Problemy Prawa Karnego 2024, T. 8, nr 2
s. 1 z 37
ISSN 2353-9712
https://doi.org/10.31261/PPK.2024.08.02.06

Oskar Peče
University of Maribor,
Slovenia
https://orcid.org/0009-0003-6682-4643

Miha Šepec
University of Maribor,
Slovenia
https://orcid.org/0000-0002-3220-8901

The dilemma of the location of digital evidence

Abstract: Determining the legally relevant location of digital evidence requires an analysis of the technical and legal aspects of obtaining such evidence by law enforcement. The problem relates to the complexity of determining the location of digital evidence, especially in the case of cloud storage, where data is often stored in various locations worldwide. The associated uncertainty regarding the location of digital evidence poses a significant legal challenge in cross-border evidence collection. This article acknowledges that the technical location of digital evidence is tied to the physical location of the storage unit. However, it also explores alternative ways to define the location of digital evidence based on existing regulations for cross-border collection of digital evidence. The problem of the location of digital evidence is analysed from the perspective of the concept of territorial jurisdiction in the digital age.

Keywords: cloud storage, cross-border investigations, digital evidence, jurisdiction, the location of evidence

1. Introduction

The discussion on the location of digital evidence involves a theoretical examination of the legal aspects related to law enforcement's acquisition of such evidence. It addresses the ambiguity of the location of digital data when using online storage solutions (cloud storage) and the related jurisdictional issues faced by law enforcement agencies in obtaining this sort of evidence. Digital data must always be stored on a physical storage media, and in the case of cloud storage, investigators often do not know

where this physical media (in this case, the server) are located.[1] Cloud service providers frequently use servers located in various cities, countries, and even continents with user data often being stored simultaneously on multiple servers for protection in case one of them fails.[2] This means that not only can the user or the person investigating the content of a cloud not be certain of the location where the data is stored, but they may also not know how many duplicates exist on how many servers, where those servers are located, and from which one they are accessing the data at any given moment. Online services can be provided from anywhere, meaning that in the country where the provider offers the service, there is no need for physical infrastructure, premises, or staff.[3] The problem relates to the investigation of remote, internet-connected devices, for example servers, that store email not yet downloaded to the user's computer. When an investigator accesses a foreign internet server, they effectively leave their local jurisdiction and enter a foreign jurisdiction, raising questions about the legality of their actions and the appropriateness of a national judge's search order, which serves as the legal basis for investigating the device.[4]

While the use of digital evidence used to be limited mainly to cases of cybercrime, these days this type of evidence is common in cases involving all types of crimes.[5] The gathering of digital evidence presents certain opportunities (for example, it can be obtained with relative ease) as well as challenges, especially concerning the reluctance of governments to allow foreign law enforcement to gather evidence across borders, even in cyberspace.[6] The problem pertains to the concept of territorial jurisdiction in the

---

[1] NIST, "Digital Evidence Preservation. Considerations for Evidence Handlers," September 2022, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf, 1.

[2] Michalas Antonis and Yigzaw Kassaye Yitbarek: "LocLess: Do you Really Care Where Your Cloud Files Are?," IEEE International Conference on Cloud Computing Technology and Science, Luxembourg: The Institute of Electrical and Electronics Engineers (2016): 515.

[3] Recital 7 of Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on the European Production Order and the European Preservation Order for electronic evidence in criminal proceedings and on the execution of custodial sentences following criminal proceedings.

[4] Janja Bernard, "Problematika pregona računalniškega kriminala in uporabe digitalnih dokazov z vidika državnega tožilstva," in *Digitalna forenzika v kazenskih postopkih*, ed. Liljana Selinšek (Ljubljana: GV Založba, 2008), 77.

[5] Alberto R. Gonzales, Regina B. Schofield and David W. Hagy," Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors," Washington: U.S. Department of Justice, Office of Justice Programs, 2007, https://www.ojp.gov/pdffiles1/nij/211314.pdf, xi.

[6] Robert J. Currie, " Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the 'Next Frontier'?," *Canadian Yearbook of international Law*, vol. 54 (2017): 66.

digital age, where national borders become blurred from the perspective of daily interactions of information-savvy individuals. An investigator may have full access to a crucial piece of evidence, but the question arises whether obtaining this evidence is permissible, as it is located on a device situated abroad. In such a situation, the investigator may not feel like they are conducting an investigative action in a foreign country, as they are physically operating their own computer within their jurisdiction. However, they are still accessing an IT system on a device located outside their jurisdiction.

The investigation of data obtained online can raise sovereignty issues if it involves accessing data located abroad or stored on electronic devices located in a foreign country. This brings into question the infringement of the sovereignty of other states. Analysing these problems requires a consideration of both technical and normative aspects. If the data being accessed (and consequently obtained) is located on servers in another country, the investigating state undertakes a sovereign act within another state.[7] Territorial sovereignty is therefore violated when foreign investigators access foreign IT systems without permission (even if this is done to investigate or stop a cyberattack originating from that country).[8] Accessing digital evidence is often complicated by (according to some) outdated territorial rules and the involvement of foreign IT service providers. As a result, cross-border acquisition of digital evidence frequently necessitates the use of time-consuming instruments of international mutual legal assistance.[9] Whether such a stringent system is necessary, impractical or a downright thorn in the heel of criminal investigators is up for debate and it certainly concerns the question of where digital evidence is actually located.

Compared to criminal offenders, law enforcement agencies are significantly limited in their investigations when it requires obtaining and analysing digital evidence, especially when such evidence is stored remotely. In addition to national legislative restrictions, their work is hindered by international borders, as accessing data content on remote de-

---

[7] Ulrich Sieber and Carl-Wendelin Neubert, „Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty," *Max Planck Yearbook of United Nations Law Online*, vol. 20, no.1 (2017): 254–255.

[8] "Sovereignty and jurisdiction," E4J University Module Series: Cybercrime, Module 7: International Cooperation against Cybercrime, United Nations Office on Drugs and Crime, accesed May 25, 2024, https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html#:~:text=Cybercrime%20jurisdiction%20is%20established%20by,interests%20and%20security%20of%20the.

[9] Athina Sachoulidou, "Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation," New Journal of European Criminal Law, vol. 0, no. 2 (2023): 2.

vices raises questions about respecting the sovereignty of the countries where these devices are located. [10] These types of reservations are certainly not absurd. They serve an important purpose, not only from the standpoint of protecting national sovereignty but also national security. Accessing various types of digital data is critical for preventing and effectively combating modern criminal activity, but limited by legislation in the jurisdiction where electronic data is stored, and the existence of bilateral or international agreements on cross-border access to digital data or evidence.[11]

In cross-border acquisition of digital evidence, it is always necessary to consider territorial sovereignty, as defined by the Court of International Justice in the *Lotus* case.[12] Stemming from this ruling, states must not exercise their jurisdiction over the territory of other states.[13] The prosecution of criminal offenses and related investigative actions fall within the jurisdiction of the state, meaning that conducting such actions on the territory of other states constitutes an infringement of their territorial sovereignty. Due to the nature of digital evidence (it can be located anywhere in the world and accessed from practically anywhere), it is often questionable where this type of evidence is actually located and which copy of identical data a person is actually accessing.[14]

The purpose of this article is to categorically define the types of determining the location of digital evidence that are currently established in the international legal order, with a focus on the European Union, and to identify the essential aspects of these types of determining the location of digital evidence. In it, we highlight that the location of digital evidence is primarily tied to the location of storage units, while taking into the account that in international law, legally fictitious alternative approaches to determining the location of digital evidence have been developed. In line with these developments, considering the issue of the location of digital evidence from the perspective of state sovereignty and the jurisdiction of law enforcement authorities, as well as the need for international coop-

---

[10] Sieber and Neubert, „Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty," 244–245.

[11] Stanislaw Tosza, " Gathering Electronic Evidence for Administrative Investigations. Exploring an Under-the-Radar Area", eucrim, no. 0 (2024): 2.

[12] Permanent Court of International Justice, "Affaire Du "Lotus" ... = The Case of the S.S. "Lotus," accessed 12.8.2024, https://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm.

[13] Sieber and Neubert, „Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty," 253.

[14] Identical copies of a file can be located in different locations. This is particularly common and relevant in case of multiple backups, which, by their very nature, often exist in multiple locations for security reasons.

eration among law enforcement agencies to effectively combat crime, we can expect the development of some form of a shared digital investigative territory.

2. Where is the data?

The issue discussed here pertains to stored files rather than the content that is being created. When we talk about cross-border acquisition of digital evidence, we refer to stored and existing data content.[15] The issue pertains to the specific difference between acquiring existing files and real-time surveillance. In the realm of digital evidence, we can encounter borderline situations where accessing a remote device in relation to a specific file blurs the practical distinction between acquiring stored files for investigative analysis and conducting direct real-time surveillance of an individual's activities. This involves scenarios where the user of a remote device is still creating or modifying a specific file at the time of access, highlighting the important distinction between an investigation of an electronic device and real-time surveillance. This distinction is crucial due to the different legal assumptions underpinning the lawful execution of each investigative action. It presents a particularly specific situation in remote investigation of electronic devices, compared to conventional investigations where a device is initially seized, and a static identical copy of data is created and later examined. In remote investigations, the user often or at least potentially retains access to the device during law enforcement's access. Even with this distinction, it would be necessary to analyse when a file is considered stored in the context of the boundary between investigating an electronic device and remotely monitoring its use. Is the acquisition of an open file (a file available to an application on the operating system for reading and/or writing)[16] questionable from this perspective? The crucial difference needs to be defined not purely from a technical standpoint (the method or status of how the file is stored) but from the user's activity at the time of the investigative action concerning the specific file. In other words, did the user interact with the file in any way at the time of remote access and securing of the file? In line with this

[15] Eurojust, "Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers." accessed January 23, 2024, https://www.eurojust.europa.eu/sites/default/files/assets/trans-border-access-to-stored-computer-data-under-article-32-of-the-budapest-convention-on-cybercrime-and-extraterritorial-powers-23-01-2024.pdf: 2.

