PIOTR LEWULIS*

COLLECTING DIGITAL EVIDENCE FROM ONLINE SOURCES: DEFICIENCIES IN CURRENT POLISH CRIMINAL LAW

Accepted: 30 November 2021; Published online: 29 December 2021

ABSTRACT. The importance of digital evidence, especially online content, is continuously increasing due to the proliferation of digital technologies in socio-economic life. However, the legal means of criminal evidence gathering in Polish legislation remain unchanged and do not take into account some contemporary challenges. In various countries, traditional rules of evidence gathering were created in the context of a physical world. These rules may be insufficient to safeguard the forensic soundness of evidence gathering methods. Inadequacies of current procedures may be especially visible in the context of transborder digital evidence gathering from online open sources. This article describes the practical shortcomings of Polish criminal evidence law in the context of digital evidence with particular attention to online open-source materials. Empirical data indicate that existing legal limitations are bypassed in practice to enable evidence collection. This unfortunately often happens at the expense of the forensic soundness of digital evidence.

I INTRODUCTION

Considering the widespread proliferation of computer technology and the increasing use of digital means of remote communication in daily socio-economic life, a great amount of information useful in criminal proceedings may come from online sources. The importance of digital evidence¹ extends to the prosecution of all types of crimes in all jurisdictions. In recent years an increase in the use of digital evidence in criminal proceedings has been noted,² and various digital materials are often of value in complex “cybercrimes” as well as in

*Piotr Lewulis, Ph.D., Department of Criminalistics, University of Warsaw, Warsaw, Poland. E-mail: p.lewulis@wpia.uw.edu.pl

¹ “Digital evidence” and “electronic evidence” are often used interchangeably in previous literature and official documents. In this article the term “digital evidence” will be used as understandable and technically correct.

² Fernando Molina Granja and Glen D Rodríguez Rafael, “The Preservation of Digital Evidence and Its Admissibility in the Court” (2017) 9 International Journal of Electronic Security and Digital Forensics 1.

“analogue” crimes such as fraud, hate speech, and copyright infringements.³

Of course, appropriate substantive criminal law responses to cybercrime issues are well developed on national and international levels. Existing legal measures include provisions of the Budapest Convention on Cybercrime⁴ – implemented in various national jurisdictions. However, some procedural aspects of combating cybercrime are still under development. Unsolved problems primarily relate to the rules of digital evidence collection in various transborder contexts.

The Internet’s borderless nature causes the need for international procedural cooperation in cybercrime cases. Basic mechanisms of international mutual legal assistance were developed years ago.⁵ Still, many aspects of evidentiary procedures rely on national legislation. Apart from the tools of international legal assistance, it is necessary to maintain internally consistent, clear, and forensically valid national rules for securing digital evidence from online sources. On the example of the Polish criminal procedure, which is discussed in this article, it is visible how such an issue may be overlooked even despite the existence of some legal provisions designed with digital evidence in mind.

It should be underlined that proper administration of criminal justice requires digital evidence in all cases to be collected, analysed, presented, and assessed in a forensically sound manner (thus allowing them to maintain the necessary credibility in the judicial context). In addition to strictly forensic requirements of evidence handling, all evidence should be collected in accordance with appropriate provisions of law. This requirement includes digital evidence from online sources. The collection of open-source digital materials may seem easy since they are readily available to the public. However, it still requires appropriate legal grounding, which is sometimes overlooked in national legislations despite the legal framework set out in article 32 of the Convention.

³ Paul Grimm, Daniel Capra and Gregory Joseph, “Authenticating Digital Evidence” (2017) 69 *Baylor Law Review* <https://ir.lawnet.fordham.edu/faculty_scholarship/856> accessed 1 May 2021.

⁴ Council of Europe, ETS 185 – Convention on Cybercrime.

⁵ In the Union, mutual recognition mechanisms, now based on the European Investigation Order Directive; with third countries, mutual legal assistance (MLA) mechanisms.

The use of digital evidence was accepted by the judiciary in Poland years ago, yet minimal digital evidence legislation exists and there is an apparent lack of appropriate legal procedures for collecting open-source digital materials as evidence. Simultaneously, empirical data shows that online open-source materials are often present in criminal proceedings – this is possible due to a flexible, yet incorrect, use of the existing legal framework. Similar problems may be present in other jurisdictions as well – when some digital evidence solutions are introduced into the procedure, but in a way that does not take into account some specific scenarios.

This article describes existing legal issues in Polish criminal proceedings regarding the collection and use of two specific types of digital evidence available online: open-source (e.g., social media postings or website contents) and covert online materials (such as remotely accessible webmail or cloud data storage). The article provides an in-depth legal analysis of how digital evidence fits into Poland's currently existing evidence-gathering procedures. The legal analysis is supplemented by quantitative analysis of empirical data gathered from criminal proceedings. The identified issues are discussed in the context of possible solutions under international law, applicable in various jurisdictions.

II DIGITAL EVIDENCE IN POLISH CRIMINAL PROCEDURE

To discuss how online materials, among other digital data, may be incorporated into the evidence in a criminal case in Poland, it is crucial to provide a general outline of the applicable law on evidence gathering. Therefore, this section focuses on the current legal framework for evidence use in the Polish criminal procedure. The description of the fundamental theoretical background of evidence law is followed by a practical legal analysis of currently existing evidence gathering rules in the context of digital evidence.

