules for deciding the admissibility of evidence, nor has the ECtHR formulated any such rules" (Juozapavičius and Leonaitė 2021, p.81).

The final act of a court can only be based on reliable evidence. Reliability of evidence is a characteristic established by the assessment of the evidence, which means that the data relevant for the fair disposition of a criminal case correspond to the truth. The reliability of evidence shall be determined by an analysis of the way in which it was obtained, its verification by the procedures laid down by law, and its comparison with other evidence in the criminal case (Ruling of the Supreme Court of Lithuania of January 30, 2018 in criminal case No. 2K-26-689/2018). The evidence itself is assessed by the court through legal procedures, as well as by comparing evidence from different sources. For example, a conclusion on the reliability of the testimony of persons (defendants, victims, witnesses) may be reached by assessing the consistency, detail, completeness, and logic of the testimony, and by comparing it with the other evidence in the case obtained from different sources (Ruling of the Supreme Court of Lithuania of November 12, 2019 in criminal case No. 2K-264-976/2019).

The requirements discussed above are important for the analysis of the various types and forms of evidence that are relevant for the fair resolution of a case, and compliance with these requirements is fundamental to ensuring justice in criminal proceedings. On the other hand, given the specific nature of electronic evidence, there are other aspects which detail – and, at the same time, justify – the reliability of this type of evidence in criminal proceedings. The identification and proper assessment of these characteristics is relevant in order to substantiate the reliability of electronic data, and at the same time to ensure that they are truthful and properly establish the facts crucial for the fair resolution of a criminal case.

The Specifics of Electronic Evidence: The Justification of the Reliability of Electronic Evidence

As more and more criminal offenses move from the physical world to cyberspace, "more and more investigations become dependent on digital evidence"

(Grigaliūnas and Toldinas 2016, p.30). On the other hand, in the process of obtaining, presenting, verifying, and evaluating electronic data it is important that such data, compared to other types, are relatively easy to alter, both because of deliberate (or negligent) human activity and the peculiarities of the functioning of information systems themselves. As noted in the scientific literature, "digital evidence is especially volatile and voluminous, susceptible to climatic or environmental factors as well as human errors. It may be vulnerable to power surges, electromagnetic fields, or extreme temperatures" (Britz 2009, p.297). It is also important to note that the alteration of electronic data may be difficult to trace and establish in certain cases. Therefore, it should come as no surprise that "the application of traditional evidentiary rules to modern electronic content may warrant a higher degree of scrutiny in the wake of concerns regarding the trustworthiness of e-evidence" (Trigkas 2017, p.21).

Electronic data may be altered, corrupted, or destroyed if they are improperly obtained, processed, or examined. In criminal proceedings, these cases would mean that the data obtained have lost their reliability and can no longer be the basis for a final judicial decision as they no longer reflect true facts. Such electronic data shall not be admissible as evidence in criminal proceedings. In this respect, it should also be noted that "the more vulnerable computer and network-derived evidence is to exclusion, the more problematic will be the prosecution of […] cybercrimes" (Walden 2007, p.367).

The reliability of electronic data is linked to the reliability of both the electronic data itself and the process by which the data were obtained. The requirements that electronic data must meet can be derived from the area of data security and relate, *inter alia*, to preserving their authenticity, integrity, and accountability. These aspects are also mentioned in the Guidelines on Electronic Evidence in Civil and Administrative Proceedings adopted by the Committee of Ministers to serve as a practical tool to facilitate the use of electronic evidence in court proceedings (Council of Europe 2019).