[16] "open file," Encyclopedia, PCmag, accesed April 30, 2024, https://www.pcmag.com/encyclopedia/term/open-file

explanation, the essential distinction would be the user's actual engagement with the file at the time of access, rather than the technical status of the file.[17] This is both a theoretical and practical issue of remote device investigations, which could be the subject of its own paper as it deserves a detailed analysis. For the purposes of this specific paper, it is essential that it pertains to files statically stored on a specific storage medium, which are not being accessed or modified by anyone (at least as a general rule or to the knowledge of the investigative authority) at the time of their securing.

The question of the location of a certain piece of digital evidence primarily relates to distinguishing between the informational content of the evidence and its stored shape. From a technical perspective, digital evidence is merely a series of electronic impulses, stored in a more or less permanent form.[18] When we talk about informational content, we refer to the information or data presented or stored within the digital evidence. This can relate directly to the contained information or the file itself (for example a video of a committed crime), information that can be extracted from the content of such evidence (such as bank transaction data from a spreadsheet file), as well as information about the file itself (metadata). Thus, digital evidence can contain developed information or merely data from which information can be extracted through analysis and comparison with other data. The storage unit as a carrier of digital data represents the physical manifestation of digital evidence, much like a piece of paper for a written document or a photograph. Information itself can be located in many places simultaneously, and ultimately, it can exist in the memory of any person. Even though certain information can be found in various accessible places, the appropriateness of obtaining or accessing specific information is tied to its' actual accessed source. In the modern digital age, accessing data and information stored on devices worldwide has become so effortless that the physical location of these devices is often not even considered. As a result, many question the rationale behind rigidly assessing the legality of obtained digital evidence with regard to the location of accessed devices. However, the assessment of the legality of obtaining specific digital evidence in relation to the particular source or device from which the evidence was acquired becomes undoubtedly necessary when compared to other sources of evidence. A defendant cannot be compelled to provide a defense or disclose information solely because another person knows that information, re-

[17] The difference is significant, as a computer user can leave a file open for an extended period of time without making any changes to it.

[18] Liljana Selinšek, "Digitalna forenzika v kazenskih postopkih." In *Digitalna forenzika v kazenskih postopkih*, ed. Liljana Selinšek (Ljubljana: GV Založba, 2008), 31.

gardless of whether the identity of that person is known and they are otherwise obliged to testify. To this, one must sensibly add the extremely important aspect of state sovereignty and the associated prohibition of cross-border investigative actions, which substantiate the linking of the location of digital evidence to a physical storage unit as a legal fact of international public law.

When dealing with digital evidence, we must also consider the intermediate stage between the physical storage medium and the contained data or information, namely, the computer file. »A file is a container in a computer system for storing information.«[19] Files represent the digital equivalent of physical information and data carriers in the domain of documentary evidence, such as a piece of paper, a printed photograph, or an audio recording on a magnetic tape. In the context of an actual investigation, it is primarily the files that are acquired or secured. The reason for this is that files serve as a medium through which data can be presented or information can be conveyed to an individual in an understandable manner. Therefore, to access their content, these files need to be opened using a program that supports the specific file format.[20] If an investigator were to only acquire data contained within a file, it would mean copying the data from an open file into another file, or creating a completely different file to replicate the source data being acquired. An example of this would be an investigator opening a text file on a computer using a text editor and taking a screenshot of the displayed text. A comparable scenario in the physical domain would be a police officer photographing a relevant document found during a house search instead of seizing it. From this, we can deduce that such copying of the digital representation of files is not the most trustworthy method of obtaining evidence in criminal proceedings, as it merely provides an assumed replica or approximation of the original evidence. In criminal proceedings, to satisfy the requirement of evidence authenticity, we strive to obtain the original, which in the digital domain can only be represented by the original file containing the relevant data. This distinction is important as defining the file as the actual form of digital evidence theoretically provides an answer to the location of digital evidence as tied to the location where the specific file with relevant evidentiary content is stored.

When dealing with the process of obtaining evidence in criminal law, we are foremost concerned with the sources of information rather than the

---

[19] Margaret Rouse, "File," Technopedia, accessed June 26, 2024, https://www.techopedia.com/definition/7199/file

[20] The file format is the structure of a file that tells a program how to display its contents.« Computer Hope, Dictionary, "File format," accessed June 26, 2024, https://www.computerhope.com/jargon/f/file-format.htm.

content itself. Legislation (typically) regulates the seizure of objects and documents, the interrogation of witnesses, house searches, the examination of electronic devices, etc. Thus, the process, as it relates to obtaining information from these sources, is determined by the form of the source themselves. The content or anticipated content of the evidence is however also important as investigative actions aim to obtain evidence related to the specific investigated crime. The content of the examined electronic device is crucial in assessing the appropriateness of the investigative measure in terms of the proportionality test between the means used and the goal of the investigation, as stipulated by the European Court of Human Rights in the case of Kruglov and Others v. Russia.[21]

Similarly, we find prohibitions on conducting certain types of evidence collection based on the content of the evidence. An example of this is the interrogation or other investigative actions involving a lawyer in connection with their client. This is a special situation where such intrusion into privacy is specifically limited due to attorney-client privilege. It is one of the oldest recognized privileges for confidential communications[22] which, despite extensive practice, often encounters new legal questions and violations in the realm of electronic evidence and the investigation of electronic devices. Superficially, it may seem that this condition pertains to the means, such as the lawyer, their office, documentation, and electronic devices. However, it is actually a substantive prohibition on collecting evidence containing content that the defendant has shared with the lawyer or that the lawyer has gathered for their client's case. When conducting investigative actions, where the means involve a lawyer or objects and items related to their work, there are often restrictions. The European Court of Human Rights has explicitly emphasized that the persecution and harassment of members of the legal profession strike at the very heart of the Convention[23] system, and therefore, the searching of lawyers' premises should be subject to especially strict scrutiny.[24] This restriction also applies to the presence of legal advice from a lawyer to a client found in the data content of the investigated device.[25] The EU Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial

---

[21] European Court of Human Rights, Kruglov and others v. Russia, case 11264/04.

[22] Adjoa Linyz, "The Attorney–Client Privilege and Discovery of Electronically-Stored Information." *Duke Law & Technology Review*, vol. 10, no. 1 (2011): 12.

[23] Council of Europe: *Convention for the Protection of Human Rights and Fundamental Freedoms*. Council of Europe Treaty Series 005. Strasbourg, 1950.

[24] European Court of Human Rights, Kolesnichenko v. Russia, case 1956/04, par. 31

[25] European Court of Human Rights, Visy v. Slovakia, case 70288/13

sentences following criminal proceedings[26] (hereinafter referred to as the E-evidence Regulation) also considers certain immunities and privileges that may apply to categories of persons, such as diplomats, or specially protected relationships, such as the aforementioned confidentiality between a lawyer and client, or the right of journalists not to disclose their sources, as mentioned in other mutual recognition instruments.[27]

In Slovenia, it is legally required[28] to create an identical copy of the data content for the purpose of investigating a seized device, thereby creating a new medium to be examined. The investigation is conducted on this identical copy, not the seized device. This is an established forensic practice aimed at ensuring the integrity of the investigated data. In the case of Kruglov and Others v. Russia the ECHR also highlighted that for electronic devices which are not tools or products of a crime, prolonged retention is not justified if there are no legitimate reasons why the content of the device could not be copied. The Budapest Convention[29] similarly anticipates this procedure in the third paragraph of Article 19, stating that each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data, including the power to make and retain a copy of those computer data and to maintain the integrity of the relevant stored computer data. In the expert analysis of digital evidence, particularly the process of obtaining and investigating it, their volatility must be considered.[30] Digital evidence is extremely volatile, both in terms of changes and deletion. This aspect is particularly problematic in cases where services are moderated by service providers.[31] Consequently, if the procedure is

---

[26] 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

[27] Recital 47 – 48 of the E-evidence Regulation (Regulation (EU) 2023/1543)

[28] Paragraph 1 of Article 223.a of the Slovenian Criminal Procedure Act stipulates that if an electronic device is seized for the purpose of investigation, the electronic data must be preserved by storing it on another suitable data carrier in such a manner that the identity and integrity of the data are maintained, and its use in subsequent proceedings is ensured, or an identical copy of the entire data carrier is made, ensuring the integrity of the copy of the data.

[29] Council of Europe: *Convention on Cybercrime*. European Treaty Series – No. 185, Budapest 2001.

[30] Recital 41 of the E-evidence Regulation (Regulation (EU) 2023/1543).