2.1 General Theoretical Framework for Evidence Law

The overall shape of evidence proceedings in Poland is governed by several core principles. All legal proceedings are based on statutory law. In criminal cases, most of the relevant legal provisions are in-

cluded in the Criminal Code⁶ and Code of Criminal Procedure⁷ (hereinafter: CCP). In line with the continental legal system's features, court precedents are not a source of law. However, legal assessments made by the Polish Supreme Court are carefully looked upon by lower courts. In practice, the Supreme Court's judgments are of great interpretative importance and highly valued as a source of jurisprudence.

The CCP formally recognizes only two general types of evidence sources: personal and material (or real) evidence. It is traditionally underlined that this division is mostly of theoretical importance⁸ as neither type of evidence is *a priori* more reliable than the other. A practical difference is that all personal evidence sources are strictly determined by a closed list which includes: witnesses, suspects, and experts. The list of potentially admissible material evidence sources is open. The broad "material evidence" category, therefore, includes everything except personal statements: tools, weapons, trace evidence, documents, DNA evidence, as well as other material objects. Since digital information does not possess a physical form, digital evidence placement in such an exhaustive division of evidence types might be problematic. However, out of necessity digital evidence falls into the "material evidence" category despite not having a physical form.

The concept of "evidence" itself is legally undefined. The general principle of criminal proceedings stipulated in Article 7 CCP states that criminal courts are authorized to determine all factual and legal matters at their discretion, with due consideration to the principles of sound reasoning, knowledge, and personal experience. Therefore in practice, anything (including digital data) may be presented as material evidence in criminal proceedings as long as it meets the requirement of rationality and brings the court closer to establishing material truth.⁹

Subsequently, there is no legal definition of "digital evidence". Legal and forensic communities in Poland tend to share the inter-

⁶ Polish Penal Code of 6 June 1997 (Journal Of Laws 1997 No. 88 item 553) as amended.

⁷ Polish Code of Criminal Procedure of 6 June 1997 (Journal of Laws 1997 No. 89 item 555) as amended.

⁸ Stanisław Śliwiński, *Polski Proces Karny Przed Sądem Powszechnym* (I, Gebethner i Wolff 1948) p. 602.

⁹ Marian Cieślak, *Polska Procedura Karna. Podstawowe Zaożenia Teoretyczne* (1984) p. 361.

national theoretical understanding of “digital evidence” defined as any information of evidentiary value drawn from electronically processed binary data (i.e. data in digital form). Such a broad definition is a synthesis of the definitions proposed to date in the existing literature.¹⁰ A recently updated Council of Europe guide similarly defines digital (or electronic, as it is sometimes referred to) evidence as “any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings”.¹¹ Despite some editorial and stylistic differences, it is safe to say that the essence of what is understood as “digital evidence” in the legal context has not changed since the beginning of the 21st century.

In this article, “digital evidence” is understood as defined above. The definition is broad and includes all the evidentiary value information drawn from openly accessible online data. All general considerations on digital evidence use in Polish criminal proceedings apply to either covert and open-source data unless stated otherwise.

Open-source digital materials have been described in previous Polish literature as extremely useful in the context of police investigations,¹² but their use as evidence in the courtroom remains devoid of a separate theoretical framework. However, there is nothing to suggest that open source digital materials should be treated differently in terms of admissibility criteria than other evidence.

From a forensic point of view, the intangible nature of all digital data makes it much easier to copy or manipulate than traditional

¹⁰ Carrie Whitcomb, “An Historical Perspective of Digital Evidence: A Forensic Scientist’s View” (2002) 1 *International Journal of Digital Evidence* <<https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf>> accessed 28 December 2020; Michael Mukasey, Jeffrey Sedgwick and David Hagy, “Electronic Crime Scene Investigation: A Guide for First Responders” (US Department of Justice 2008) NCJ 219941 <<https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>> accessed 1 May 2021.

¹¹ Nigel Jones and others, “Electronic Evidence Guide. A Basic Guide for Police Officers, Prosecutors and Judges” (Council of Europe 2020) 12 <<https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4>> accessed 1 May 2021.

¹² Bażej Stromczyński and Pawe Waszkiewicz, “Biały Wywiad w Praktyce Pracy Organów Ścigania Na Przykładzie Wykorzystania Serwisów Społecznościowych” [2014] *Prokuratura i Prawo* p. 146.

forms of evidence. This created a new challenge for the justice system, as digital evidence must be handled with care to ensure its integrity.¹³ Digital data is stored on electronic mediums as a series of ones and zeros. Even common, everyday experience dictates that such data may be easily modified (intentionally or unintentionally) since changes in the data structure may be caused even by the simplest activation of a particular electronic device. Its probative value in a judicial setting depends on the authenticity and integrity of digital data. Crucial is the ability to prove that the content presented in court is exactly the same as the one captured during the investigation. Fortunately in this context, strings of binary digits are not individually distinguishable and it is possible to create their truly lossless copies to be used in criminal proceedings. Of course, this is only possible if appropriate forensic procedures are followed. A copy should be authenticated using, for example, an appropriate hash algorithm, so that the integrity of data can be demonstrated through a checksum comparison.¹⁴ Data collected in such a forensically sound manner, unlike printouts, may be subject to a proper forensic examination.

Polish law does not describe any specific techniques or methods of material evidence gathering, leaving that to experts in relevant disciplines of forensic science. Any existing guidelines on digital evidence handling, therefore, remain formally unbinding. However, all the methods used for evidence collection, processing, analysis, and presentation are subsequently subjected to judicial assessment based on Article 7 CCP.