Authenticity describes the origin of electronic evidence in the most general sense. The International Electrotechnical Commission (2019a) interprets the term authenticity in the field of digital technology as a "property of data that ensures that the identity of an entity is the one claimed." Authenticity is also understood as a "state in which information is valid and known to have originated from the stated source" (International Electrotechnical Commission 2019a). In fulfilling this requirement, "the investigator must be able to persuasively show that the evidence originated from the computer under attack or the computer in the crime scene" (Kanellis *et al.* 2006, p.60). Accordingly, the authenticity of electronic data should be based on a two-fold relationship (Walden 2007, p.380):

1) the relationship between electronic data and the offender, which is described as an "identity problem" (Walden 2007, p.380). Problems related to the identification of the offender in such cases are solved in several steps: firstly, establishing a proper link between the electronic data and the virtual identity of the person who possesses them; secondly, substantiating that this virtual identity belongs to the offender. In this respect, it is important to note that this is unlike physical identity, which is "tied to social networks, legal documentation, and biological characteristics, virtual identities are, for the most part, personally constructed" (Britz 2009, p.122). Since virtual identities can be shared and information systems can have multiple users, there may be doubts in criminal proceedings as to whether it was the offender who initiated the actions using the information system.
2) the connection between electronic data and an information system, which is called "computer source" (Walden 2007, p.381). This problem of justifying authenticity arises in the context of the specificities of the information system and communication in cyberspace. An information system is usually defined as "interrelated components that collect, manipulate, store, and disseminate information and provide a feedback mechanism to achieve a goal" (Zemmouchi-Ghomari 2021, p.4). This concept is consistent with systems theory, which states that a system is a unit that functions in an environment, contributes to the achievement of common goals, and is composed of many interacting parts. The location of these parts of the system, including the electronic data they contain, depends on many factors. In this context, the source of the electronic data must be established and confirmed in the criminal proceedings.

Another requirement for establishing the reliability of electronic evidence in criminal proceedings is its integrity. In the context of digital technologies, the integrity of electronic data in the most general sense means that the data have not been altered without legitimate reason during their processing. For example, the International Electrotechnical Commission (2019b) defines the integrity of electronic data in the field of digital technology as a "property of data that have not been altered or destroyed in an unauthorized and undetected manner." As mentioned above, electronic data can easily be altered due to the peculiarities of the functioning of information systems, as well as due to inappropriate (both intentional and negligent) human activity. Accordingly, the processing of such data, for example their collection or transmission in criminal proceedings, must be carried out in accordance with procedural requirements and using the tools provided for that purpose. If electronic data have been changed for objective

reasons, an "accurate and reliable method of documenting any such changes, including the reasons for any such modifications" (Mason 2016, p.23) should be followed. In this respect, it should be mentioned that different types of electronic data may be subject to different collection methods and technologies, and different methods and technologies may be used for the storage of this type of data during criminal proceedings.

Closely related to the requirement for the integrity of electronic data is the need to ensure the accountability of electronic data. Accountability implies that an appropriate mechanism for the collection and management of electronic data should be ensured. The protection of electronic data must be guaranteed through the choice of the appropriate means of obtaining the data, the processing of such data during pre-trial investigations and the presentation of the data in court. As cybercrime methods and techniques vary, "data recovery tools, data capture tools, data duplication tools, and data analysis tools may vary for every investigation" (Britz 2009, p.276). These aspects become particularly important when the circumstances in criminal proceedings are based exclusively on electronic evidence. In this context, criminal proceedings must follow procedures designed to minimize the risks to accountability and, consequently, to avoid doubts about the evidentiary value of electronic data.

In terms of accountability, it should be mentioned that "as well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources (e.g., in social media cases), or authenticate documents" (Eoghan 2010, cited in Grigaliūnas and Toldinas 2016, p.30). Although the data contained in an expert's report are considered evidence and are evaluated according to the same rules as other evidence, they do have some specificities. This is because the circumstances relevant to the disposition of the case are established by a person with special knowledge, not held by other participants to the criminal proceedings. For example, "an understanding of attacks is a necessary prerequisite to designing proper digital forensic methods to collect and analyse of attacks" (Kanellis *et al.* 2006, p.22). An understanding of the mechanism by which cybercrime is committed is essential for the identification and subsequent analysis of electronic evidence. For example, some investigative steps "include reading the partition table, searching existing files for relevant information such as keywords, system state changes, or text strings, retrieving information from deleted files, checking for data hidden in the boot record […] cracking passwords, and so on" (Kanellis *et al.* 2006, p.60). Therefore, when determining the circumstances relevant to a case on the basis of an expert's report, additional circumstances must also be assessed which are related not only to the adequacy of the material submitted to