[31] Elizabeth White, "Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism," Leiden Journal of International Law, vol. 37, no. 1 (2024): 228–250, accessed April 19, 2024. https://www.cambridge.org/core/journals/leiden-journal-of-international-law/article/closing-cases-with-opensource-facilitating-

correctly executed to ensure data integrity, we are addressing the issue of the location during the preservation or securement phase. The evidentiary value of digital evidence is significantly dependent on the procedure used to secure it. This evidentiary value can primarily be assessed based on three attributes: authenticity, integrity, and accountability.[32] All three attributes are crucially linked to the precise identification of the actual source of the data and ensuring the consistency of the data content stored at the source with the data that was investigated.

Since the medium for evidentiary content in the form of digital data is the storage unit, it is logical to consider the location of the digital evidence during the acquisition phase as being tied to the location of this storage unit. This concept is not contentious in cases where digital evidence or data content is found on individual smaller electronic devices or memory units, which the data holder likely physically had in his possession. These are devices that will be physically seized for the purpose of investigation. In most cases, they require direct possession to access their data content. For these devices, the location of digital evidence is not problematic, as it is entirely tied to the physical device on which it is stored. Since the investigation of this data is inseparably linked to the seizure of these devices, the limitation of law enforcement's jurisdiction regarding seizure, which can only be directly carried out within their area of jurisdiction, is evident. The concept of the location of digital evidence becomes somewhat blurred in the case of remote access to digital evidence stored in the cloud or on other remote devices. The question is where the police are actually acting in this case. Physically, they do not go abroad, but instead use a computer within their jurisdiction for the purpose of the investigation. Nevertheless, their actions interfere with a device located in a foreign country.

3. The problem of international infringement on individual rights

An important aspect of the contentious nature of cross-border investigative actions and the acquisition of digital evidence is that such investigative actions constitute an infringement on the rights of individuals. In the context of cross-border infringements, we primarily talk about the administrators of information systems or digital services and the users of these services whose data is stored on the servers hosting these serv-

---

the-use-of-usergenerated-opensource-evidence-in-international-criminal-investigations-through-the-creation-of-a-standing-investigative.

[32] Selinšek, "Digitalna forenzika v kazenskih postopkih." 31.

ices. Such actions may very well represent unlawful infringements on the rights of these individuals (and legal entities). For the purposes of criminal prosecution, the illegality of such infringements by authorities is usually excluded if it is legally determined and based on a judicial act or an act of another competent authority (usually a type of search order).[33] This means that the actions of the competent authorities are bound by compliance with national legislation and individual decisions of the competent national authorities. This results in a strong limitation to the territory of the state police, as the reach of the validity of national legal acts, in the absence of existing international agreements or specific recognitions, is only within the territory of that state. Such infringements on the rights of individuals are problematic in the context of cross-border investigative actions from the perspective of both involved states. On one hand, such actions in a foreign country are illegal by the concept of territorial sovereignty, as the legal acts of the state conducting the investigation do not exclude the illegality of investigative measures in another country. On the other hand, the other country, where the investigated devices are actually located, is obliged to protect the rights of individuals on its territory, the property located on its territory, and, generally, act so as to prevent unlawful actions on its territory.

Cross-border intrusions into information systems by foreign investigators constitute illegal access to an informational system if they are not conducted in accordance with national legislation and an existing international agreement. The criminalization of illegal access to an informational system is required by the Budapest Convention and the Directive on attacks against information systems[34] The Budapest Convention, in Article 2, states that "each party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right." It also mentions that this may require the offense to be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system connected to another computer system. Directive 2013/40/EU, in Article 3, states that member states of the EU must take the necessary measures to ensure that, when committed intentionally, unauthorized access to the whole or any part of an information system is punishable as a criminal offense when committed by infringing a security measure, at least for cases that are not minor. The described

[33] Such is the case in Slovenia.

[34] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

criminal offense does not pertain to physical access to computer hardware (any manipulation with computer components), but to access the information content stored on an electronic device. It pertains to causing damage, abuse of confidentiality of information, or abuse of the system itself through unauthorized access to the information system or its data content. The purpose of criminalizing such unauthorized access is to protect the uninterrupted operation and integrity of information systems.[35]

At this point, it is important to highlight the distinction between the two forms of criminalization of such intrusions into an information system, as required by the Budapest Convention. The first is the criminalization of the access to the whole or any part of a computer system without right, and the second is the criminalization of the first form, when committed by infringing security measures in relation to a computer system that is connected to another computer system.[36]This distinction refers to the difference between cases where investigators access an online service from a device that is already logged into the service (or they know the password[37] and simply log into the user account) and cases where investigators access an information system or user account by "hacking it" and infringing on its security measures. If the country where the device hosting the information system is located only criminalizes the aforementioned qualified form of access,[38] cross-border investigative accesses that do not involve circumventing the target information system's security measures using special technical means[39] would not, in themselves, be illegal in the absence of international limitations on police jurisdiction. This distinction could be an important condition or limitation in the future, in the case of the formation of international agreements that would allow such cross-border investigative accesses. It would conceptually limit the intrusion to the sphere of the investigated persons and restrict the interference

---

[35] Miha Šepec, Kibernetski kriminal, kazniva dejanja in kazenskopravna analiza (Maribor: Univerzitetna založba Univerze v Mariboru, 2018), 62.

[36] The qualified form of illegal access also includes the intent of obtaining computer data or other dishonest intent, but for the purposes of the discussed topic, this addition is not as essential since obtaining computer data is the very purpose of the investigative actions conducted by the police.

[37] The fact that the police know the password of a user account, even if obtained from the service user, does not mean that the police have obtained the user's consent to search their account.

[38] Šepec, Kibernetski kriminal, kazniva dejanja in kazenskopravna analiza, 64.

[39] The question arises whether this condition would be met in the case of social hacking. On one hand, such actions do not involve the use of special technical means to bypass the security measures of the information system in a technical way, but often exploit the users use of certain services and technical support. Here we stumble upon a question of the extent of the interpretation of the system's security measures.

with the information system itself. This would be particularly reasonable if such international investigative measures were limited to user accounts of persons who are in a meaningful way connected to the country conducting the investigation.[40] However, even such a legal framework would undoubtedly require appropriate safeguards as two issues remain evident even with this limited approach. The first issue is that, even in investigations limited solely to a specific user account or the accounts of a particular individual, it is necessary to ensure that the rights of that individual are adequately respected. States must not allow other states to violate the rights of individuals within their territory, even if those individuals are citizens of the infringing state. The second issue is that limiting investigations to individual user account does not prevent the potential abuse of initiating an exceptional number of "individual" investigations into user accounts. If the legal thresholds for investigating a single user account in the country conducting the investigation are too low, restricting investigations to individual user accounts does not provide effective protection against indiscriminate and large-scale surveillance of user accounts. This reveals the need for a certain level of harmonization of conditions for investigating remote devices among countries potentially adopting an agreement permitting such cross-border investigations.

This brings us to another highly contentious infringement on individual rights, namely the infringement on the privacy of individuals. Under Article 8 of the European Convention on Human Rights[41] (hereinafter referred to as ECHR), everyone has the right to respect for their private and family life, their home, and their correspondence. Interference by a public authority with the exercise of this right is acceptable only if it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.[42] It is well established through case law of the European Court of Human Rights, among them in the case of Ivaschenko v. Russia,[43] that the search and seizure of electronic data constitutes an infringement on the right to privacy of correspondence, as specified in Article 8 of the ECHR.

While an intrusion carried out within the framework of investigative actions pursues a legitimate aim (the prevention of crime), it is always questionable whether it is conducted in accordance with the law and is

[40] Such as citizens, residents, legal entities with a registered office in that country, etc.

[41] Council of Europe: *Convention for the Protection of Human Rights and Fundamental Freedoms*. Council of Europe Treaty Series 005. Strasbourg 1950.

[42] Article 8 of the European Convention on Human Rights.

[43] European Court of Human Rights, Ivashchenko v. Russia, case 61064/10.

necessary in a democratic society. The condition of being necessary in a democratic society must be assessed in the context of the individual case, focusing on the person whose privacy is being infringed upon and the crime being investigated. The crucial question regarding the topic at hand arises concerning the condition of the investigative task being in accordance with the law. While a cross-border investigative measure may comply with the conditions and procedures stipulated in national legislation, the legality of such an action under international law is questionable, as international law generally prohibits the arbitrary intervention of national authorities into foreign territories. Ultimately, actions contrary to the provisions of international conventions which the signatory states have ratified, such as the Budapest Convention, which specifically regulates various forms of cross-border acquisition of digital evidence, cannot be considered actions in accordance with the law.

Up until this point, we have discussed the negative obligation of the state to refrain from infringing on the right to privacy. Now, we must also consider the positive obligation. The right to privacy requires not only that national authorities abstain from unjustified intrusions into privacy but also that they protect individuals from such intrusions by taking appropriate measures to ensure respect for their right to privacy.[44] Accordingly, states must act to prevent unjustified intrusions into privacy within their territory.[45] In the context of investigative actions by other states, several questions arise, including where the intrusion into an individual's privacy actually occurs (whether it is linked to the location where their data is stored). Here, the primary guiding principle can be the conditions for establishing jurisdiction for prosecuting cybercrime. According to the first paragraph of Article 22 of the Budapest Convention, each party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over crimes established in this convention, when they are committed in its territory. However, determining whether a crime occurred within the territory of a particular state is often difficult if the crime was committed in cyberspace. Therefore, jurisdiction for prosecuting cybercrime often needs to be determined based on other factors, such as the nationality of the perpetrator and the victim, as well as the impact of the cybercrime on the interests and security of the state.[46] This

---

[44] European Court of Human Rights, "Guide on Article 8 of the European Convention on Human Rights," accessed 9.4.2024, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.

