JUST-2021-JACC

Action grants to support transnational projects
to enhance the rights of persons suspected
or accused of crime and the rights of victims of crime

JUSTICE PROGRAMME

GA No. 101056685

Improving the application of the presumption of iNNOCENce when applying elecTronic evidence

INNOCENT

WP2: Comparative Analysis of data

D2.2 INNOCENT case law analysis

WP2 leader: UNIWERSYTET IM. ADAMA MICKIEWICZA WPOZNANIU (AMU)

Funded by the European Union

This deliverable was funded by the European Union under Grant Agreement 101056685. The content of this report, including views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the European Commission can be held responsible for them.

Acronym	**INNOCENT**
Title	Improving the application of the presumption of iNNOCENce when applying elecTronic evidence
Coordinator	Law and Internet Foundation
GA No.	101056685
Programme	Justice Programme (JUST)
Topic	JUST-2021-JACC
Start	16 May 2022
Duration	24 months
Consortium	Law and Internet Foundation (LIF), Bulgaria Adam Mickiewicz University Poznań (AMU), Poland Human Rights House Zagreb (HRHZ), Croatia Bratislava Policy Institute (BPI), Slovakia CEELI Institute (CEELI), Czechia Science and Research Centre of Koper (ZRS), Slovenia

Dissemination level		
PU	Public	X
SEN	Sensitive, limited under the conditions of the Grant Agreement	
EU - R	RESTREINT-UE/EU-RESTRICTED under Decision 2015/444.	
EU - C	CONFIDENTIEL-UE/EU-CONFIDENTIAL under Decision 2015/444	
EU - S	SECRET-UE/EU-SECRET under Decision 2015/444	
Document version control:		
	Author(s)	**Date**
Version 1	Case Law Data Collection Template: LIF	01/08/2022
	Case Law Data Collection: HRZR	12/10/2022
	Case Law Data Collection: AMU	14/10/2022
	Case Law Data Collection: CEELI	21/10/2022
Version 2	D2.2 first draft: LIF	30/10/2022
	Case Law Data Collection: BPI	10/11/2022
	Case Law Data Collection: ZRS	02/12/2022
Version 3	D2.2 second draft: LIF	19/12/2022
Version 4	D2.2 final version: LIF	04/01/2023

Table of contents

Executive Summary

This report presents analysis of selected case law in criminal matters examining the relationship between the use of electronic evidence and the application of the presumption of innocence. The case law has been selected at national level – Bulgaria, Poland, Croatia, Slovakia, the Czech Republic and Slovenia, and at European level – the Court of Justice of the European Union and the European Court of Human Rights.

The analysis focuses on the progress of the identified national case law through the respective judicial instances and notes on any changes in the indictment and/ or the judicial decision, while commenting on the (non)involvement of expert witnesses/ forensic examiners, the (non)collaboration with electronic and internet service providers, and last but not least the (non)cross-border cooperation. The treatment of the procedural parties is likewise presented. The same approach is applied to the European case law. Conclusions are drawn looking for similarities but also best practices which might find universal application.

Abbreviations

Abbreviations	Descriptions
BG	Bulgaria
CD	Compact Disc
CJEU	Court of Justice of the European Union
CZ	Czechia
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EIO	European Investigation Order
EU	European Union
HR	Croatia
HU	Hungary
IP	Internet Protocol
IT	Information Technology
MSN	Microsoft Network
NIC	National Institute of Chemistry
PL	Poland
SD	Secure Digital
SI	Slovenia
SK	Slovakia
SMS	Short Message Service
USB	Universal Serial Bus

1. Purpose of the case law analysis

The main aim of the current report is to present information on the partner countries – Bulgaria, Poland, Croatia, Slovakia, the Czech Republic and Slovenia, as well as the ECtHR and CJEU case-law relating to the presumption of innocence in the context of using e- evidence. It also focuses on the existing practices and existing/potential challenges in ensuring procedural rights of the persons suspected or accused of crime, in particular the right to be presumed innocent until proven guilty, and its application in regard to the usage of electronic evidence. The purpose of this analysis is also to identify opportunities and barriers to allow the creation of European policy guidelines.

As part of the data collection activities all partners contributed with providing reviews of national case law, basing their analysis on a data collection template (available as Appendix 1). The current document also includes the evaluation of the data collection results for both the domestic and European case law. These outcomes were consequently discussed in an online focus group during which further insights were introduced and deliberated.

2. Data Collection Methods

The data analysed in the current report has been collected via a dedicated template (Appendix 1). This template includes the 7 main sections, each of them covering different aspects of the respective case in order for a detailed review to be achieved:

- The first section “Details of the case” includes the information of the parties, the competent court, the stage of the criminal proceedings, the year of start and end of the criminal proceedings. It acts as an introduction to the case as well as to inform of the stage of the case and the competent court concerned.
- The second field “Facts of the case” describes the crime, and the key facts of the case that are relevant to the use of e-evidence and its impact on the right to fair trial from legal and practical standpoint.
- The next section “The relevant legal issues” includes the key issues in relation to the interpretation of the right to fair trial when applying e-evidence and application of the applicable legal framework. It also covers the provisions which were named in the indictment and those outlined in the court’s decision.
- The section after that is dedicated to “The relevant practical issues” in relation to the practices of the investigating and prosecuting authorities which may have impacted the right to fair trial in the effective investigation and prosecution of the case.
- The fifth field in the template - “Collaboration”, includes information whether there was ongoing cross-border collaboration, or collaboration with electronic service providers/ Internet Service Providers.
- The next section is the “Outcome of the case”, which describes the outcome of the case, with reference to the different stages of the proceedings and the crime(s) the defendant was acquitted/convicted for. The usage of this template for the analysis of all national and European cases will allow the coherent and comparable collection of the findings.