the expert and the comprehensiveness of its examination, but also to the reasonableness and appropriateness of the methods used (Review of the application of the provisions of the Criminal Procedure Code on evidence in case law 2007). As stated in the scientific literature, "tested and validated tools should be used, or if other tools are used, then the investigator must ensure that the evidence is not tainted" (Kanellis *et al.* 2006, p.60).

In the case of cybercrime, the importance of substantiating the reliability of electronic evidence in criminal proceedings inevitably becomes apparent. Doubts as to whether such evidence is authentic and properly testifies to the facts arise from the very nature of the electronic data discussed above, namely the ease with which they can be altered and the difficulty of tracing such changes.

In such cases, an understanding of the specificities of electronic evidence and the development of a uniform practice of obtaining, presenting, verifying, and assessing it in criminal proceedings would ensure the development of a consistent and thus coherent approach to evidence and the emergence of good practice.

Interim Findings

A coherent approach to electronic evidence and a proper assessment of the reliability of this type of evidence is essential. In criminal cases relating to cybercrime, the quality of the proof-taking process can often be an issue when it comes to obtaining, presenting, verifying, and assessing electronic evidence. One of the main reasons for this relates to the peculiarities of such a type of evidence: 1) its instability, as electronic evidence can be altered quite easily, both due to the specificities of the operation of the information systems and intentional (or negligent) human activity; 2) the difficulty of tracing the changes made; and 3) the circumstances relevant to the case are usually determined by a person with special knowledge that is not held by the other parties involved in the criminal procedure.

The assessment of the reliability of electronic evidence in criminal proceedings is complex. Once it has been established that such evidence meets the requirements of correlation and admissibility, the assessment of its reliability also considers whether the preservation of the authenticity, integrity, and accountability of electronic evidence has been guaranteed during the proof-taking process.

In the interests of coherent regulation, legislation should not give priority to evidence based on its form. In accordance with the principle of technological neutrality, electronic data, irrespective of the technology that generated or processed them, should be admissible as evidence in criminal proceedings if they fulfil the purpose of evidence, its function in criminal proceedings and the other requirements laid down for evidence.

The speed, economy, and efficiency of criminal proceedings depend, among other aspects, on whether electronic evidence can be used seamlessly in its original electronic form in criminal proceedings. The preservation of this form may also be relevant in cases where it is necessary to implement obligations arising from international (European Union) law in the context of cooperation in criminal matters. Thus, a coherent approach to electronic data management in criminal proceedings contributes, *inter alia*, to efficient criminal proceedings.

References

Ablamskyi, S., and Vasko, A., 2022. Evidentiary Process in Ukrainian and Slovakian Criminal Proceedings: A Comparative Analysis and Implications on Criminal Proceedings. *Journal of Legal, Ethical and Regulatory Issues*, 25 (1S), 1–14.

Britz, M. T., 2009. *Computer Forensics and Cyber Crime: An Introduction*. 2nd edn. Columbus (Ohio): Pearson: Prentice Hall.

Butterfield, K., 2001. Metadata: An Overview. *AALL Spectrum*, 6 (3).

Code of Criminal Procedure of the Republic of Lithuania 2002. *Valstybės žinios*, 2002-04-09, No. 37-1341; with further amendments and supplements.

Constitution of the Republic of Lithuania (Adopted by the citizens of the Republic of Lithuania in the Referendum of 25 October 1992). Available from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/079fcad0cf8711ecb69ea7b9ba9d787b?jfwid=-cyl92hylw [Accessed 7 August 2023]; with further amendments.