[45] Similarly, Directive 2013/40/EU of 12 August 2013 stipulates this as well, with the addition that it was committed by their citizen.

[46] "Sovereignty and jurisdiction," E4J University Module Series: Cybercrime, Module 7: International Cooperation against Cybercrime.

last factor is perhaps the most important, as the security and integrity of information systems within a state are certainly in its interest, especially from the economic perspective of trust in locally based digital services and the protection of national security from the perspective of state information systems.

4. The legal fiction of the location of evidence

From a purely technical standpoint, the location of digital evidence is clear as it shares the location with the medium on which it is stored. This position is confirmed by international legal instruments which regulate special types of cross-border acquisition due to the recognition of the problem related to the technical location of digital evidence. The logical basis for such regulation, founded on international consensus, is the acknowledgment that the issue in conducting such investigations pertains to state jurisdiction. Nonetheless, we discuss the concept of remote access which inherently recognizes the source (another device) and thus the location of the evidence on that remote device. By acknowledging the technical location of the evidence and the related jurisdictional aspect, the focus shifts from whether law enforcement agencies can obtain evidence abroad to when and how they can do so. Addressing this question can clarify the legal pathway for legitimate acquisition and allow for constructive critiques to improve these procedures while respecting the rights of the accused and the territorial sovereignty of individual states while pursuing the goal of effective prosecution of crime.

Based on the aforementioned points and a review of various methods of international acquisition of digital evidence, we can identify three types of digital evidence locations, as sensibly defined through the lens of jurisdiction and the process of their acquisition. The location of digital evidence as tied to the location of the storage unit where the sought data is stored, the location of the provider of the digital service within which the data is stored, and the location from which the data content can be accessed.

5. The location of digital evidence as tied to the location of the storage unit

The determination of the location of digital evidence based on the location of the device on which it is stored is accurate from a strictly technical perspective, as it is based on the only actual physical manifestation

of digital content in the form of a "record" on a physical medium. This approach is practical from the standpoint of pure determinability, as tying the location of digital evidence to a physical, tangible object limits the ambiguous nature of digital evidence and its associated problems. By linking the evidence location to a specific physical device, we assign a temporally and spatially stable location to the data content based on which we can ascertain the specific jurisdiction or lack thereof of the authority obtaining the evidence, which consequently allows us to determine who is actually authorized to obtain a certain piece of evidence. This subordinates the acquisition of digital evidence to the rules of seizure, requests for cooperation, and investigations of objects and information abroad, which are largely adequately defined by the laws of international police, prosecutorial, and judicial assistance. Although the flow of data in the digital domain is largely territorially unrestricted, criminal prosecution is still limited to national borders according to the aforementioned judgment in the *Lotus* case. [47] This makes the acquisition of data, which is often stored abroad, significantly constrained by other states' territorial sovereignty.[48] Therefore, various instruments of cross-border cooperation represent an extremely reliable solution, as they help avoid potential jurisdictional conflicts. For this reason, such a determination of location, and, consequently, international cooperation in obtaining digital evidence, can be considered a 'safe bet.'

The Budapest Convention on Cybercrime sensibly addresses the location of digital evidence. In the first paragraph of Article 19, which regulates the search and seizure of stored computer data, it is clearly stipulated that each state must adopt legislative and other measures to enable its law enforcement authorities to search or similarly access a computer system or part of it, as well as computer data stored therein and a computer-data storage medium in which computer data may be stored in its territory. The addition that such powers are defined for the territory of each state seems self-evident and unnecessary at first glance due to the general understanding of the territorial jurisdiction of law enforcement authorities. However, from the perspective of the convention's purpose, clearly outlined in the preamble,[49] which highlights the need for international cooperation and a joint fight due to the very nature of cybercrime and the consequently related nature of digital evidence, the provisions of this

---

[47] Sachoulidou, "Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation," 70.

[48] Sieber and Neubert, "Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty," 252–253.

[49] ?????????????

convention addressing specific prosecutorial actions, in the absence of the added limitation "in its territory," could lead to interpretations of cross-border jurisdiction of law enforcement authorities of individual states. It is difficult to imagine a legal order that would allow law enforcement authorities of one country to cross the border into another country and, for the purpose of criminal proceedings, seize an electronic device from an individual and secure its data content on the territory of the other country. This provision in question does not only refer to the physical seizure of an electronic device and the consequent securing and examination of its data content but must also be understood in the context of remote access.

The addition of "in its territory" clearly limits the jurisdiction of each state's law enforcement authorities within the confines of their territory. This not only promotes and sensibly enables actual and effective international cooperation but also appropriately defines the location of digital evidence as tied to the physical device on which the data is stored. Anchoring the location to the physical storage medium and its location establishes the concept of a "true source" of the obtained evidence, which, due to international cooperation and the consequent agreement on the actual location of the evidence by the law enforcement authorities of both countries, attains a certain institutional level of authenticity. The physical location of the acquisition or discovery of the evidence is now clearly known, which (at least theoretically) allows for a satisfactory level of examination of the legality and acquisition of the evidence and its probative value.

The notion of location, as tied to the storage unit, is further emphasized in the second paragraph of Article 19 of the Budapest Convention, which stipulates the investigation of a remote device that is lawfully accessible from the initially investigated device and contains the content sought . This type of investigation is also limited by the condition that the other, albeit remote, device, which the police would access via the initially investigated (and seized) device, is located within the territory of the investigating authority. In this case, the concretization of the location of digital data in accordance with the location of the storage device is even more evident, as it directly addresses remote access.

6. Doubt about the location

When considering the technical location of digital evidence, that is, the location of the storage unit, we encounter an important question: what is the appropriate procedure in situations where investigators do not

exactly know where the remotely accessed storage unit (e.g., a server) is located. The situation in which the investigators do not know the location of the storage unit is referred to as "loss of location" or "loss of knowledge of location". Such situations raise the question of whether the investigative authority should refrain from obtaining and examining digital evidence if it is in doubt about whether it can obtain it due to territorial jurisdiction or because it does not know which country would have jurisdiction for obtaining it within the framework of international assistance. [50] In line with the posed question, contentious cases arise where the police would not know whether they have the jurisdiction to obtain certain digital evidence due to the lack of knowledge of its location but would obtain it nonetheless. This is an extremely problematic situation as it is often difficult to determine the location of remote devices on which data is actually stored.

If the police obtained evidence outside their territory, they obtained it illegally. This conclusion is based on the general understanding of the national jurisdiction of investigative authorities and the consequent prohibition of infringing on the sovereign jurisdiction of other states, as derived from the previously mentioned *Lotus* case. Within the given assessment, police conduct in doubtful situations must be analysed from the perspective of the Exclusionary Rule. We will not determine here whether evidence obtained by the police from devices located in other countries without proper legal basis must necessarily be excluded from proceedings as this issue is regulated differently in various countries. The need to exclude evidence is assessed based on rules developed in different countries according to their specific historical, cultural, and institutional values.[51] The European Court of Human Rights (ECHR), in its decisions, also does not assess whether evidence obtained illegally under domestic law is admissible but whether the overall procedure, including the method of obtaining evidence, was fair. In doing so, it considers not only the illegality of obtaining the evidence but also the nature of the violation of any convention rights. In this context, the court also examines whether the defence was given the opportunity to challenge the authenticity of the evidence and oppose its use, as well as the quality of the evidence.[52]

---

[50] Sieber and Neubert, "Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty," 246–247.

[51] Michele Panzavolta, Elise Maes and Anna Mosna. " Streamlining the exclusion of illegally obtained evidence in criminal justice," 4, accessed April 25, 2024, https://www.law.kuleuven.be/linc/english/research/Panzavolta_Streamlining_The_Exclusion_Of_Illegally_Obtained_Evidence_In_Criminal_Justice.

[52] European Court of Human Rights, Bykov v. Russia, case 4378/02, par. 89–90.