In practice, the Polish judiciary has accepted digital evidence in the courtroom without much hesitation. There are no formal restrictions on what types of digital data (e.g. text, images, metadata, social

¹³ Piotr Lewulis, "Digital Forensic Standards and Digital Evidence in Polish Criminal Proceedings. An Updated Definition of Digital Evidence in Forensic Science." (2021) 13 *International Journal of Electronic Security and Digital Forensics* 1 p. 403–417; Reza Montasari, "Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction" in Hamid Jahankhani and others (eds), *Global Security, Safety and Sustainability – The Security Challenges of the Connected World* (Springer International Publishing 2016).

¹⁴ Digital Forensics Engineering, Technology Faculty, Firat University, Elazig, Turkey, Erhan Akbal and Sengul Dogan, "Forensics Image Acquisition Process of Digital Evidence" (2018) 10 *International Journal of Computer Network and Information Security* p. 1.

media postings, or others) may be used as evidence. Substantive technical guidelines on digital evidence admissibility are described in various international¹⁵ and Polish forensic literature on the subject.¹⁶ The importance of such principles in the context of evidence value preservation has also been underlined in the Polish Supreme Court judgment of 20 June 2013, which stated clearly that:¹⁷

Electronic data are equal to other evidence as a basis for issuing the judgment. Considering the nature of electronic data, their judicial evaluation must be extremely cautious, as the personal experience of any user of computer equipment shows that digital data are often easily modified. This is due to the very essence of electronic data. ... Digital data must be analysed in an extremely thorough manner based on the state of the art knowledge.

Such “state of the art knowledge” may be accessed through various sets of guidelines and best practices grounded in the discipline of digital forensics. Practical guidance for handling digital evidence is provided on a national and international level by several actors.¹⁸ Judges themselves generally lack expert knowledge on digital evidence,¹⁹ so to maintain high standards of evidence proceedings, lawyers must turn to professional literature. According to the newest Council of Europe guide,²⁰ digital evidence must be obtained in compliance with existing legislation and best practices. Although some authors have tried over the years to propose a universal and

¹⁵ See e.g.: Eoghan Casey, Robert A Dunne and Inc NetLibrary, *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet* (Academic Press 2004); Jasmin Cosic, “Formal Acceptability of Digital Evidence” in Aboul Ella Hassanien and others (eds), *Multimedia Forensics and Security*, vol 115 (Springer International Publishing 2017) p. 327–348.

¹⁶ See e.g.: Arkadiusz Lach, *Dowody elektroniczne w procesie karnym* (Dom Organizatora 2004); Wojciech Andrzej Kasprzak and Difin, *Ślady cyfrowe: studium prawnokryminalistyczne* (Difin 2015).

¹⁷ Polish Supreme Court’s Judgment of 20 June 2013 (sygn. III KK 12/13).

¹⁸ Jeanne Pia Mifsud Bonnici, Melania Tudorica and Joseph A Cannataci, “The European Legal Framework on Electronic Evidence: Complex and in Need of Reform” in Maria Angela Biasiotti and others (eds), *Handling and Exchanging Electronic Evidence Across Europe*, vol 39 (Springer International Publishing 2018) p. 205.

¹⁹ Gary Kessler, “Judges’ Awareness, Understanding, and Application of Digital Evidence” [2011] *Journal of Digital Forensics, Security and Law* 55.

²⁰ Jones and others (n 10) 13.

abstract model of digital evidence handling,²¹ such proposals quickly run obsolete due to the rapid changes in technology and there is no universally accepted “model”. There is, however, a set of generally accepted basic principles governing all digital forensic activities which has been developed at the beginning of the century.²² The main tenet of these principles is to always have a properly authenticated, intact copy of digital evidence and that all examinations should be performed by appropriately trained personnel. To always protect the original digital content against alterations.

Digital evidence admissibility is based on data authenticity, completeness, and reliability. This should be achieved by following forensic guidelines of digital evidence acquisition, analysis, and presentation while fulfilling other evidence gathering’s legal requirements.

2.2 *Rules of Material Evidence Collection*

The actual collection of evidence requires law enforcement officials to act on an appropriate legal basis. Polish criminal procedure defines specific legal means of evidence gathering depending on the type of evidence at hand. While all personal evidence (e.g. witness testimony) is obtained through statements made during hearings, there is also a defined range of legal procedures for the collection of material evidence. Depending on the circumstances, on the grounds of the Polish Code of Criminal Procedure, one of the three legal tools may be appropriate for material evidence gathering:

- a) Through “search” procedure (Chapter 25, Article 219 CCP). A search may be performed to locate and collect objects that might serve as evidence in criminal proceedings. A search may be per-

²¹ Ankit Agarwal and others, “Systematic Digital Forensic Investigation Model” [2011] Gupta International Journal of Computer Science and Security 2011; Richard Adams, Val Hobbs and Graham Mann, “The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice” (2013) 8 Journal of Digital Forensics, Security and Law <<https://commons.erau.edu/jdfls/vol8/iss4/2>>.

²² Warren G Kruse and Jay G Heiser, *Computer Forensics: Incident Response Essentials* (Addison-Wesley 2001); Michael G Noblett, Mark M Pollitt and Lawrence A Presley, “Recovering and Examining Computer Forensic Evidence” (2000) 2 Forensic Science Communications <<https://go.gale.com/ps/i.do?p=AONE&sw=w&issn=15288005&v=2.1&it=r&id=GALE%7CA137921526&sid=googleScholar&linkaccess=abs>> accessed 14 November 2021; Rodney McKemmish, “When Is Digital Evidence Forensically Sound?” in Indrajit Ray and Sujeet Shenoj (eds), *Advances in Digital Forensics IV* (Springer US 2008).

formed on private premises and other places whenever there is good reason to suspect that objects sought are to be located there. Importantly, search activities are deliberately designed to be overt. A search warrant stating the extent of the evidence sought should be presented to the person whose premises the search is to be conducted. A warranted search may be conducted with or without the consent of an interested party, but secret or remote searches are not allowed on the grounds of criminal procedure.