A minimum of 3 cases from each partner country (Bulgaria, Poland, Croatia, Slovakia, Czech Republic and Slovenia) have been analysed in order for conclusions at national level to be drawn. All of them concern sentences and respective courts decisions that considered electronic evidence. In addition to this, the connection between this type of evidence and the presumption of evidence was also examined into detail. Each of the partners has been responsible for the data collection from their respective county. In addition to these national analyses, data was collected at European level. Cases from the ECtHR and CJEU have been reviewed, and the gaps and needs at EU level have been identified. Each of these cases, in addition to the analyses conducted in the sections below, are also included as part of the annexes in the current report.

3. Scope of the case law analysis

As mentioned above, the main aim of this report is to present data concerning the implementation of the presumption of innocence in the context of electronic evidence use. The selected case law was also chosen based on the topic and impact level. All identified cases refer to court decisions issued after 2010 in order for the most up to date and relevant data to be collected. In addition, some of the sections below include comparative analysis on the basis of the conclusions of the reviewed national and European cases.

The national data collection covers 6 EU jurisdictions, each of the partner countries – Bulgaria, Croatia, Poland, Slovakia, Slovenia, the Czech Republic. The geographical scope of INNOCENT is driven by the cultural and legal similarities of the selected jurisdictions.[1] These allow the identification of issues commonly met in the selected jurisdictions, therefore, the exchange of good practices between them will also be more relevant.

[1] M Mendelski, "The EU's Rule of Law Promotion in Central and Eastern Europe: Where and Why Does it Fail, and What Can be Done About It?", p.10, Global Rule of Law Exchange Practice Notes, Bingham Centre for the Rule of Law, London, 2016.

4. Bulgarian case law analysis

CASE	CASE 1	CASE 2	CASE 3	CASE 4	CASE 5
Type of crime	MURDER	UNLAWFUL ACCESS TO A DATA SYSTEM	POSSESSION AND CREATION OF CHILD PORNOGRAPHY	DRIVING AFTER SUBSTANCES USAGE	DISTRIBUTION OF CHILD PORNOGRAPHY
Collaborations	CARTOGRAPHIC FORENSIC EXPERT	EXPERT WITNESSES	INTERPOL, FORENSIC EXPERTS	NO EXPLICIT COLLABORATION	EXPERT WITNESSES
Legal issues	LACK OF CONSIDERATION FOR EVIDENCE	CERTAINTY OF ELECTRONIC EVIDENCE	DEFENDANT'S RIGHTS AND CERTAINTY OF EVIDENCE	ALLEGED PROCEDURAL VIOLATION	CERTAINTY OF ELECTRONIC EVIDENCE
Practical issues	LACK OF ADMISSION OF THE EXPERTS' OPINION	EXAMINATION OF ELECTRONIC EVIDENCE	EXAMINATION OF ELECTRONIC EVIDENCE	ACCESS TO ELECTRONIC DOCUMENTATION	INABILITY TO OPEN ELECTRONIC EVIDENCE
Presumption of innocence	OVERLY RELIED ON	RESPECTED DURING THE PROCEEDINGS	RESPECTED BY THE COURT DECISION	ENHANCED BY THE COURT'S DECISION	RESPECTED DURING THE PROCEEDINGS
Convictions	ISSUED CONVICTION	TERMINATED DUE TO LACK OF EVIDENCE	RETURNED FOR A NEW EXAMINATION	GUIDANCE FOR PROCEDURAL DOCUMENTATION	JUDGEMENT CONFIRMED

4.1. Investigation methods and identified issues

Five cases decided under the Bulgarian jurisdiction have been analysed. They concern different types of crime, including murder, dissemination of child pornography and unlawful access to information. Although some of them have violent aspects, while others do not, they were chosen due to the role that electronic evidence had in them. It could be seen from the analysis below that in all cases, evidence in electronic format had greatly influenced the outcome of the cases. In addition, its connection with the implementation of the presumption of innocence could also be noticed, as well as the balance between the presumption of innocence and the right to fair trial in general and the use of electronic evidence in practice. The data collection aimed to cover different topics, considered in the court's judgements, in order for an objective review to be done regarding the implementation of the presumption of innocence in the context of electronic evidence. The approximate length of the described proceedings is from 2 to 5 years. It could be concluded from the cases below that during the investigation phase this type of evidence is being generally considered, however, electronic evidence governance still needs to be fully incorporated into the Bulgarian legislation.