The question at hand is how an investigator should act when they are not sure where the remote device is located. Considering that the problem of illegally obtained evidence is (if necessary and appropriate) resolved using the Exclusionary Rule, it is only reasonable to examine this problem from the standpoint of this rule. The Exclusionary Rule is meant to prevent, not to repair, legal shortcomings in the process of a criminal investigation by compelling law enforcement to act according to the law and by removing the incentive to disregard it. [53] The exclusion of illegally obtained evidence in such a manner could be examined from the standpoint of the reliability principle (whether the manner in which the evidence was gathered has tainted its reliability), the deterrence principle (preventing investigators from committing improprieties by prohibiting the use of the fruits of these acts to secure a conviction), the protective rationale (exclusion serves as a remedy for the violation of defendants' rights), and moral legitimacy (in accordance with the need to appear legitimate in the eyes of the public).[54] It is only reasonable to consider the deterrence principle applicable in cases when law enforcement does not know if the actions they are about to execute are in fact legal. Infringements on individual rights and territorial privacy constitute illegal actions, which are only lawful under specific conditions. If law enforcement authorities are not certain that their actions meet the necessary conditions, they must assume that their actions are illegal based on the presumption of conditional legality. This stance is valid because, under this principle, we aim to prevent arbitrary and inappropriate behaviour of law enforcement. Accordingly, we can also refer to the protective rationale under which we seek to protect individuals' rights against unjustified intrusions since, when law enforcement is unsure of the justification of their actions, a higher number of rights violations can reasonably be expected. From the standpoint of moral legitimacy, we can also argue that reckless and dubious behaviour by law enforcement, when unsure of the legality of their actions, cannot inspire public confidence in the criminal justice system. Perhaps, the most problematic aspect of the discussed topic is the reliability principle. As previously mentioned, the proper determination of the source, which reasonably includes its location, is crucial for assessing the evidentiary value of digital evidence. There is a legitimate argument to be made that the reliability of the obtained evidence can be reformed by the subsequent determination of the source's location. However, it is entirely possible that

[53] Justia, "The Foundations of the Exclusionary Rule," accessed May 25, 2024, https://law.justia.com/constitution/us/amendment-04/34-the-foundations-of-the-exclusionary-rule.html

[54] Panzavolta, Maes and Mosna. "Streamlining the exclusion of illegally obtained evidence in criminal justice," 79–82.

the subsequent determination will be dubious or that its credibility will be compromised. Nonetheless, taking into account various aspects of the exclusionary rule, we can certainly conclude that it would be appropriate for law enforcement authorities to refrain from investigating remote electronic devices if they do not know in which state they are located

Regardless of the credibility of the subsequently determined location of the evidence source (or its location), it is problematic for law enforcement to determine the legality of their actions only after they have already been carried out as they have already infringed on individual rights and the territorial sovereignty of another state. Furthermore, the subsequent determination of the legality of the obtained evidence is problematic because the timely exclusion of illegal evidence is essential to prevent it from being deeply embedded in the investigation, making its negative effects impossible to fully remove later in proceedings. It becomes impossible to trace what later obtained evidence was gathered as a result of it.[55] If the location of the source was not known beforehand, it is questionable whether proper subsequent verification is even possible. In the "overall fairness" test of the ECHR, within the assessment of whether the applicant was given an opportunity to challenge the authenticity of the evidence and oppose its use, it is unfortunately often overlooked whether the defence and the court had sufficient information about the circumstances of the evidence's acquisition to assess whether it was obtained legally.[56] It is certainly difficult to support the position that the defendant (in most cases) is effectively capable of challenging the legality of the obtained evidence from the perspective of its location, if determining the location of storage devices poses a significant challenge for law enforcement authorities. In line with this, it is certainly essential that, from the perspective of the principle *in dubio pro reo*, the burden of proof regarding the location of storage devices falls on the shoulders of law enforcement authorities. However, this raises questions about the actual technical ability to prove the location of the accessed device beyond a reasonable doubt in cases where a digital piece of evidence is located on multiple storage devices in different locations. This is just one of the reasons why tying the location of digital evidence to the location of the storage device is not always practical, especially in cases of cloud storage solutions and other digital services that use multiple servers but give the impression of a unified ac-

[55] Fair Trials, "Unlawful evidence in Europe's courts: principles, practice and remedies," accessed June 25, 2024, https://www.fairtrials.org/app/uploads/2021/11/DREP-report.pdf, 42.

[56] Fair Trials, "Unlawful evidence in Europe's courts: principles, practice and remedies," 43–44.

cess point. This logically leads us to the next approach to determining the location of digital evidence.

7. Location of the Storage Service Provider

Another definition of the location of digital evidence from the perspective of its acquisition is tying the location of the evidence to the location of the provider of a service, within which the data is stored on a device remote from the user, typically a server. This approach departs from recognizing the actual physical location of data as electrical impulses on a physical medium, moving towards a concept that ties the location to the possibility or legitimacy of accessing the device where the data is stored. This concept acknowledges that storage units or, predominantly, servers where the data sought is located are not necessarily in the same location or under the same jurisdiction as the service providers operating on these servers. However, it focuses on providers' technical capability and, more importantly, their legal right to access these systems and consequently obtain the data. By conditioning the acquisition of evidence on the location of the service providers, the actual location of the data or servers becomes irrelevant, since law enforcement authorities do not intrude into these remote systems. This approach skilfully exploits a unique characteristic of digital evidence: the possibility of obtaining it through a third party, the digital service provider.[57]

A clear example of tying the location of digital evidence to the location of the service provider is the request for the preservation and production of electronic evidence in accordance with the E-evidence Regulation. This regulation, together with The Directive on harmonised rules for the designation of establishments and appointment of legal representatives for electronic evidence[58], represents the "EU e-evidence package," which establishes a framework within which EU member states can directly request digital evidence from digital service providers in other member states, thereby bypassing traditional channels of mutual legal assistance. [59]

---

[57] Sachoulidou, "Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation," 83.

[58] 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.

[59] Anže Erbežnik, " A new EU system on cross-border gathering of e-evidence - analysis and open questions ," *Digitas*, no. 98 (2023): 47.

The Regulation on Production and Preservation Orders for electronic evidence establishes rules under which a competent judicial authority in the Union, in criminal proceedings including criminal investigations or for the execution of a custodial sentence or a security measure involving deprivation of liberty following a criminal procedure, can, in accordance with this regulation, require a service provider offering services in the Union to produce or preserve digital evidence based on a European Production Order or a European Preservation Order.[60] This constitutes an important instrument for obtaining digital evidence related to online services when the service provider has a designated business unit or legal representative in another member state. Besides the location restriction, the use of this regulation is also limited to data related to the service provided by the service provider within the Union.[61] Offering services in the Union relates to enabling the use of the service by both individuals and legal entities in one or more member states, where mere accessibility of the interface in the Union is not sufficient. To satisfy the condition of "offering services in the Union," there must also be a significant connection to the Union, which exists when the provider has a business unit in a member state or is based on other specific factual criteria, such as having a significant number of users in one or more member states or targeting the service[62] towards one or more member states.[63]

While the previously adopted Directive on the European Investigation Order[64] is based on the principle of mutual recognition of judgments and judicial decisions, the acquisition of electronic evidence has, up until the adoption of the E-evidence regulation, relied on voluntary and direct cooperation between foreign service providers, national law enforcement and judicial authorities. This method of obtaining evidence represented a faster and less bureaucratic alternative compared to international legal assistance, which is why it became a popular practice. Despite its general effectiveness, this method did not always guarantee successful outcomes

[60] Recital 18 of the E-evidence Regulation (Regulation (EU) 2023/1543).

[61] Recital 26 of the E-evidence Regulation (Regulation (EU) 2023/1543).

[62] Whether a provider targets their service at one or more Member States can be assessed based on whether the service includes localization of the language for individual Member States, uses the currency of the Member States, enables the ordering of goods or services in the Member States, has an application related to the service available in app stores of a specific Member State, advertises the service in a specific Member State in the language of that Member State, and offers customer support in a specific Member State.

[63] Recital 29 and 30 of the E-evidence Regulation (Regulation (EU) 2023/1543).

[64] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

for cooperation requests.[65] Before the E-evidence regulation, direct cooperation with foreign service providers was not formally regulated in most member states.[66] The formal regulation of this method of cross-border acquisition of digital evidence represents a critical shift towards transforming informal cooperation into formalized cooperation, thereby providing a predictable and reliable instrument for cross-border evidence acquisition. This method of obtaining evidence through direct cooperation with service providers does significantly limit the national sovereignty of the state where the service provider is located. However, such a limitation of sovereignty, due to its formal regulation by an internationally valid act or regulation, aligns with the principle of international sovereignty as described in the aforementioned *Lotus* case regarding the cross-border exercise of state authority.[67] Despite its formal regulation and compliance with established aspects of international law, it is important to emphasize that this method of evidence acquisition raises significant questions regarding the sovereignty and territoriality of the involved states, as well as the protection of human rights, particularly in terms of privacy and data protection.[68] This kind of intrusion into human rights without the knowledge or objection of the state where the service provider is located, through the introduction of extraterritorial application of legislation, redefines the national and territorial sovereignty of the involved states. [69]

This approach of tying the location of digital evidence and, thus, the jurisdiction for obtaining it to service providers is also present in the U.S. Cloud Act[70], which was enacted in 2018, prior to the E-evidence regulation, with the explicit aim of reducing delays associated with MLAT[71] requests for obtaining digital evidence. This law primarily enables U.S. law enforcement authorities to access data held by communications service providers in the USA regardless of where the data is actually stored. Additionally,

---

[65] Tosza, "Gathering Electronic Evidence for Administrative Investigations. Exploring an Under-the-Radar Area" 2–3.

[66] Tosza, "Gathering Electronic Evidence for Administrative Investigations. Exploring an Under-the-Radar Area" 3.

[67] Tosza, "Gathering Electronic Evidence for Administrative Investigations. Exploring an Under-the-Radar Area" 10.

[68] Erbežnik, "A new EU system on cross-border gathering of e-evidence - analysis and open questions ," 47.