- b) Through “seizure of objects” which may serve as evidence (Chapter 25, Article 217 CCP). Objects that might serve as evidence in criminal proceedings should be surrendered by any person who is in their possession when required by the authorized law enforcement officials. Every entity within Polish jurisdiction (including all private and legal persons) has a legal obligation to comply with such a request. In case of refusal, a search is justified. Of course, objects sought by the law enforcement may be also provided voluntarily by any party without coercion either spontaneously (e.g. when the victim presents evidence) or as a result of other statutory obligations (e.g. when a nationally operating Internet Service Provider delivers metadata to law enforcement, which is required by the provisions of telecommunications law²³ and Article 218 CCP).
- c) Material evidence may also be collected during a “visual examination” (Chapter 23, Article 207 CCP). According to the Code of Criminal Procedure, any place, person, or physical item may be submitted to a visual examination whenever it is needed (the necessity is determined individually given the circumstances). This relatively flexible procedure is designed to allow a careful, well-documented inspection of either a place (typically a crime scene, e.g. to collect trace evidence), a person or person’s remains (e.g. to determine one’s injuries), or an object (e.g. a tool, to examine its features or to collect traces).

As stated, within the Polish criminal procedure, all digital evidence falls into the legal category of “material evidence” without further distinctions or subdivisions. Therefore, legal instruments applicable for material evidence gathering should be applied for digital data. However, these provisions of criminal procedure have been designed

²³ Polish Telecommunications Act of 16 July 2004 (Journal of Laws 2004 No. 171 item 1800) as amended.

in the context of the physical world. In order to enable the use of search and seizure procedures in the context of digital evidence, Article 236a CCP was added in 2003.²⁴ It warrants that “the provisions of this Chapter [i.e. Chapter 25] apply accordingly to the holder and user of a device containing electronic data or of an IT system, with regard to the data stored on this device or in this system or on a data storage medium in their possession or use, including correspondence sent by e-mail”. Therefore the scope of search and seizure procedures has been explicitly extended to digital data and electronic equipment that may and should be collected during criminal proceedings consistent with digital forensics guidelines. However, the “visual examination” procedure based on Article 207 CCP (placed in Chapter 23 CCP) remains uncovered by the scope of Article 236a CCP. Therefore digital materials formally cannot be subjected to visual examination, for they are neither place, person, nor physical item.

2.3 The Shortcomings of the Existing Legislation

Since more than half of all criminal investigations today require access to cross-border electronic evidence,²⁵ the above-described provisions on material evidence gathering are often tested, showing some serious shortcomings in the context of contemporary criminal investigations.

Whenever digital materials of probative value are stored within Polish jurisdiction, open-source or not, they may be collected through search and seizure procedures (based on Article 217 or 219 CCP). In such cases some additional legal conditions apply – a search warrant may be needed, but obtaining digital evidence stored on Polish servers is relatively uncomplicated in legal terms. All entities storing information within Polish jurisdiction are obligated to cooperate with law enforcement.

Some problems arise, however, whenever digital content is stored outside Polish jurisdiction yet remotely accessible online. This includes data stored privately by users in remotely accessible foreign data centres and processed by foreign entities, such as those offering

²⁴ Polish Code of Criminal Procedure Amendment of 7 January 2003 (Journal of Laws of 2003 No. 17 item 155) as amended.

²⁵ European Commission, “Recommendation for a Council Decision Authorising the Opening of Negotiations in View of an Agreement between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters COM/2019/70 final”.

online cloud storage or providing other online services. Under the current Polish legislation, such data cannot be accessed directly by the authorities. They cannot be subjected to a warranted search even if the resources sought are readily available remotely (e.g. from a logged-in account from computer equipment found on the searched premises) because the hardware which stores the data is placed outside Polish jurisdiction and cannot be covered by a search warrant. Polish officials may officially access such digital data using international legal aid tools (via judicial cooperation)²⁶ or through semi-official cooperation with the foreign data processing entity (via direct cooperation). Unfortunately, such methods are viewed by Polish experts and practitioners as time-consuming, overcomplicated, yielding uncertain results, and overall grossly inefficient.²⁷ Some concerns were also raised as to whether direct, semi-official cooperation with foreign entities is an entirely correct practice as bypassing official channels of communication should be generally discouraged.

Similar problems arise in the context of openly available online information sources. Open-source information (e.g. social media posts) may be of important probative value, but even though such data is easily accessible to law enforcement, it cannot be officially collected as evidence since there is no appropriate legal procedure for doing so. Such a scenario is highly common in practice given that many critical and popular IT services associated with open source content of probative value are hosted outside Polish jurisdiction – especially in the US.

There is no national legal procedure allowing for a forensically and legally sound digital evidence gathering in such cases. Search and seizure procedures are unsuitable for jurisdictional reasons (not to mention that it would be highly unreasonable to “search and seize” openly available information). The visual examination procedure based on Article 207 CCP, on the other hand, formally cannot be used on digital materials.