The first Bulgarian case[2] concerns the offence of murder. The initial proceedings started in 2007 and the final decision has been ruled in 2012. Various forensic examinations have been carried out with respect to numerous telephone records and GPS mapping locations in order to identify the actual location of the defendant at the time of the crime. It was found that the conclusions of the cartographic forensic examination and the data from the call records by the telecom operator, have been misinterpreted and contradict the explanations of the defendant and the three witnesses who were his colleagues about his whereabouts at the time of the murder. The data from the call records of the conversations of the defendant and the victim were ignored during the investigation, although they could have proven the statements by the defendant and the witnesses false. This negligence towards this evidence significantly influenced the lower instances courts' decision as it led to the acquittal of the defendant, which was later revoked by the cassation court. If an adequate and detailed examination of this data had been done, the guilt of the defendant could have been established at a much earlier stage, thus avoiding the prolonged proceedings. This is an example of how, even though electronic evidence has been considered, it has not been examined properly, therefore, it did not serve its purpose of providing actual information that will lead to the solving of the case.

The criminal proceedings in the second case[3] have been initiated in 2015 and the final decision has been ruled in 2019, concerning the offence of unlawful access to an information system. The defendant was accused of unlawfully accessing the computer system of his ex-employer company and that computer data constituting personal data had been compromised in the conditions of a continuous crime with 11 acts. In this case, one of the main items that were admitted as evidence, was the defendant's computer. In the sections below it is described in greater detail how, even though the electronic evidence has been carefully considered, some technical aspects did not allow for this evidence to serve as an undoubtful proof of the defendant's guilt.

The third case[4] concerns the charge of pornographic materials' possession and creation of such with persons under the age of 18. The start of the criminal proceedings against the defendant was in 2010 and the final court decision is from 2012. During the proceedings, a violation of the procedural rights of the defendant was claimed. Upon data provided by Interpol-Wiesbaden, it was established that the defendant was a suspected user of a platform for child pornographic content. A search and seizure were carried out in the apartment occupied by the defendant and his parents. Apart from the several technical aspects, described in the sections below, it was also found that during the investigation the administrator of the platform in question had not been contacted, which would have made possible to further collect of evidence.

The criminal proceedings in the fourth case[5] were initiated in 2021 upon indictment that the accused has repeatedly driven a motor vehicle after the use of narcotic

[2] Case no. 2485/2003
[3] Case No 524/2019
[4] Case 5895/2012
[5] No. 50114

substances. The legal documentation before the court of first instance was submitted entirely on paper. The second instance court issued them as certified copies of documents signed with an electronic signature rather than as documents with hand signature. This later became one of the main questions before the third instance court

The fifth case[6], starting in 2010, final decision delivered in 2014, concerns the offence of offering and distributing of pornographic materials involving persons under 18 years of age, or persons who look like such, via the Internet-chat program "Hello". The defence claimed that the first instance court incorrectly analysed the evidentiary material collected, ignoring the testimony of a witness interrogated by delegation - a police officer at Interpol Ottawa in Canada. In addition, an encrypted CD provided by Interpol-Ottawa could not be accessed by the court without specified access password. Although these aspects were carefully considered in the court, in its final decision it was ruled that during the investigation and lower instances hearings no procedural rights were infringed.

4.2. Collaborations

The majority of the analysed cases involve expert witnesses that delivered an expert opinion in regard to the collection and examination of electronic evidence. They undoubtfully had an important role in the outcome of the case as they outlined the level of reliability and authenticity of a certain piece of evidence. In addition, two of the cases concerned international cooperation with Interpol, which proves that the cross-border exchange of information could significantly increase the number of identified crime, such as child pornography.

In the first case[7] the court has rejected the conclusion of the cartographic forensic examination as it credited a letter where the respective telecom operator commented on the state and capacity of its system four years after the commission of the act, and not on its state as per 2002. The expert witness' opinion was based on data from 2003 - a year after the criminal act was committed, thus assuming that at the date of the forensic report the system had not changed in any significant way for the past year. The baseline data presented by the expert witness' report, as of one year later than the date of the crime, was consistent with the location of the cellular antennas at the time of its preparation, so that the argument that their range had changed significantly was untenable.

Forensics repots have been delivered as well in the second case[8] in regard to the electronic evidence. They have been relied on during the proceedings as they stated that the specific person who had accessed the information system could not be identified due to technical reasons. This shows the expert witness' important role in regard to the implementation of the presumption of innocence as they are the only one that have the necessary knowledge to assess the reliability of a certain piece of evidence.

---

[6] Case No. 1465/2010
[7] Case no. 2485/2003
[8] Case No 524/2019

The third case[9] is an example of collaborations at different levels – the cooperation between the Interpol-Wiesbaden and the Bulgarian Ministry of Interior regarding a signal for the use of the software "eDonkey 2000" and also the collaboration with experts during the investigation and proceedings regarding the technical aspects of the identification and examination of evidence. Despite the fact that this cooperation is one of the main reasons for the case ending up in court, there are also many important aspects that were neglected during the evidence collection and examination that led to the outcome of the current case. Some of the traits that might have led to conclusive pieces of electronic evidence had not been fully followed, which later significantly influenced the proceedings' outcome.