Convention on Cybercrime, 21 November 2001. ETS No. 185 [online]. Available from: https://rm.coe.int/1680081561 [Accessed 8 August 2023].

Council of Europe, 2019. *Electronic Evidence in Civil and Administrative Proceedings* [online]. Available from: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5 [Accessed 8 August 2023].

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. OJ L 191, 181–190. Available from: http://data.europa.eu/eli/dir/2023/1544/oj [Accessed 7 August 2023].

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950. *ETS* 5 [online]. Available from: https://www.refworld.org/docid/3ae6b3b04.html [Accessed 7 August 2023].

ECtHR, Ibrahim and Others v. United Kingdom, 2016, Nos. 50541/08, 50571/08, 50573/08 and 40351/09 [online]. Available from: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-166680%22]} [Accessed 7 August 2023].

ECtHR, Vera Fernandez-Huidobro v. Spain, 2010, No. 74181/01 [online]. Available from:https://hudoc.echr.coe.int/tkp197/view.asp#{%22fulltext%22:[%22Vera%20Fernandez%22],%22itemid%22:[%22001-80608%22]} [Accessed 7 August 2023].

ECtHR, Telfner v. Austria, 2001, No. 33501/96 [online]. Available from: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-59347%22]} [Accessed 7 August 2023].

Eoghan, C., 2010. Handbook of Digital Forensics and Investigation. Academic Press.

Goda, G., Kazlauskas, M., and Kuconis, P., 2005. *Baudžiamojo proceso teisė [Criminal procedure law]*. Vilnius: Registrų centras.

Grigaliūnas, Š., and Toldinas, J., 2016. Digital Evidence Investigation Using Habits Attribution. *The 4th International Virtual Research Conference In Technical Disciplines, 17–21 October 2016* [online]. Available from: https://www.researchgate.net/publication/311616212_Digital_Evidence_Investigation_Using_Habits_Attribution [Accessed 8 August 2023].

International Electrotechnical Commission, 2019a. *Authenticity*. [online]. Available from: https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=171-08-07 [Accessed 8 August 2023].

International Electrotechnical Commission, 2019b. *Integrity <of data>*. [online]. Available from: https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=171-08-05 [Accessed 8 August 2023].

Juozapavičius, A., and Leonaitė, E., 2021. Procedūriniai įrodymų leistinumo aspektai baudžiamajame procese[Procedural Aspects of the Admissibility of Evidence in Criminal Procedure]. *Teisė*, 121, 80–97. Available from: https://www.journals.vu.lt/teise/article/view/25168/24458 [Accessed 8 August 2023]

Kanellis, P., Kiountouzis, E., Kolokotronis, N., and Martakos, D. (eds.), 2006. *Digital Crime and Forensic Science in Cyberspace*. Hershey, PA: Idea Group Publishing.

Mason, S., 2016. The Concept of a Convention on Electronic Evidence. *Amicus Curiae*, 105, 21–28.

Matulienė, S., n.d. *Įrodymai* [Evidence]. Universal Lithuanian Encyclopaedia [online]. Available from: https://www.vle.lt/straipsnis/irodymai/ [Accessed 8 August 2023].

National Information Standards Organization, 2004. *Understanding Metadata* [online]. Available from: https://www.lter.uaf.edu/metadata_files/UnderstandingMetadata.pdf [Accessed 8 August 2023].

Ohm, P., 2010. The Argument Against Technology-Neutral Surveillance Laws. *Texas Law Review,* 88 (7), 1685–1714.

Raghavan, S., and Raghavan, S. V., 2009. Digital Evidence Composition in Fraud Detection. In: *Digital forensics and cyber crime: first international ICST conference, ICDF2C 2009, Albany, NY, USA, September 30-October 2009, revised selected papers*.

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. OJ L 191, 118–180. Available from: http://data.europa.eu/eli/reg/2023/1543/oj [Accessed 7 August 2023].