Due to a shared technological reality, similar digital evidence issues are simultaneously faced by judicial authorities in various countries, as confirmed in the European Commission’s report of open

²⁶ Such these based on the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

²⁷ Paweł Opitek, “Wybrane Aspekty Pozyskiwania Dowodów Cyfrowych w Sprawach Karnych” [2018] *Prokuratura i Prawo* p. 65, 73.

public consultation on e-evidence.²⁸ The Polish perspective outlined above is not unique, and the deficiencies and fragmentation of legal frameworks concerning digital evidence gathering have already been recognized at the European level. To ensure member states' authorities' ability to access data stored outside their jurisdiction, the European Commission has presented a legislative proposal for a regulation²⁹ and a directive³⁰ aimed at enhancing cross-border digital evidence gathering. The proposal, if enacted, would provide a legal framework for member state authorities to quickly access digital evidence from other EU states through European Production and Preservation Orders for electronic evidence in criminal matters. Such a legal tool would allow member state authorities to demand digital content from foreign entities in a similar way as it is now possible within the national jurisdiction through a seizure of objects (or data). However, the initial proposal was published in April 2018 and as of 2021 inter-institutional negotiations are still ongoing. The actual effectiveness of any future solutions is yet to be assessed. Otherwise, the existing primary and secondary EU law does not currently harmonize digital evidence gathering issues. Some relevant provisions are, however, present in the Budapest Convention on Cybercrime – these will be discussed in the final section of this article.

2.4 *Potential Legal Consequences of Procedural Violations*

In the current legal landscape, Polish law enforcement authorities may try to bypass or even ignore the described procedural shortcomings. Given the existing legal deficiencies, it is well imaginable that digital evidence is collected with the omission, or even contrary to some regulations (e.g. data in the cloud may be accessed in course of a search in excess of law enforcement powers or online content may be “collected” without proper legal grounding). Such evidence could be considered illegally obtained (*tertium non datur*). Although

²⁸ European Commission, “Report of Open Public Consultation on E-Evidence” (2018) <https://ec.europa.eu/info/sites/info/files/report_of_open_public_consultation_on_e_evidence_april2018.pdf> accessed 1 May 2021.

²⁹ European Commission, “Proposal for a Regulation of the European Parliament and of The Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters COM/2018/225 Final – 2018/0108 (COD)”.

³⁰ European Commission, “Proposal for a Directive of the European Parliament and of The Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final – 2018/0107 (COD)”.

undesirable, such breaches of procedural law would not prevent the use of the collected data as evidence. Under Article 168a CCP (added on 15 April 2016³¹) “evidence cannot be considered inadmissible solely because it was obtained in breach of the procedural provisions”. Therefore, on national legal grounds, any procedural errors are *de facto* acceptable as long as they do not have a “direct influence on the content of the judgement” because only then they may serve as grounds for an appeal under Article 438 CCP (potentially leading to a mistrial). In other words, if procedural errors in criminal proceedings do not impact (at least potentially) the judicial ability to correctly assess the evidence at hand, their legal consequences are inexistent.

Of course, it is clear that Article 168a CCP effectively and explicitly validates illegal evidence in Polish criminal proceedings which is understandably a source of controversy. The provision has been already rightly criticized as unconstitutional.³² Polish Supreme Court has previously pointed out that in light of Polish constitutional principles it is unacceptable that the state authorities could gather evidence in violation of applicable regulations (such a view has been expressed in 2010, in the context of illegal wiretapping).³³ Illegal evidence gathering should be negatively assessed in the context of both principles of the rule of law and the right to a fair trial, as guaranteed in the Polish constitution (in Article 2 and Article 45, respectively).³⁴ However, Article 168a has not yet been formally reviewed by the Polish Constitutional Tribunal which has the authority to assess it. A motion to do so was first submitted by the Polish national Ombudsman (in 2016). However, it was later withdrawn (in 2018) due to concerns about the composition of the constitutional court itself.³⁵

³¹ Polish Act of 11 March 2016 on the Change of the Code of Criminal Procedure and Some Other Acts (Journal of Laws of 2016 item 437).

³² ukasz Cora, “Procedural Axiology and the Permissibility of Evidence Described in Art. 168a of the Code of Criminal Procedure” [2018] *Państwo i Prawo* p. 121.

³³ Polish Supreme Court’s Judgment of 30 November 2010 (sygn. III KK 152/10).

³⁴ Constitution of the Republic of Poland of 2 April 1998 (Dz. U. 1997 nr 78 poz. 483).

³⁵ ukasz Starzewski, “RPO Wycofa z Trybunału Konstytucyjnego Wniosek Ws. „owoców Zatrutego Drzewa” | Rzecznik Praw Obywatelskich” (2018) <<https://bip.brpo.gov.pl/pl/content/rpo-wycofal-z-trybunalu-konstytucyjnego-wniosek-ws-%E2%80%9Eowocow-zatrutego-drzewa%E2%80%9D>> accessed 14 November 2021.

On the other hand, the severity of procedural infringements may be gradual, and the exclusion of evidence may not always be the right consequence in case of minor errors which do not affect the veracity of the factual findings.³⁶ Of course, investigative interests of law enforcement authorities must be balanced with procedural safeguards to human rights. Interestingly, Polish legislative authorities justified the introduction of the Article 168a CCP, among other arguments, that such a regulation is not contradictory to the European Court of Human Rights jurisprudence on Article 6 ECHR which guarantees the right to a fair trial.³⁷ Such compliance is important not only for ideological or political reasons but also because the ECHR takes clear precedence before national law in Poland under Article 91 of the Polish Constitution (as such, the ECHR has a superlegal status and is an important point of reference for national legislation).³⁸ The expectation that illegally obtained evidence is excluded from criminal proceedings plays a vital role in many legal systems. However, the European Court on Human Rights does not take a strong position in the matter and intervenes only in the most flagrant cases of illegally obtained evidence (e.g. evidence obtained through torture).³⁹ The ECHR does not lay down any specific rules on the admissibility of evidence as such, leaving that matter for regulation under national law.⁴⁰

Despite the warranted criticism, illegally obtained digital evidence (such as data collected in collision with the provisions of criminal procedure) is admissible in court, given its credibility is otherwise uncompromised. As long as the evidence is subject to an effective

³⁶ Sebastian Brzozowski, "Dopuszczalność Dowodów Uzyskanych z Naruszeniem Przepisów Postępowania w Kontekście Art. 168a k.p.k." (2017) 1–2 *Palestra* p. 52.