The fourth case[10] does not include any explicitly mentioned cooperation as its main focus is the defendant's rights to access the information relevant to the criminal proceedings.

The collaboration with the expert witnesses had a major role in the fifth case[11]. Based on their skills and knowledge, it was established that no stored or deleted files were found on the computers used by the defendant that would match those sent by means of the "Hello" program, and it was not established that this chat program was installed on any of the computers used by the defendant. In addition, it was also proven without doubt that it was the defendant's IP from which the files were sent. However, they also outlined the fact that it is possible for another person, besides the defendant, to have done it from his IP address, which could be claimed to have acted as a safeguard for the presumption of innocence.

4.3. Nature of legal issues

The section below describes the main legal issues which have been identified during the data collection. The main focus in the majority of the cases was proving whether it was precisely the respective defendant the one who has committed the respective criminal act. Due to the fact that there is a general risk of an unauthorised remote access to any person's network, nobody's guilt could be proven beyond the reasonable doubt. The identified cases show the difficult balance between respecting the presumption of innocence and accessing evidence to undoubtfully prove the guilt.

The appellate court in the first case[12] did not consider the call records between the defendant and the victim that took place in the areas near the crime scene. The court's findings failed to account for the difference in the remoteness of the area where the defendant claimed to had been. It also ignored the forensic examination's conclusion that a telecommunication cell has a specific range of coverage perimeter. This directly concerned the fact that the calls made by the defendant and the victim during the time period in question were covered by the cellular antennas referred to in the expert witness' report, which also served the area where the criminal act was committed. This shows that in this specific case both the investigation and judiciary were not entirely

[9] Case 5895/2012
[10] No. 50114
[11] Case No. 1465/2010
[12] Case no. 2485/2003

prepared to deal with the electronic evidence adequately in a manner that serves the proceedings.

The evidence in the second case[13] unequivocally established unregulated access to the websites of the company through a malicious code launched by a hacker group, carried out by a person with prior access to the company's system at administrative level. However, it has not been established whether this malicious code was launched precisely by the defendant. The facts that the defendant had the necessary access and skills and that he built parallel websites of the same type and purchased domains were insufficient for the competent court to conclude that he was the one who implemented the malicious code because this would have been only an assumption. According to the appellate court, it was impossible for the accused to be connected directly with the e-mail established in the system settings of the websites, receiving internal company information. The fact that this is the email that could only direct the site to a server with an IP address where the domain was registered by the accused is also considered not sufficient proof. The court stated that this decision secures the principle of the burden of the proof while the prosecution could not fulfil it in compliance with the rules for fair trial and in compliance with the requirements of the law for issuing a judgment of conviction, namely - only when the accusation is proven beyond the reasonable doubt.

The essential problem in the third case[14] was the lack of description of the criminal act in the indictment - when and how the defendant gained access to the incriminated pornographic materials. In addition, the defendant was not presented with specific facts upon which to defend himself in connection with the process of downloading the files containing the incriminated pornographic material onto the hard drive of the incriminated computer system. Therefore, it should be assumed that there was a substantial procedural violation, which limited the defendant's rights to organise his defence. The forensic computer and technical expertise established that the holding of the pornographic material require a user registration to the program "eMule". The decryption of the information regarding the username could have been done by the administrator, who holds the rights to the programme itself, but no actions were taken in this regard during the investigation. However, such actions were of great importance in regard to the prosecution of the defendant. In addition, evidence was found that a Trojan virus was installed on the accused computer, which could download files from or to the computer in question without the user's knowledge or consent. Once the risk of files' manipulation on the accused's computer was established, proving the accusation in the necessary undoubted and indisputable way required establishing the exact moment of infection with this virus and establishing whether there were files with pornographic content downloaded (and simultaneously distributed) prior to this moment.

According to the Supreme Court of Cassation in the fourth case[15], the second instance court had made a procedural violation. The normative requirements are to be

[13] Case No 524/2019
[14] Case 5895/2012
[15] No. 50114

interpreted in relation to the provisions of Art. 6 and Art. 13 of the European Convention of Human Rights (ECHR) regarding the right to fair trial and the right to effective legal remedies and Art. 41, §2, b. "b" of the Charter of Fundamental Rights of the European Union (the Charter), establishing the right of access of every person to the documents that concern them. It is therefore relevant to examine whether the normative criminal proceedings' requirements are to be interpreted so that an obligation exists for the court to provide access to the original paper documents instead of electronic documents signed with an electronic signature.

According to the search and seizure report in the fifth case[16], the router used was not seized from the defendant's home and it was impossible to determine whether his IP address was protected or not. No incriminating files were found on his computer. It was established that an IP address could be breached by another person located nearby, if not password protected. The evidence supports the defendant's argument that another person could have used his IP address and sent the files. However, it was undoubtful that the files were sent from the same IP address based on the investigation and produced reports. Nevertheless, this fact is not sufficient for the court to accept that it was the defendant who participated in the Internet communication and that he sent the incriminated pornographic materials, since it is impossible to establish with certainty whether another person did not use this e-mail or simply indicated this mailbox when registering in the "Hello" chat program.