[69] Erbežnik, "A new EU system on cross-border gathering of e-evidence - analysis and open questions ," 50.

[70] Clarifying Lawful Overseas Use of Data Act (The CLOUD Act), Pub. L. 115-141, div. V, Mar. 23, 2018, 132 Stat. 1213.

[71] An MLAT or mutual legal assistance treaty is an agreement between two or more countries for the purpose of gathering and exchanging information for the purpose of enforcing public or criminal laws.

the Cloud Act establishes a framework for bilateral international agreements with other countries under which they can mutually request and obtain digital evidence from service providers located in the territories of the signatory states. The first such agreement was concluded by the USA with the United Kingdom in 2019, under which U.S. and British law enforcement authorities, having obtained the appropriate authorization, can request digital evidence related to serious crimes, such as terrorism, child sexual abuse, and cybercrime, from technology companies located in the other signatory state.[72] The content of this agreement, regarding the essential concept of cross-border evidence acquisition from digital service providers, is therefore largely similar to the E-evidence regulation, but functionally much more limited.

8. The location of access

There is an idea to resolve the issue of the legality of remote access to a device (in some cases) through the reasonable application of procedural provisions and practices related to the lawful entry of the police into a private residence without a prior court order, provided that the resident invites the police into their premises or consents to it.[73] This involves considering reasonably the voluntary surrender of the username and password as an invitation for the police to enter a private space.[74]

The legality of police access to a remote device and the subsequent investigation, when based on the consent of the user of that remote service, is reasonable as it excludes two grounds for disputing such an investigation. The first stems from the perspective of communication privacy as it is not violated if the individual, who reasonably expects privacy over the data content in question, consents to disclose this data content to the police, thereby indirectly revealing it to this limited extent and consequently relinquishing their privacy over specific content. The second reason concerns the legality or illegality of the access or entry into the system itself. Unauthorized access is not an issue if the person accessing the system has

[72] Evand Norris and Morgan J. Cohen, "How US Authorities Obtain Foreign Evidence in Cross-Border Investigations." *New Global Investigations Review*, (2020), accessed June 27, 2024. https://globalinvestigationsreview.com/review/the-investigations-review-of-the-americas/2021/article/how-us-authorities-obtain-foreign-evidence-in-cross-border-investigations.

[73] In accordance with Article 218 of the Slovenian Criminal Procedural Code, police officers may enter another person's apartment and other premises and, if necessary, conduct a search without a court order, if the occupant of the apartment consents to it.

[74] Bernard, "Problematika pregona računalniškega kriminala in uporabe digitalnih dokazov z vidika državnega tožilstva," 77.

the permission of the owner or user.[75] Since access to the system in this case is based on the permission or consent of the user, it inherently justifies the police's investigative authority in the sense of legally safeguarding their actions or excluding illegality.

The solution, which justifies the location of digital evidence based on the location of access to the data, is also addressed in Article 32 of the Budapest Convention, which allows trans-border access to stored computer data with consent or where publicly available. This article represents the most important provision regarding cross-border evidence collection in the Budapest Convention.[76] It allows a Party to unilaterally access computer data stored in another Party without seeking mutual assistance or without the authorization, thereby remotely investigating data content located on a device in another country. This is permitted in two cases: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. When drafting the Budapest Convention, the authors were aware that it was too early to establish a comprehensive system for unilateral cross-border acquisition of digital evidence. This decision was based on the understanding that, due to the lack of concrete experience and the recognition that appropriate solutions often depend on specific circumstances, it is difficult to formulate general rules. Therefore, they limited this method of free cross-border acquisition of digital evidence to the aforementioned situations and refrained from regulating other situations until concrete experience was gained and further debates were conducted. [77] The complexity and contentious nature of this regulatory area is evidenced by the fact that since the adoption of the Budapest Convention, two additional protocols have been adopted: the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems[78] in 2003, and the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and dis-

---

[75] Šepec, Kibernetski kriminal, kazniva dejanja in kazenskopravna analiza, 63.

[76] Eurojust, "Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers." 1.

[77] Council of Europe: *Explanatory Report to the Convention on Cybercrime*. European Treaty Series – No. 185, 2001, https://rm.coe.int/16800cce5b (accessed 27.7.2024), p. 53.

[78] Council of Europe: *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).

closure of electronic evidence (ETS No. 215)[79] in 2022. However, neither of these protocols added additional cases in which such free or unauthorized acquisition of digital evidence by another state on its territory would be allowed.

First, we must address the cross-border acquisition of digital evidence based on consent. Under this provision of the Budapest Convention, law enforcement authorities of one Party can access and obtain evidence located in another Party, meaning, it is stored on a device in that country, provided they have obtained prior consent from the data owner or processor. Such access to the device located in another country does not require notification of the competent authorities of that country, however the Budapest Convention does not exclude such voluntary notifications.[80] We must consider the key location condition, namely, that such cross-border evidence acquisition is permitted only when the location of the data (where it is stored) is known and is within another Party of the Budapest Convention. This provision does not cover situations where the data is stored in a third country or where the location of the accessed data is unknown or questionable.[81] Based on this, we can assess that this is only a partial approach to tying the location of digital evidence to the access location. In this case, one could say that the jurisdiction as tied to the access location is only functional, not legal. It allows law enforcement authorities (under the condition of consent) remote cross-border access but limits this based on the technical location of the data in certain countries. From a legal perspective, it still completely ties the location of evidence to the location of the storage device, with precise, limited, and reciprocal extension of the investigative territorial jurisdiction under the Budapest Convention. In terms of our legal understanding of where the digital evidence is located, such access in no way affects the conventional unification of the legal and technical location of digital evidence as consistent with the location of the storage unit. This is most evident from the previously described problem of the uncertainty regarding the actual storage location of the data.

The acquisition of evidence in this manner theoretically does not require the use of special law enforcement powers, which, through the concept of consent, suggests that such acquisition does not initially ap-

---

[79] Council of Europe: *Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence* (ETS No. 215).

[80] Even though such notification is not required, the development of this kind of good faith practice would represent a positive step in promoting mutual trust between countries, thereby strengthening cross-border cooperation in criminal prosecution.

[81] Eurojust, " Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers." 13.

pear to constitute repressive state action. This does not mean that the contentiousness of cross-border police actions is excluded. It all relies on the assumption that the obtained consent is genuinely voluntary, making it crucial that the individual giving consent is truly aware that they are not obligated to do so. The question arises as to whether the consent is voluntary if it was obtained during the course of another investigation, such as a house search. It is necessary to consider whether an individual unversed in law understands in such a specific situation that they do not have to provide "consent," or whether other circumstances (such as fear of potential additional costs associated with obtaining the desired data content) influence their will. It is clear that consent for such cooperation in a criminal investigation must be explicit, as a general consent to the terms of use of an online service, allowing access to data by law enforcement, is not sufficient.[82] Service providers of digital services are opposed to such methods of data acquisition for criminal proceedings. For example, Facebook (or Meta) suggests that when law enforcement seeks data related to a user account on the social media platform. If the user has given consent for law enforcement to obtain this data, the user should provide the data to the police themselves using the data transfer function.[83] This is an extremely practical method of obtaining evidence as it excludes the aspect of cross-border investigative actions. Such acquisition might be problematic in terms of ensuring the actual data provided by the user matches that on the specific user account, but this issue could likely be resolved with specific technical verification measures or merely through the formalization of the process, such as the presence of a police officer during the user's data retrieval and the creation of an appropriate record. This could perhaps be conducted within the framework of data preservation or securing procedures, in which the data holder (at least in Slovenia[84]) has the right to be present.

---

[82] Eurojust, " Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers." 13.

[83] Facebook, Help Center, "Information for law enforcement," accessed April 30, 2024, https://www.facebook.com/help/494561080557017.

[84] In accordance with paragraph 4 of Article 223.a of the Slovenian Criminal Procedure Act, the owner and any known and reachable user of the device are invited to be present themselves, through their representative, lawyer, or expert during the preservation of the data.

9. Open source evidence

With the increasing use of digital evidence, the application of open-source investigations (OSINT) or investigations based entirely or partially on publicly accessible information or digital evidence, is coming to the forefront. Such information represents a new and unregulated, yet critical, form of evidence in modern criminal proceedings. [85] In these procedures, open-source information is obtained or collected for evidentiary purposes. This information is accessible to the general public or available for purchase or request by anyone. Open-source information in a digital form is predominantly accessible via the internet and encompasses both user-generated and machine-generated data. [86] It is necessary to clarify the term user-generated data or content. Although the term itself, when directly explained, is understood as content created by users of a particular service, which can be interpreted as evidentiary content not merely resulting as a byproduct of users' actions but intentionally created content published to inform the broader public, in the era of popular discussions about generative artificial intelligence, it is important to emphasize that this does not (or does not only) refer to the content created using such generative AI systems. This emphasis is important because the use of generative AI is currently a frequently highlighted topic in the media, and within the legal community, discussions on digital topics often encounter the misuse of popular terms and awkward, non-substantive translations.