³⁷ Aleksandra Rychlewska, "O Przepisie Art. 168a k.p.k. Jako Przyzwoleniu Na Korzystanie w Ramach Procesu Karnego z Dowodów Zdobytych w Sposób Nielegalny" (2016) 5 *Palestra*. <<https://palestra.pl/pl/czasopismo/wydanie/5-2016/artykul/o-przepisie-art.-168a-k.p.k.-jako-przyzwoleniu-na-korzystanie-w-ramach-procesu-karnego-z-dowodow-zdobytych-w-sposob-nielegalny>> accessed 14 November 2021.

³⁸ See: Kai Ambos, *European Criminal Law* (Cambridge University Press 2019) p. 74.

³⁹ Joachim Meese, "The Use of Illegally Obtained Evidence in Criminal Cases: A Brief Overview" (2017) 18 *ERA Forum* 297, *Gäfgen v. Germany*, Grand Chamber (1 June 2010), Application no. 22978/05, §162.

⁴⁰ Joelle Vuille, Luca Luparia and Franco Taront, "Scientific Evidence and the Right to a Fair Trial under Article 6 ECHR" (2017) 16 *Law, Probability And Risk* 55.

judicial review, procedural errors in its collection may not be formally considered as violating the right to a fair trial. As a result, the practical impact of the described procedural deficiencies remains minimal, which may be potentially seen encouraging law enforcement authorities to ignore some of the existing restrictions.

III EMPIRICAL DATA ON DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS

Publicly available digital content processed outside Polish national jurisdiction is crucial in various criminal proceedings involving fraudulent sales offers online, copyright infringements, or hate speech in social media. It would be unreasonable to expect online open sources not to be used in criminal proceedings only because of the abovementioned legal difficulties. It may be hypothesized that in practice, the legal limitations in open-source digital evidence collection are circumvented or purely ignored by law enforcement practitioners. To test such a hypothesis, a qualitative study of the criminal cases files has been conducted.

The study's primary objective was to establish the actual image of the current practice regarding the use of digital evidence in Polish criminal proceedings. The study's specific purpose was to show what types of digital materials are used as evidence and how they are formally introduced into evidence in criminal cases. To that end, the most accurate research method is criminal cases' files analysis. A strong point of such a method is that case files present actual reality instead of research based on questionnaires or interviews presenting opinions or ideas about reality.

The study methodology involved the analysis of criminal cases concluded legally between 2016 and 2018. The study was conducted during the first half of 2019 (January – June) in 7 out of 8 district courts within Warsaw's Provincial Court jurisdiction. The research was therefore carried out in District Court (hereinafter: DC) for Warsaw Mokotów, DC for Warsaw Wola, DC for the Capital City of Warsaw, DC for Warsaw Śródmieście, DC in Piaseczno, DC in Pruszków, and DC in Grodzisk Mazowiecki.⁴¹ It is worth mentioning that district courts in the Polish legal system are the first and most

⁴¹ President of the DC for Warsaw Żoliborz did not consent to making the files accessible for research purposes, and the files for proceedings from this court were excluded from the researched population.

basic rung on the judiciary's hierarchy, hearing the vast majority of all criminal matters at first instance.

The research included proceedings in cases directly associated with computer technology (so-called cybercrimes or computer crimes) and other types of offenses that are often linked with the use of a computer and the Internet (these included: fraud, copyright crimes, and hate speech). Therefore, the representativeness of the studied sample was limited due to the qualitative criterion for the selection of legal qualifications. However, this did not affect the primary study objective. A total of $N = 3545$ cases have met the criteria, out of which a total of $n = 370$ randomly chosen proceedings were examined.

The variables taken into account in the research included circumstances related to digital evidence present in the analysed court cases. Several variables were taken into account,⁴² out of which the most important in the discussed context were:

- 1) Was there any digital evidence present in the given case.
- 2) What kind of digital information was relevant in the given proceeding specifically (e.g. e-mails, electronic messages, open-source website content, stored files, data obtained from electronic entrepreneurs or telecommunications operators, etc.). If possible, applied legal grounds for the evidence gathering have been noted.
- 3) Whether or not the digital evidence presented by either party has been found inadmissible or unreliable by the court for any reason (if so, why?).

Digital evidence was present in 253 out of the 370 proceedings included in the study (68%). Digital content used as evidence in the analysed proceedings originated from diverse sources. The type of data and the number of proceedings in which they were present (regardless of the legal means of their introduction) are included in Table 1 below. It is worth noticing that digital evidence originating from files extracted from secured electronic equipment occurred in a relatively small number of cases. Content from open sources or that provided by external data processing entities (telecommunications companies, banks, or website administrators) often proved useful, with open-source information being the most popular type of digital content used in criminal proceedings.

Importantly, in none of the analysed cases the court has deemed digital content inadmissible or unreliable for any reason.