4.4. Nature of practical issues

The five identified cases include practical issues that are closely connected to proving the authenticity and integrity of electronic evidence. One of the significant challenges identified should the main source of evidence is in electronic format, is to ensure that no modifications have been made during the course of the investigation or the trial proceedings. Different practices are applied in this direction, however, as it can be seen from the identified case law, there are still instances where file integrity is not guaranteed. Another concern is the fact that in an online environment it is very difficult to prove who is committing the criminal act. Although in most of the cases, the practice of tracing IP addresses is followed, the possibility of someone else accessing the same IP is also considered. In such cases it is left to the court to decide which probability is more likely, therefore defining the balance between the presumption of innocence and the electronic evidence conclusions. This shows the importance of the judiciary's skills and competence in the context of assessing electronic evidence and their implementation.

In the first case[17] one of the main practical issues is the lack of considering the forensic examination's report by the court. In this instance, the court completely neglected the provided conclusions, although it could have significantly relied on them in order to deliver a sentence as they were proving the location of the defendant near the crime scene.

[16] Case No. 1465/2010
[17] Case no. 2485/2003

The defence in the second case[18] appealed on the grounds that upon careful examination of the forensic technical computer report, it was established that all the records that were made on the website and were provided to the investigation authorities can be manipulated by any person with administrator's rights. The unregulated access was detected via a dynamic IP address as there was no way to determine which person specifically accessed it. The facts showed that there is a possibility that other persons might have also had access. Therefore, it could not have been concluded it was the defendant who accessed the websites, especially since after his departure, the access passwords were changed, and considering the dynamic IP address. In regard to the lack of evidentiary seizure, it was noted that the computer system of the defendant was not seized by the investigative authorities in a timely manner. This was one of the reasons why during the court proceedings was impossible to examine the IP addresses and the traffic data.

The practical issues in the third case[19] are closely connected to the manner in which the evidence trails have been followed and handled. Although, there was a possibility for the username information to be described by the administrator of the programme, no such inquiries were taken during the investigation stage. This would have been of great importance in regard to the consequent proceedings. In addition, the finding of the virus on the defendant's computer completely undermines the indictment at it casts significant doubt on the fact whether the found pornographic files were actually put there by the defendant or by the person who has installed the virus.

The fourth case[20] concerns the access of documentation when stored in an electronic environment. An information system contains all electronic documents and information provided by the participants in the proceedings and the judicial authorities in connection with exercised procedural rights. Therefore, the courts should provide remote, continuous, and free access, as well as technologies and means of access, to the electronic file of right holders in order to secure the right to a fair trial and the right to effective legal remedy.

In the fifth case[21] before the first instance court, it was found that it was impossible to open and read the encrypted hard disk, sent by Interpol-Canada and, thus impossible to be admitted as physical evidence to the case. Due to the inability to open and read the encrypted file, it is also impossible to establish the content of the conversation within the Hello programme between the users and the type of files sent by the first. However, this disc was read in the pre-trial proceedings during the assigned forensic audio-visual examination, according to which 356 photographic images were indecent, unacceptable, and incompatible with public morals. But in view of the centrality of the trial phase of the criminal proceedings and the principle of immediacy in the collection of evidence, the court found that since the content of the disk cannot be reproduced during the trial and the other participant in the Internet communication couldn't be interrogated, the specific content of the incriminated conversation could not have

[18] Case No 524/2019
[19] Case 5895/2012
[20] No. 50114
[21] Case No. 1465/2010

been established in a proper manner, and accordingly, the distribution and offering of pornographic materials is not proven.

4.5. Victims and defendant – two sides of a criminal proceeding

The identified cases allow to observe that the court had carefully considered the defendants' procedural and fundamental rights in all of them. It might also be argued that the presumption of innocence in some of the cases had been overly relied on in contrast with what the particular cases' circumstance suppose. Nevertheless, the Bulgarian court as per presented case law has tried to keep the balance between the defendant's rights and presented evidence, especially in cases where the electronic evidence has proven not to be of conclusive nature.

In the first case[22], it could be claimed that the presumption of innocence has been fully guaranteed. The lower instances courts relied on witness' statements and the defendant's self-declaration, claiming that he was not at the location of the crime scene at the time of the criminal act. The court did not carefully examine evidence that later proved incriminating such as the calls made between the defendant and the victim. When the final sentence was delivered, the defendant was also sentenced to compensate the non-pecuniary damage caused to the civil plaintiffs by the criminal act, together with the statutory interest from the day of the act until the final payment of the amount.

The second case[23] shows the adequate implementation of two main legal principles – the burden of proof and the presumption of innocence. Due to the lack of sufficient evidence, the court did not establish the guilt of the defendant as it could not be proven beyond reasonable doubt. There are several circumstances in the case that do not allow the identification of the specific person that had accessed the information system. Therefore, it could not be proven that it was the defendant, despite the numerous facts from which this could be assumed.

One of the questions raised in the third case[24] was whether the defendant's procedural rights have been duly respected. There are several claims that he did not receive the required information that was needed to adequately prepare his defence. Furthermore, once the fact that a malicious virus has been installed on his computer was established, the presumption of innocence had been respected and the court ruled that he could not be proven guilty beyond reasonable doubt since there is a significant risk of file manipulation.