Open-source information encompasses data that anyone can access without a special legal status or the use of an unauthorized access. It contrasts with closed-source information where access is restricted or legally protected and is available through private channels. A good indicator of the type of content is that open-source content does not require interaction with or the obtaining of information from individual internet users. [87] This distinction becomes somewhat questionable in the case of interest groups on social networks which are formally of a closed nature but effectively accept anyone upon a request to join that requires only the press of a button without substantive interaction with another person. On one

---

[85] White, "Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism,"

[86] The Office of the United Nations High Commissioner for Human Rights (OHCHR) and the Human Rights Center at the University of California, Berkeley, School of Law, "*Berkeley Protocol on Digital Open Source Investigations,*" accessed July 15, 2024, https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf, 3.

[87] Berkeley, School of Law, *Berkeley Protocol on Digital Open Source Investigations, p.* 6.

hand, some authorization is required, but it is of such a nature that it does not effectively exclude the condition that anyone can access its content. This represents a form of apparent selection or limitation. In such cases, the acquisition of data by law enforcement should be assessed based on whether the investigator used a fake profile created for this purpose, and the assessment of such cases should also consider national rules on covert investigative measures.

A major problem with the use of open-source evidence is the lack of consistent mechanisms for their collection. Standardized mechanisms or the standardization of the use of specific evidence improve the quality of investigations by including the verification of the authenticity and reliability of the evidence as well as its integrity. To verify the authenticity of open-source evidence, both internal indicators such as geolocation and metadata, as well as external indicators such as the source and chain of custody, are often examined. [88]

The acquisition of open-source evidence is already permitted by the Budapest Convention which in Article 32 stipulates that a Party may, without the authorization of another Party, access publicly available (open-source) stored computer data, regardless of where the data is located geographically. This represents an important exception, in addition to obtaining data located in another signatory state based on the consent, as it ties the location of digital evidence to the location of access. This method of acquiring digital evidence, therefore, pertains to any publicly accessible data that, from a technical perspective, is located on foreign territory. In this context, law enforcement authorities can subscribe to services available to the public and download, mirror, or otherwise secure the accessed data, without needing the permission of the country where the electronic device storing the data is located. [89] An important difference from the previously mentioned acquisition based on consent is the absence of the condition that the accessed data content must be stored on a device located in another signatory state of the Budapest Convention. This represents an absolute realization of the concept of tying the location of digital evidence to the location from which the data content is accessed, while entirely disregarding the location where the storage device is located and the associated aspect of jurisdiction. The acquisition of such evidence in itself does not constitute an act that would otherwise be unlawful unless exceptionally permitted in criminal proceedings. This provision of

[88] White, "Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism,"

[89] Eurojust, "Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers." 2–3.

the Budapest Convention simply allows law enforcement authorities to engage in actions that are not contentious when performed by civilians, with this provision further excluding the unlawfulness of cross-border law enforcement investigative actions.

The acquisition and use of open-source evidence can represent an intrusion into the right to privacy, which is why it is recommended that investigators obtain the consent of the author of the content that constitutes such evidence. However, this is often extremely difficult due to the challenge of determining the true identity of the author. [90] The prevailing view aligns with the established idea that people enjoy a certain level of privacy even regarding publicly accessible material they have published themselves. Perhaps the most recognized example of this approach is the restricted use of photographs from social networks for facial recognition. Interpol's evidence recognition system, for instance, is based on comparing facial profiles that are pre-stored in their system.[91] Similarly, the use of the Face Trace system by the Slovenian police is limited to comparing photographs and composite sketches from the police database of photographed persons, as confirmed by the Information Commissioner of the Republic of Slovenia in an inspection procedure.[92]

The use of open-source evidence is established in the international criminal law, with the ICC taking the position that although Article 69(7) of the Rome Statute of the International Criminal Court[93] stipulates that evidence obtained in violation of human rights, such as the right to privacy, may be inadmissible, such a violation affects the reliability of the evidence only if respecting the violated right would have influenced the content of the evidence. In the case of evidence obtained from open sources, the intrusion into privacy in most cases, from the perspective of ICC practice, would likely not affect its admissibility.[94]

---

[90] White, "Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism,"

[91] Forensics, Interpol, "Facial Recognition," accessed April 26, 2024 https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition.

[92] Although the Face Trace police system is based on biometric processing of personal data, it does not enable identification. Informacijski pooblaščenec, "Policijski sistem Face Trace," accessed August 1, 2024, https://www.ip-rs.si/novice/policijski-sistem-face-trace-sicer-temelji-na-biometrični-obdelavi-osebnih-podatkov-a-ne-omogoča-identifikacije.

[93] International Criminal Court, *Rome Statute of the International Criminal Court*, 1998.

[94] White, "Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism,"

This raises the question of when a violation of the right to privacy affects the content of the evidence. In the case of a photograph or video recording that itself demonstrates an important fact and has intrinsic evidentiary value, and is, therefore, used independently in the evidentiary process, a potential intrusion into privacy does not alter its content. However, when certain photographs lack independent evidentiary value and do not independently demonstrate a relevant fact but are used solely for analytical purposes, such as in the case of facial recognition systems, this type of intrusion into the right to privacy certainly alters their content as it creates their evidentiary significance through the analysis itself.

10. Conclusion – the development of a shared digital investigative territory

The location of digital evidence is a critical aspect in determining the legality of the procurement of such evidence as it determines the jurisdiction of law enforcement authorities to exercise state power in the context of criminal proceedings by infringing upon the rights of individuals and organizations. The boundless nature of the digital world, due to established international legal concepts of territorial jurisdiction and the related prohibition on exercising state power beyond national borders, significantly complicates the acquisition of crucial evidence. Successful prosecution of crime (especially cybercrime) increasingly requires close cooperation not only among cybersecurity experts, digital forensic experts, and legal professionals but also among law enforcement agencies of different countries as this is the only way to prevent the exploitation of jurisdictional gaps by criminals.[95]

While direct and unilateral investigative measures in foreign countries constitute clear violations of international law, accessing digital evidence via an internet connection presents a more complex situation. The global and intangible nature of the internet reduces the significance of national territories.[96] The elusive and often changing location of digital evidence poses not only a significant problem for modern criminal investigations but also challenges the practicality and rigidity of traditional concepts of

---

[95] O. Oladipupo Amoo, A. Akoh Abrahams, T, Oluwaseun Farayola, O, Ajoke, O, Femi, A. Benjamin Samson: *The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system*. "World Journal of Advanced Research and Reviews" 2011, no. 2, p. 213.

[96] Sieber and Neubert, "Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty," 249.

strict territorial jurisdiction. However, these concepts remain valid and for good reason. It is difficult to imagine a practice where states would partially relinquish their sovereignty over law enforcement within their own territories. Instead, we see a rapid development of mechanisms for international cooperation that more or less solve the problems of cross-border acquisition of digital evidence without (at least theoretically) infringing on the territorial sovereignty of another state. While these cooperation systems provide a partial solution to the described problems, they are often slow, and their use depends on investigators knowing where the evidence is located. Additionally, the prosecuting state must either have an agreement with the state where the evidence is located, or both must be members of the same international organization that governs such measures.

With the growing consensus among countries regarding international cooperation in criminal prosecution and the gradual acceptance of certain direct cross-border investigative actions, the development of some sort of »shared digital territory« can be expected in the future. Although this idea currently seems rather fantastical and difficult to achieve from both legal and political perspectives, it is not entirely impossible. Before the terrorist attack in the United States on September 11, 2001, achieving consensus among EU member states in the field of criminal law was difficult, and efforts were predominantly focused on protecting the financial interests of the Union in connection with organized crime. However, after the mentioned attack, willingness among the member states to reach consensus on unified or joint measures emerged, aiming for swift, effective, and repressive action.[97] The introduction of the European Arrest Warrant abolished specific criminal law protectionism for citizens of individual member states within the EU by removing the prohibition on extraditing their own citizens.[98] Following this gradual development of cross-border criminal action, both the adoption of the Budapest Convention and the recent EU Digital Evidence Package have opened the door to the concept of a shared digital territory. By recognizing the issues of cross-border evidence acquisition in connection with the specific properties of digital evidence, these measures have regulated or permitted certain cross-border police investigative actions.

Based on the aforementioned, it is, of course, questionable how (if at all) international criminal cooperation or perhaps even a shared digital territory will continue to develop. It might move towards an ac-

[97] Katja Šugman Stubbs and Primož Gorkič, *Evropski nalog za prijetje in predajo: teoretični in praktični vidiki* (Ljubljana: GV Založba, 2010), 21–22.

[98] Šugman Stubbs and Gorkič, *Evropski nalog za prijetje in predajo: teoretični in praktični vidiki*, 28–29.

tual shared territory, following the principle of location tied to the access point whereby law enforcement within this territory could freely (with the appropriate legal basis and in accordance with prescribed procedures) obtain digital evidence, just as they would within their own country. This direction would be ideal for the efficiency of law enforcement, however, it is the most problematic. It would certainly require consistent harmonization of such investigative procedures and key safeguards against the abuse of individual rights. For the proper functioning of such a territory and the maintenance of mutual trust, it would likely be necessary to prohibit cross-border investigations of electronic devices used by state authorities, institutions, companies, or other managers of critical state infrastructure.[99] Realistically, through international agreements, such as those based on the previously mentioned American Cloud Act, we can expect an increasing recognition of the concept of the location of digital evidence as being tied to the service provider, and thereby an agreement on the direct cross-border acquisition of evidence from these providers. Given that such evidence acquisition is now regulated within the EU among member states, and that the USA has MLATs signed with more than 70 countries, including all EU members,[100] it is expected that this method of cross-border digital evidence acquisition will be regulated in the relatively near future at least between the USA and EU member states. How, if at all, broader global coordination of cross-border cooperation in criminal prosecution will proceed, only time will tell. Such coordination will be subject to the alignment of different legal traditions, cultural values, and political systems. [101] On the other hand, we can expect the exact opposite: the development of practices where countries, disregarding the existing concept of territorial sovereignty, arbitrarily acquire digital evidence located in other countries.