Riekkinen, J., 2019. Electronic Evidence in Criminal Procedure: On the Effects of ICT and the Development towards the Network Society on the Life-cycle of Evidence. *Digital Evidence and Electronic Signature Law Review*, 16, 6–10.

Ruling of the Supreme Court of Lithuania of 9 April 2020 in criminal case No. 2K-81-895/2020.

Ruling of the Supreme Court of Lithuania of 14 July 2020 in criminal case No. 2K-141-303/2020.

Ruling of the Supreme Court of Lithuania of 17 July 2020 in criminal case No. 2K-164-458/2020.

Ruling of the Supreme Court of Lithuania of 12 November 2019 in criminal case No. 2K-264-976/2019.

Ruling of the Supreme Court of Lithuania of 30 January 2018 in criminal case No. 2K-26-689/2018.

Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, 12 May 2022. CETS No. 224 [online]. Available from: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 [Accessed 8 August 2023].

Sethia, A., 2016. Rethinking Admissibility of Electronic Evidence. *International Journal of Law and Information Technology*, 24 (3), 229–250.

Supreme Court of Lithuania, 2007. Review of the application of the provisions of the Criminal Procedure Code on evidence in case law approved by the Criminal Divisions of the Supreme Court of Lithuania. *Bulletin Court Practice*, 27.

Tadros, V., and Tierney, S., 2004. The Presumption of Innocence and the Human Rights Act. *The Modern Law Review*, 67 (3), 402–434.

Trigkas, N., 2017. The Authenticity of Electronic Evidence: First Steps Toward Improvement. *Edinburgh Student Law Review*, 3 (2), 20–27.

Vasko, A., and Klimek, L., 2023. Means of Proof in Criminal Proceedings in the Slovak Republic – New Challenges. *Access to Justice in Eastern Europe*, 1, 168–177. https://doi.org/10.33327/AJEE-18-6.1-n000106

Zemmouchi-Ghomari, L., 2021. Basic Concepts of Information Systems. In: D. Reilly (ed.). *Contemporary Issues in Information Systems – A Global Perspective*. IntechOpen. https://doi.org/10.5772/intechopen.97644

Walden, I., 2007. *Computer Crimes and Digital Investigations*. Oxford: Oxford University Press.

Jolanta Zajančkauskienė / Rima Ažubalytė /
Oleg Fedosiuk (eds.)

Towards Coherence in Criminal Justice

Challenges, Discussions And/Or Solutions

PETER LANG

Berlin - Bruxelles - Chennai - Lausanne - New York - Oxford

Library of Congress Cataloging-in-Publication Data

Names: Zajančkauskienė, Jolanta, editor. | Ažubalytė, Rima, editor. | Fedosiuk, Oleg, editor.
Title: Towards coherence in criminal justice : challenges, discussions, and/or solutions / edited by Jolanta Zajančkauskienė, Rima Ažubalytė, and Oleg Fedosiuk.
Description: New York : Peter Lang, 2025. | Includes bibliographical references and index.
Identifiers: LCCN 2025015805 (print) | LCCN 2025015806 (ebook) | ISBN 9783631929445 (hardcover) | ISBN 9783631935323 (ebook) | ISBN 9783631935330 (epub)
Subjects: LCSH: Criminal justice, Administration of. | Criminal jurisdiction. | Criminal law. | Criminal liability. | Evidence, Criminal. | Electronic evidence. | Convention for the Protection of Human Rights and Fundamental Freedoms (1950 November 5) | Fair trial.
Classification: LCC K5001 .T69 2025 (print) | LCC K5001 (ebook) | DDC 345—dc23/eng/20250403
LC record available at https://lccn.loc.gov/2025015805
LC ebook record available at https://lccn.loc.gov/2025015806

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek collects this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at .Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de.