⁴² See: own research sourced (See: Piotr Lewulis, *Dowody cyfrowe - teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Warsaw University Press 2021, <https://doi.org/10.31338/uw.9788323548027>).

A thorough quantitative analysis of the legal bases used to secure digital evidence source materials proved to be impossible due to various mistakes and chaotic application of the law. Legal grounds for actions undertaken by law enforcement officials in the analysed cases were often cited incorrectly or inconsistently. Basic quantitative results are presented in the Table 2 below. Any procedural errors in evidence gathering had no measurable impact on the outcome of these cases. However, it was possible to perform a qualitative analysis and to point out some particularly interesting aspects of the analysed practice.

Firstly, digital materials were successfully collected from various entities within the national jurisdiction (service providers and telecommunications companies, and banks based in Poland). To that end, usually Articles 217 and 218 CCP (sometimes in connection with art. 236a CCP) were used. Such requests for data from domestic entities usually yielded solid results. The data were often provided as printouts (originating from internal data processing systems). The data was provided in digital form (on electronic media) in 59 cases. Data from foreign entities (IT companies, webpages administrators, e-commerce entities) were sought in 24 cases – requests were successful in only six.

Secondly, physical searches on the grounds of Article 219 CCP were performed in 32 cases. In none of them digital evidence was collected on-site using advanced digital forensic techniques. The searches aimed to secure physical computer equipment to be later analysed (which did not always happen).

Thirdly, various digital evidence was often provided by witnesses or victims of their own volition. This happened in the majority of all the analysed cases: witnesses came to police hearings with printouts of digital content (these included especially e-mails, but also openly available online content – such as social media postings) to support their vocal claims. Such printouts were usually included in the case files as attachments to the witness interview report. Usually, they were not examined forensically.

Fourthly, in case of online open sources data, in the absence of a better procedure, Article 207 CCP was used. In 12 cases openly available websites were accessed by a law enforcement official who then described its visual content in writing. Within such reports, submitted to the case files, websites were labelled as “objects” or “places” interchangeably in various proceedings. Content collected this way included Facebook postings (seven cases), private websites

containing alleged copyright infringements (four cases), and the contents of remote access hard drive (in one case). In the latter case, the data were stored on a foreign server that the police accessed with the defendant's consent (informally obtained). This is especially worth underlining in the context of the later considerations on the Convention on Cybercrime.

Fifthly, when not performing visual examination, police officers often used internal notes to describe publicly available data contents. In Table 2. these cases were labelled as "OSINT (internal notes only)". Notably, according to the Polish criminal procedure, internal notes cannot be a source of evidence. To introduce their contents into evidence, the police officers were subsequently interviewed as witnesses to the website's visual content.

In other words, digital evidence from online open sources was either collected via visual examination (Article 207 CCP) or otherwise documented in writing, often informally or subsequently confirmed by witness testimony, thus bypassing the shortcomings of evidence-gathering procedures. Unverifiable from a digital forensic perspective, printouts seem to be the default method of online content presentation in the Polish courtroom. Due to the limitations of the conducted exploratory study, the precise scale of these practices in Polish criminal proceedings needs confirmation in future research.

IV DISCUSSION AND CONCLUSIONS

Current criminal procedure in Poland lacks specific legal tools for online digital materials acquisition in a trans-border context. The same may be true in many other jurisdictions even if digital evidence regulations are seemingly put in place (alike Article 236a CCP in Poland). Since legal difficulties in accessing digital evidence are highly undesirable within the European legal area, the European Commission has proposed the creation of a European Production and Preservation Orders, designed to allow judicial authorities of the Member States to obtain digital data directly from the relevant entities in Europe. However, the designed solutions will not fully address the problem of online data collection. Moreover, materials available online are often stored outside European jurisdictions altogether, which may render EU-oriented legal tools useless in such cases. According to a recent SIRIUS EU survey conducted among judicial authorities in the European Union, in 2019, US-based tech companies (namely: Google, Facebook, Microsoft) were the over-

whelming majority of entities contacted for digital content.⁴³ Of course, any specifically European legal solutions will not cover these entities which call for designing relevant international regulations.

Legal grounds for online data gathering should therefore be sought in other international regulations. A relatively obvious answer to the presented problem may be the use of the legal framework provided in the Council of Europe's Convention on Cybercrime. Importantly, it has a grand international scope, as it has been ratified by dozens of countries worldwide – including the US. Besides substantive regulations, the Convention includes specific provisions on procedural aspects of digital evidence collection. A 2nd Additional Protocol to the Convention is currently under development, which aims to provide a more effective mutual legal assistance with a more transparent framework for existing practices in transborder access to data.⁴⁴ Regardless of the exact future shape of the 2nd Additional Protocol and regardless of other provisions on procedural powers to secure digital evidence (specified in art. 15 to 21 of the Convention), the issue of access to online digital materials physically processed in another jurisdiction has already been specifically recognized in the art. 32 of the Convention on Cybercrime. It explicitly allows to cross jurisdictional boundaries unilaterally when collecting digital evidence available online⁴⁵:

A party may, without the authorization of another Party:

- a) Access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b) Access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

This regulation addresses explicitly the two discussed transborder data-gathering scenarios: access to publicly available data (which is unrestricted under art. 32a of the Convention) and access to covert,

⁴³ SIRIUS EU, “SIRIUS EU Digital Evidence Situation Report” (2020) <https://www.europol.europa.eu/sites/default/files/documents/sirius_desr_2020.pdf> accessed 1 May 2021.

⁴⁴ Council of Europe Cybercrime Convention Committee (T-CY) “Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime – State of Play” T-CY(2020)3.