The fourth case[25] specifically concerns the implementation of the defendant's right to receive information regarding the proceedings and access to the evidence. The

[22] Case no. 2485/2003
[23] Case No 524/2019
[24] Case 5895/2012
[25] No. 50114

judgment confirms that the defendant needs to have access to the information at all instances, no matter the form of the data – physical or electronic.

The fifth case[26] is an example of the difficult balance between establishing an undoubtful chain of evidence that will result in a rightful sentence and respecting the procedural rights of the person accused. Although there were aspects that have proven the possibility of another person committing the criminal act while using the defendant's IP address, evidence was also presented that his personal data was used for the registration of the user account that has sent the respective files. In addition, no incriminating files were found on the accused computer. The lower instance court had guaranteed the defendant's presumption of innocence, confirmed by the appellate court which held that there were no violations of the defendant's rights. Therefore, the delivered sentence was a result of a fair trial.

4.6. Conviction rates

The final decisions in the five cases show different approach and results. Some of them upheld the previous sentence, while others revoked them. In all of them electronic evidence had a significant role, either by confirming the defendant's guilt or by providing new aspects for consideration before the court.

In the first case[27] the cassation court revoked the previous decision, holding the defendant guilty and sentencing him to ten years of imprisonment. This was a direct result of the electronic evidence (i.e. the location of the defendant's mobile phone and the calls he made) that was able prove the defendant had been at the crime scene at the time of the commitment of the offence.

The Court has confirmed the initial decision in the second case[28], terminating the criminal proceedings due to the impossibility of proving who is the perpetrator of the crime. This decision shows the Bulgarian court upholds the presumption of innocence adequately.

It was held in the third case[29] that the substantial procedural violation can only be remedied by a prosecutor through submitting a new indictment. Therefore, the Court voided the judgement and returned the case for a new examination by the prosecutor to eliminate committed recoverable violations of the procedural rules. This decision proves that the Court is prepared to void a conviction if any of the defendant's procedural and fundamental rights had been infringed during the proceedings by the investigators or the prosecution.

The third instance court in the fourth case[30] had given the guidance that procedural documents in the trial phase of the proceedings should be in the same format - physically or electronically, across all competent instances. In addition, until the introduction of full-fledged and real electronic justice in Bulgaria, it is mandatory for

[26] Case No. 1465/2010
[27] Case no. 2485/2003
[28] Case No 524/2019
[29] Case 5895/2012
[30] No. 50114

courts to prepare originals of the acts with handwritten signatures for initiated all cases and if this is not possible specific, requirements need to be followed.

The appellate court and the district court in the fifth case[31] concluded that it was impossible to establish the connection between the incriminated pornographic content and the defendant. However, the appellate court did not find incorrect application of the substantive law, significant violations of the procedural rules or unreasonableness, giving grounds for annulment or amendment of the sentence, and had concluded that the judgement should be confirmed.

5. Polish case law analysis

CASE	CASE 1	CASE 2	CASE 3	CASE 4
Type of crime	AIDING TO MURDER	PARTICIPATION IN ORGANISED CRIMINAL GROUP AND ROBBERY	BRIBERY	FRAUD
Collaborations	COMPUTER FORENSIC EXPERT	LACK OF EXPERT INVOLVEMENT	COMPUTER FORENSIC AND PHONOSCOPY EXPERT	SERVICE PROVIDERS
Legal issues	METHODS OF HANDLING ELECTRONIC EVIDENCE	INCORRECT FINDINGS AND EVIDENCE EVALUATION	SECURING AND AUTHENTICITY OF ELECRONIC EVIDENCE	LACK OF CONSIDERATION FOR ELECTRONIC EVIDENCE
Practical issues	FORENSIC KNOWLEDGE ON E-EVIDENCE	NO VERIFICATION AND WRONG SECURING METHODS OF EVIDENCE	METHODS FOR HANDLING ELECTRONIC EVIDENCE	COURT'S RELUCTANCE TO DEAL WITH ELECTRONIC EVIDENCE
Presumption of innocence	STRENGTHENED BY THE SUPREME COURT DECISION	AFFECTED BY THE FIRST INSTANCE COURT ACTIONS	FULLY RESPECTED DURING THE PROCEEDINGS	AFFECTED BY THE FIRST INSTANCE COURT ACTIONS
Convictions	LIFTED JUDGEMENT	ACQUITTAL AND LIGHTER SENTENCES IMPOSED	UPHELD SENTENCE	LIFTED JUDGEMENT

5.1. Investigation methods and identified issues

Four cases under the Polish legal system were identified, all of which based their decisions on evidence presented in electronic form. None of them concerns violent crimes directly, although the actions of the accused in one of them led to the murder of a person. The length of the proceedings differs in the different cases, being from 3 to 10 years from the time of the crime commitment until the end of the proceedings. In some of them it was the prosecutor actions that put a focus on the electronic evidence, while in other the investigators closely followed these traces. The courts, however, especially those of lower instance, have showed little or no understanding

[31] Case No. 1465/2010

in regard to this type of evidence. Although the presumption of innocence was not explicitly mentioned in all cases, it is observed that the pronounced judgements had strongly considered it as well as other procedural and fundamental rights.