---

[99] It is difficult to imagine, for example, a regulation that would allow law enforcement agencies of one country to legally access the information system of another country's ministry remotely and obtain stored data content there, based on an order from a judge in their own country, for the purpose of their own criminal investigation.

[100] Norris and. Cohen, "How US Authorities Obtain Foreign Evidence in Cross-Border Investigations."

[101] Olukunle Oladipupo Amoo, Akoh Atadoga, Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Femi Osasona and Benjamin Samson Ayinla, " The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system." *World Journal of Advanced Research and Reviews*, vol. 21, no. 2 (2011): 212.

Bibliography

Amoo, Olukunle Oladipupo, Atadoga, Akoh , Abrahams , Temitayo Oluwaseun, Farayola, Oluwatoyin Ajoke, Osasona, Femi and Ayinla, Benjamin Samson. " The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system." *World Journal of Advanced Research and Reviews*, vol. 21, no. 2 (2011): 205-217.

Tosza, Stanislaw, " Gathering Electronic Evidence for Administrative Investigations. Exploring an Under-the-Radar Area", *eucrim*, no. 0 (2024): 1-19.

Berkeley Protocol on Digital Open Source Investigations. New York and Geneva: the Office of the United Nations High Commissioner for Human Rights (OHCHR) and the Human Rights Center at the University of California, Berkeley, School of Law, 2022. https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

Bernard, Janja. "Problematika pregona računalniškega kriminala in uporabe digitalnih dokazov z vidika državnega tožilstva," In *Digitalna forenzika v kazenskih postopkih*, edited by Liljana Selinšek, 65-86. Ljubljana: GV Založba, 2008.

Council of Europe, "Explanatory Report to the Convention on Cybercrime." European Treaty Series – No. 185. November 23, 2001. https://rm.coe.int/16800cce5b

Currie, Robert J. " Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the 'Next Frontier'?". *Canadian Yearbook of international Law*, vol. 54 (2017): 63-97.

White, Elizabeth. "Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism," *Leiden Journal of International Law*, vol. 37, no. 1 (2024): 228-250, accessed April 19, 2024. https://www.cambridge.org/core/journals/leiden-journal-of-international-law/article/closing-cases-with-opensource-facilitating-the-use-of-usergenerated-opensource-evidence-in-international-criminal-investigations-through-the-creation-of-a-standing-investigative.

Erbežnik, Anže, " A new EU system on cross-border gathering of e-evidence - analysis and open questions," *Digitas*, no. 98 (2023): 47-72.

Eurojust, " Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers." January 23, 2024. https://www.eurojust.europa.eu/sites/default/files/assets/trans-border-access-to-stored-computer-data-under-article-32-of-the-budapest-convention-on-cybercrime-and-extraterritorial-powers-23-01-2024.pdf

European Court of Human Rights, "Guide on Article 8 of the European Convention on Human Rights". Accessed April 9, 2024. https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng

Evan Norris and Morgan J Cohen, "How US Authorities Obtain Foreign Evidence in Cross-Border Investigations," *Global Investigations Review*, (2023). Accessed May 28, 2024, https://globalinvestigationsreview.com/review/

the-investigations-review-of-the-americas/2021/article/how-us-authorities-obtain-foreign-evidence-in-cross-border-investigations

Gonzales, Alberto R., Schofield, Regina B. and Hagy, David W. "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors." Washington: U.S. Department of Justice, Office of Justice Programs, 2007. https://www.ojp.gov/pdffiles1/nij/211314.pdf

Linyz, Adjoa. " The Attorney–Client Privilege and Discovery of Electronically-Stored Information." *Duke Law & Technology Review*, vol. 10, no. 1 (2011): 1-18.

Antonis, Michalas and Kassaye Yitbarek, Yigzaw, " LocLess: Do you Really Care Where Your Cloud Files Are?." IEEE International Conference on Cloud Computing Technology and Science, Luxembourg: The Institute of Electrical and Electronics Engineers (2016): 515-520.

NIST, "Digital Evidence Preservation. Considerations for Evidence Handlers," September 2022, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf.

Norris, Evand and Cohen, Morgan J. "How US Authorities Obtain Foreign Evidence in Cross-Border Investigations." *New Global Investigations Review*, (2020). Accessed June 27, 2024. https://globalinvestigationsreview.com/review/the-investigations-review-of-the-americas/2021/article/how-us-authorities-obtain-foreign-evidence-in-cross-border-investigations.

Panzavolta, Michele, Maes, Elise and Anna Mosna. " Streamlining the exclusion of illegally obtained evidence in criminal justice." Accessed April 25, 2024. https://www.law.kuleuven.be/linc/english/research/Panzavolta_Streamlining_The_Exclusion_Of_Illegally_Obtained_Evidence_In_Criminal_Justice.

Policijski sistem Face Trace sicer temelji na biometrični obdelavi osebnih podatkov, a ne omogoča identifikacije. Informacijski pooblaščenec, 2021. https://www.ip-rs.si/novice/policijski-sistem-face-trace-sicer-temelji-na-biometricni-obdelavi-osebnih-podatkov-a-ne-omogoca-identifikacije

Selinšek, Liljana. "Digitalna forenzika v kazenskih postopkih." In *Digitalna forenzika v kazenskih postopkih*, edited by Liljana Selinšek, 13-64. Ljubljana: GV Založba, 2008.

Sieber, Ulrich, and Neubert, Carl-Wendelin. "Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty". *Max Planck Yearbook of United Nations Law Online*, vol. 20, no.1 (2017): 239-321.

Sachoulidou, Athina, "Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation," *New Journal of European Criminal Law*, vol. 0, no. 2 (2023): 216-222.

Šepec, Miha. *Kibernetski kriminal, kazniva dejanja in kazenskopravna analiza*. Maribor: Univerzitetna založba Univerze v Mariboru, 2018.

Šugman Stubbs, Katja, Gorkič, Primož. *Evropski nalog za prijetje in predajo : teoretični in praktični vidiki*. Ljubljana: GV Založba, 2010.

Unlawful evidence in Europe's courts: principles, practice and remedies. Fair Trials, 2021, Accessed May 25, 2024 .https://www.fairtrials.org/app/uploads/2021/11/DREP-report.pdf

Legal Acts

Clarifying Lawful Overseas Use of Data Act (The CLOUD Act), Pub. L. 115-141, div. V, Mar. 23, 2018, 132 Stat. 1213

Council of Europe. 1950. "Convention for the Protection of Human Rights and Fundamental Freedoms." Council of Europe Treaty Series 005. Strasbourg: Council of Europe.

Council of Europe. Convention on Cybercrime. Budapest, 23 November 2001. European Treaty Series - No. 185.

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

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters

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

Zakon o kazenskem postopku (Uradni list RS, št. 176/21 – uradno prečiščeno besedilo in 96/22 – odl. US

Case law

Kruglov and others v. Russia. Application No. 11264/04. ECLI:CE:ECHR:2020:0204JUD001126404

Visy v. Slovakia. Application No. 70288/13. ECLI:CE:ECHR:2018:1016JUD007028813

Ivashchenko v. Russia. Application No. 61064/10. ECLI:CE:ECHR:2018:0213JUD006106410

Bykov v. Russia, Application No. 4378/02. ECLI:CE:ECHR:2009:0310JUD000437802

Permanent Court of International Justice. Affaire Du »Lotus« ... = The Case of the S.S. »Lotus.«. Leyde :Société d'éditions A.W. Sijthoff, 1927.

Kolesnichenko v. Russia. Application No. 1956/04. ECLI:CE:ECHR:2009:0409JUD001985604

Internet sources

"Facial Recognition," How we work, Forensics, Interpol, accesed April 26, 2024, https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition.

"File format," Dictionary, Computer Hope, accesed June 26, 2024, https://www.computerhope.com/jargon/f/file-format.htm.

"*open file,*" Encyclopedia, PCmag, accesed April 30, 2024, https://www.pcmag.com/encyclopedia/term/open-file

"Sovereignty and jurisdiction," E4J University Module Series: Cybercrime, Module 7: International Cooperation against Cybercrime, United Nations Office on Drugs and Crime, accesed May 25, 2024, https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html#:~:text=Cybercrime%20jurisdiction%20is%20established%20by,interests%20and%20security%20of%20the.

Facebook, "Information for law enforcement," Help Center, accesed April 30, 2024, https://www.facebook.com/help/494561080557017.

Justia. " The Foundations of the Exclusionary Rule." Accessed May 25, 2024. https://law.justia.com/constitution/us/amendment-04/34-the-foundations-of-the-exclusionary-rule.html

Rouse, Margaret. "File," Technopedia, accessed June 26, 2024, https://www.techopedia.com/definition/7199/file