⁴⁵ Article 32 of the Convention on Cybercrime of 23 November 2001.

remotely accessible data (which requires the user's consent under art. 32b of the Convention). The article is an exception to the principle of territoriality. However, to actually function, the Convention on Cybercrime provisions must be properly implemented into the national law and are subject to various domestic restrictions.

According to the Council of Europe's data, 42% of states that are parties to the Convention had introduced specific procedural powers to secure digital evidence by February 2020. Such provisions exist in at least 39 European countries.⁴⁶ This does not mean that the existing provisions cover all the possible scenarios or are implemented correctly.

The European Commission stated that national law in at least 20 EU Member States empowers authorities to perform search and seizure activities on remotely accessible devices.⁴⁷ To their disadvantage, these procedures are often based on the traditional concepts of jurisdiction and physical evidence (such as the already discussed Polish regulations). A simple extension of the already existing domestic search and seizure powers to situations specified in art. 32b of the Convention on Cybercrime would often go against the provision's requirements: remotely accessible yet not publicly available data cannot be accessed without the user's consent, which must be lawful and voluntary. The person providing access or agreeing to data disclosure may not be forced or deceived,⁴⁸ which practically rules out compulsory search procedures in such situations due to their coercive nature. The consent requirement along with other possible domestic safeguards (such as the need to always produce and provide a search warrant) may significantly diminish traditional search pro-

⁴⁶ Cybercrime Programme Office of the Council of Europe (C-PROC), "The Global State of Cybercrime Legislation 2013-2020: A cursory Overview" (2020) <<https://rm.coe.int/3148-1-3-4-cyberleg-global-state-feb2020-v1-public/16809cf9a9>> accessed 1 May 2020.

⁴⁷ European Commission, "Commission Staff Working Document – Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings (SWD/2018/118 Final)".

⁴⁸ Cybercrime Convention Committee (T-CY) of the Council of Europe, "T-CY Guidance Note # 3 Transborder Access to Data (Article 32)" (2014) <<https://www.ccdcoe.org/uploads/2019/09/CoE-141203-Guidance-Note-on-Transborder-access-to-data.pdf>> accessed 1 May 2021.

TABLE 1
Types of digital content used in the analysed proceedings (number of proceedings and their percentage share in the examined sample, 100% = 370) [Variable 2].

cedures’ effectiveness in the discussed context. However, these requirements are not always followed closely, and the actual practice in some countries may be assessed as inconsistent with the Convention on Cybercrime.⁴⁹

The adopted legal solutions are imperfect, yet they exist, and the problem is recognized. Open-source online information, on the other hand, often remains unrecognized as a formal source of evidence. The art. 32a of the Convention on Cybercrime allows for a transborder open-source data collection (which seems to be the only common sense solution since the data is indeed publicly available). Despite such authorization in international law, there is no appropriate procedure for open-source digital evidence gathering in the national law in Poland, as well as in other European countries.

Digital content is undoubtedly popular as a source of evidence in criminal proceedings. A quantitative study of the court practice has

⁴⁹ Anna-Maria Osula and Mark Zoetekouw, “The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives” (2017) 11 Masaryk University Journal of Law and Technology 103; Andrii Skrypnyk and Ivan Titko, “Use of Information from Electronic Media in Criminal Proceeding of Several European States: Comparative Legal Research” (2019) 3 SOCRATES. Rīgas Stradina universitātes Juridiskās fakultātes elektroniskais juridisko zinātnisko rakstu žurnāls / SOCRATES. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law 8.

TABLE 2
Legal grounds used to introduce content of digital origin in the analysed proceedings (number of proceedings and their percentage share in the examined sample, 100% = 370) [Variable 2].

unsurprisingly confirmed that online open-source materials, among other types of data, are often used as evidence in polish criminal cases. However, the study results also suggest that the existing evidence-gathering law is applied chaotically to digital materials, with no real attention to broadly understood evidence credibility.

All the applicable rules of evidence in Poland and many other European countries were developed well before the advent of the digital era. They were created in the context of material evidence gathering in the physical world. The theoretical recognition of the differences between traditional and digital evidence was not thoroughly followed by the creation of appropriate legal instruments for digital evidence gathering. Conventional evidence-gathering means known to Polish law, such as “search and seizure”, do not stand the test of time: they are insufficient to mitigate modern challenges associated with digital evidence. The inadequacy of the existing evidence gathering regulations is apparent in the context of new technologies. The collection of remotely available digital evidence does

not have a proper legal basis in Polish legislation causing law enforcement to bypass existing procedures. Similar situations may be expected in other countries as well.

The issue may seem trivial, especially that it often has no practical consequences within the Polish procedure due to the previously mentioned Article 168a CCP. However, the acceptance and validation of such imperfect practices may cause a detrimental long term effect of loosening evidence collection standards. In the case of digital evidence, loosening evidence gathering standards will inevitably cause the deterioration of evidence quality, leading to errors in the administration of justice. As empirical research shows, printouts of digital content often replace forensically sound evidence. Reducing the entire digital evidence collection process to making a printout blatantly contradicts known forensic principles yet is accepted by the judiciary. Therefore, the main conclusion and the resulting recommendation is that the lack of specific legal tools allowing forensically sound digital evidence collection should be addressed to ensure such materials' credibility. Ideally, an entirely new legal instrument explicitly designed to collect digital evidence should be created and implemented in various national jurisdictions in a similar and coordinated fashion. Article 32 of the Convention on Cybercrime provides a general framework and ready-to-use international legal grounds for developing new national procedures of online transborder evidence gathering.

OPEN ACCESS

This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.