The first identified case[32] concerns the offence of aiding to murder by providing telecommunication data of the victim's location. The accused used his work access to provide information to another person who committed murder. Most of the evidence in this case was found on the defendant's computer. Therefore, a forensic computer examination was appointed; however, the respective forensic examiner did not follow the most recent research developments and current practice for dealing with electronic files, which consequently became a subject of a legal dispute between the defendant and court. The proceedings lasted 5 years. In this period, the case has gone through couple of courts, ending up with a final decision by the Polish Supreme Court.

The second case[33] concerns the participation in organised crime group and robbery. The case decisions concern the collection of electronic evidence in the case such as call logging site and call surveillance and the methods of collecting this data. It was also pointed out that the first instance court considered only incriminating evidence, while evidence in favour of the defendants was not collected, adequate forensic reports were also lacking. The crime was committed in 2005-2006, and the criminal proceedings ended in 2015.

The third case[34] is focused on a bribery committed by a person performing a public function. The authenticity of the electronic evidence in the case was questioned, namely the dictaphone on which the inculpatory statement of the defendant had been recorded by a private person and then delivered to the authorities. The IT police department, when securing the evidence, copied the content of the dictaphone on a CD as a backup option, which later had shown to not be properly working. This gave rise to questioning the authenticity and reliability by the defendant of the data stored on the dictaphone, which was the main evidence against him. This offence was committed in 2013 and the end of the criminal proceedings was in 2016.

The fourth case[35] does not directly refer to the presumption of innocence, however, it illustrates the court practice when dealing with e-evidence. The crime was committed in 2016 and the end of the criminal proceedings was in 2019. Since the sentence was lifted, the case is still pending at the court of first instance. The offence in question was fraud committed through online shopping platforms. The prosecutor appealed against the decision made by the first instance court that the defendant was not guilty. He claimed that the court did not make any effort to verify IT data which were of crucial

[32] Polish Supreme Court judgment of June 20, 2013. III KK 12/13, LEX No. 1341691.

[33] Judgment of the Court of Appeal in Warsaw of 30 January 2015. II AKa 238/14, LEX No. 1651984.

[34] Judgment of the Regional Court in Gliwice of December 21, 2016 VI Ka 832/16, LEX No. 2274146.

[35] Judgment of the Warszawa-Praga District Court in Warsaw of June 6, 2019. VI Ka 1392/18 LEX No. 2712607.

importance for the conviction, namely subscriber data and traffic data that would link the accused with online transactions of a criminal character.

A common pattern is appearing in all cases – either the defendant or the prosecution raises claims in regard to mishandling of electronic evidence by the court. This leads to either neglecting evidence that could prove the guilt of a person, or no appropriate consideration of the risk of faulty electronic data. One of them also shows the incompetency of a forensic expert in regard to the examination of such evidence, while another shows the same in regard to the investigators' knowledge of the perseverance of such evidence.

5.2. Collaborations

The presented cases have different collaboration aspects, yet none of them concerns cross-border collaboration. Two negative elements could be identified – the appointment of an unqualified expert that could harm the proceedings with wrongful conclusions and the negligence to not appoint a qualified person to examine the evidence at all. Nevertheless, an example of a successful collaboration with a computer forensic expert is also presented as well as collaboration with service providers. Some of the cases explicitly show how such cooperation could greatly impact a case outcome and the evidence presented in front of the court.

In the first case[36] there has been collaboration with a computer forensic expert, which however has proven to be unsuccessful due to the fact that the respective expert did not have the necessary capacity in order to deal with electronic evidence in a sound manner, without doubting its integrity and authenticity. He did not use the latest methods in the field, which consequently impacted the conviction greatly.

Despite the fact that the evidence in the second case[37] involved call recordings, location data, and the logging of a given telephone to the network, expert reports in the field of telecommunications were not requested, and the court of first instance issued an erroneous judgment. This is a clear example of how important the involvement of such professionals in fact is.

In the third case[38] an expert in the field of computer science and phonoscopy was appointed by the court of first instance in order to examine the integrity and authenticity of the electronic evidence as they were questioned by the defendant. He performed a spectral analysis of the recording in terms of its authenticity and possible interference with the continuity of the recording, and also prepared a transcript. This conclusion was used consequently as one of the main instruments that have proven the claims of the defence groundless.

---

[36] Polish Supreme Court judgment of June 20, 2013. III KK 12/13, LEX No. 1341691.

[37] Judgment of the Court of Appeal in Warsaw of 30 January 2015. II AKa 238/14, LEX No. 1651984.

[38] Judgment of the Regional Court in Gliwice of December 21, 2016 VI Ka 832/16, LEX No. 2274146.

In the fourth case[39], subscriber and traffic data were collected from various service providers (anonymised in the judgement): e-mail provider and internet shopping platform. It could be concluded from this case that there is a need for more cooperation between judges and forensic experts - experts in different domains and IT specialists. It might also be beneficial to collect several forensic reports in a given case in order to acquire a better perspective over the circumstances and to verify each other's conclusions. However, in Poland the appointment of an expert witnesses is rare due to financial reasons.