Mykolas Romeris University

Reviewers:
Prof. dr. Edita Gruodytė (Vytautas Magnus University, Lithuania)
Prof. dr. hab. Wieslaw Plywaczewski (University of Warmia and Mazur in Olsztyn, Poland)

Copy-editor:
MB "Kopis"

Approved by Mykolas Romeris University Law School Council on 11 of June 2024 by resolution No. 1T-14 (1.12 E-20401).

ISBN 978-3-631-92944-5 (Print)
ISBN 978-3-631-93532-3 (E-PDF)
ISBN 978-3-631-93533-0 (E-PUB)
DOI.10.3726/b22750





Open Access: This work is licensed under a Creative Commons Attribution NonCommercial NoDerivatives 4.0 unported license. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/

© 2024 Jolanta Zajančkauskienė / Rima Ažubalytė / Oleg Fedosiuk (eds.)
Published by Peter Lang GmbH, Berlin, Germany
info@peterlang.com - www.peterlang.com

Contents

Rima Ažubalytė, Oleg Fedosiuk, Jolanta Zajančkauskienė | MRU
Preface xiii

Jolanta Zajančkauskienė | MRU
Introduction: What is the Role of Coherence in Criminal Justice?
The Characterization of Coherence in Law 1
Coherence Between National, International, and EU Law 4
Challenges to the Coherence of Criminal Law in the EU 6
Research Object 10
Research Aim and Objectives 10
Research Methodology 11
Limitations 12
The Structure of the Book 12
References 12

Part I
The Search for Coherence in Substantive Criminal Law

Oleg Fedosiuk | MRU
The Gray Area in the Concept of Human Trafficking: Between the Text of the Law and the Purpose of Criminalization
Human Trafficking as a Legal Concept 19
The Problem of Defining the Content of Exploitation 22
The Limitlessness of the Concept of Abuse of a Position of Vulnerability 29
Interim Findings 32
References 33

Linas Žalnieriūnas | *MRU*

The Search for Legal Coherence in the Criminalization or Decriminalization of Drug Possession

Factors Influencing Drug Use 37

Causes of Drug Criminalization 41

A Brief History of Drug Prohibition 42

Factors Influencing Drug Categorization and Quantification in Europe 45

Consequences of the Criminalization of Narcotic Drugs 48

The Health-Oriented Decriminalization of Drugs 50

Interim Findings 54

References 55

Tomas Girdenis | *MRU*

Coherence in Criminal Policy for Offenses Against Justice That Obstruct the Investigation of a Case

The System of Offenses against Justice in the Criminal Code of the Republic of Lithuania and Its Coherence 65

Criminal Liability for Offenses against Justice in the United Kingdom and the United States of America 68

Punishing Crimes of Perverting the Course of Justice in the UK 68

Punishing Obstruction of Justice Crimes in the USA 70

Sentencing for Crimes Against Justice in Lithuanian Case Law 73

Sentencing for Separate Crimes Against Justice 75

The Impact of the Process of Combining Sentences on Punishing Crimes Against Justice 77

Interim Findings 82

References 83

Jolita Šukytė | MRU
The Unlawful Stalking of a Person

Stalking as a Dangerous Form of Human Behavior and the Justification for Its Criminalization 87

Indications of Stalking 90

Types of Definitions of Stalking 93

The Regulation of Stalking Actions in Lithuania 95

Interim Findings 101

References 102

Eglė Bilevičiūtė | MRU
Administrative and Criminal Liability: Toward Sustainability

Administrative Liability as a Separate Type of Responsibility 105

Administrative Liability in Different European Countries 107

Administrative and Criminal Liability According to Lithuania's Regulations 109

Researchers' Opinions on the Difference Between Criminal and Administrative Sanctions 110

The Criteria for Determining Administrative and Criminal Liability in the Case Law of Various Courts 112

The Relevance of the Application of the *non bis in idem* Principle for the Qualification of Administrative and Criminal Liability 115

Interim Findings 118

References 119

Andrius Nevera | MRU
Standards for the Coherent Application of the Principles of Criminal Jurisdiction in Relation to Criminal Acts Committed by Lithuanian Citizens and Persons Permanently Resident in Lithuania Outside the Territory of Lithuania

General Remarks 125

The Place of Commission of a Criminal Act and Its Relevance for the Coherent Application of the Principles of Criminal Jurisdiction 126

The Concept of the Flag Principle and the Possibilities of Its Application to Criminal Acts Committed Abroad by Lithuanian Citizens and Persons Permanently Resident in Lithuania 133

The Content and Possibilities of the Application of the Universal Principle in Relation to Criminal Acts Committed Abroad by Lithuanian Citizens and Persons Permanently Resident in Lithuania. Guidelines for the Coherence of the Universal Principle with the Flag Principle and the Active Personality Principle 137

Problems and Solutions for the Application of the Dual Criminality Clause to Criminal Offenses Committed Abroad by Lithuanian Citizens and Persons Permanently Resident in Lithuania 147

Interim Findings 150

References 152

Part II
The Transformation of Criminal Procedure Law in the Context of Coherence

Raimundas Jurka | MRU
The E-Evidence "Movement" in European Union Criminal Justice: Toward or Beyond Coherence?

Cross-Border Access to Electronic Evidence Within the European Union: Reasons and Regulatory Background 162

The Relationship Between the European Investigation Order and the Regulation on Electronic Evidence 167

The Issue of the Admissibility of Electronic Evidence 173

Interim Findings 177

References 178

Renata Marcinauskaitė | MRU
Electronic Evidence in Criminal Proceedings

General Remarks 183

The Concept of Proof-Taking Activity and the Assessment of Evidence in Criminal Proceedings 184

The Concept of Evidence: The Identification of Electronic Evidence 186

The Requirements Applicable to Evidence 192

The Specifics of Electronic Evidence: The Justification of the Reliability of Electronic Evidence 193

Interim Findings 197

References 198

Rima Ažubalytė | MRU
Evidence in a Non-Conviction-Based Confiscation Procedure

General Remarks 203

General Requirements for the Process of Proof of NCB Confiscation 206

The Lower Standard of Proof in the Application of NCB Confiscation: A Balance of Probabilities and/or a Reversed Burden of Proof 213

Interim Findings 222

References 223

Rasa Žibaitė - Neliubšienė | MRU
Subjective Threats to the Free Evaluation of Evidence: Toward a More Coherent Legal Regulation

Manifestations of Intuitive Factors in the Process of Free Evaluation of Evidence 232

Confirmation Bias 235

Hindsight Bias 238

Availability Heuristic 241

Possibilities to Minimize Biases 242

Interim Findings 244

References 245

Sandra Kaija | Riga Stradiņš University Latvia

The Trial of a Criminal Case in an Appellate Court Hearing: A Written or Oral Procedure in the Context of the Right to a Fair Trial

The Right to a Fair Trial and the Choice of Procedure 252

The Possibilities of a Written Procedure in Criminal Proceedings in the Appellate Court 258

Interim Findings 263

References 264

Inga Žukovaitė | MRU

Coherence Between the Model of Remote Criminal Proceedings and the Standards Under Article 6 of the European Convention on Human Rights: The Reality of Threats to a Fair Trial

General Remarks 267

The Interaction Between Strict Procedural Rules and the Changing Context of Technological Progress 270

Encouragements, Warnings, and Boundaries Set by the European Court of Human Rights 274

The Example of Lithuania: Coherence Between Regulation and Practice 278

Interim Findings 282

References 283

Jolanta Zajančkauskienė, Rima Ažubalytė, Oleg Fedosiuk | MRU

Conclusions

Part I. The Search for Coherence in Substantive Criminal Law 287

Part II. The Transformation of Criminal Procedure Law in Context of Coherence 291

Jolanta Zajančkauskienė | MRU
Summary 297

Index 305