5.3. Nature of legal issues

The nature of the legal issues presented by the Polish cases is considerably different. However, a common link is identified – the questionable dealing and examination of the electronic evidence by the Polish court. In some of the cases, a complete negligence for such type of evidence is observed in the lower instance courts, which had been consequently addressed by the higher instance courts. In other cases, the risk of evidence unauthenticity has not been considered at all or electronic traces that could prove the innocence of the accused have not been followed. Although the circumstances of the cases differ, it could be argued that the Polish courts, especially the ones at lower instances, should invest in increasing their competence in regard to electronic evidence.

The accused in the first case[40] questioned the manner in which both by the expert and the court have handled the electronic evidence. In addition to the fact that the court had not agreed to an additional opinion by computer forensic expert, it pointed out that considering the methods of dealing with electronic evidence were still underdeveloped they were not binding to the court, especially when they were no scientific or legal publications and recommendations as to how to deal with evidence in electronic format. This shows that the Polish legal framework is not in a shape to allow the application of the traditional procedural rules to electronic evidence. On the basis of the court's decision, it could be further deduced that the judicial competence was not extensive enough to deal adequately with this legislative gap. The defence appealed the conviction and pointed out that the forensic expert did not abide by the current knowledge in dealing with e-evidence. The used methods by the forensic expert were questioned which gives rise to doubts as to the integrity and, thus, the authenticity of the electronic files. The case ended up in the Supreme Court, whose decision stated that the computer forensics' developments should oblige the judicial authorities to strive to obtain knowledge about the methods of securing electronic evidence.

In the second case[41] the defence based its appeal on the claim of incorrect findings of facts and evidence evaluation, e.g. the evaluation of analytical notes regarding phone

[39] Judgment of the Warszawa-Praga District Court in Warsaw of June 6, 2019. VI Ka 1392/18 LEX No. 2712607.
[40] Polish Supreme Court judgment of June 20, 2013. III KK 12/13, LEX No. 1341691.
[41] Judgment of the Court of Appeal in Warsaw of 30 January 2015. II AKa 238/14, LEX No. 1651984.

logging sites and phone calls. The appellate court found that the first instance court focused only on the circumstances incriminating the defendents and did not take into account those that were in their favour as well as that the phonoscopic opinions used were not correct and were based on analytical notes from telephone logging locations. In addition, the court of first instance based its findings on materials from the operating surveillance which was conducted unlawfully - as a result of an incorrect assessment of evidence and failure to take into account circumstances in favour of the convicts. Moreover, the opinion of experts in the field of telecommunications was not requested, and the court of first instance issued an erroneous judgment. The main argument in the appeal was that procedural provisions were violated in connection with the establishing the location of the mobile phones which were logged on the basis of analyses or the so-called analytical notes drawn up by a police officer. The appeal claimed that such evidence has no value and that the telecom data provided by the respective telecom operators should be subject to telecommunications' forensic examination, otherwise it should not be considered.

In the third case[42], the defendant claimed that his right to defense had been infringed by taking into account the evidence from the recording of the conversation and awarding it incriminating value, stating that the material was collected in violation of the basic principles of securing electronic evidence (since it was recorded out of protocol: by a private person on a private device), and that the content of the recording is highly doubtful as the IT police department interfered with its integrity by making (failed) copies. Although it came from a third person, the recording was considered of high probative value. The court of first instance appointed a forensic expert in the field of computer science and phonoscopy. He did not find any traces of editing or any other interference of external factors in the content of the recording. All necessary measures for its safe storage were implemented, which led to disproving the defence claims that the evidence was not properly secured and there were no grounds to question the authenticity of the recording.

The appellative court in the fourth case[43] pointed out that the data gathered in electronic format had not been examined by the court of first instance. The scope of "electronic data" is not defined as well as how such data were preserved. The fact that the court initially did not make any effort to verify the electronic data and, instead, fully relied on the witnesses' statements which were insufficient to prove the accused as guilty shows that the court was not prepared in this case to adequately evaluate the electronic.

5.4. Nature of practical issues

The practical issues in the identified cases are related to either the reluctance of the court to deal with electronic evidence, or to questioning of the methods used by them. The following is observed at the same time:

---

[42] Judgment of the Regional Court in Gliwice of December 21, 2016 VI Ka 832/16, LEX No. 2274146.

[43] Judgment of the Warszawa-Praga District Court in Warsaw of June 6, 2019. VI Ka 1392/18 LEX No. 2712607.

- following incorrect approach
- implementing all necessary measures to ensure the integrity and authenticity of the collected data.

It could be thus argued that the investigation has the capacity, to some extent, to deal adequately with electronic files and ensure their validity so that they could be consequently used as a grounding aspect in the court decisions.

The first instance court in the first case[44] based the sentence on the computer forensics report which confirmed the reliability and the authenticity of the collected electronic data but without deep diving into practical, forensic and legal knowledge/research on how to proceed with such evidence. This led to a dispute in regard to the court's obligation to follow state-of-the-art investigation and examination methods, which is this case led to lifting the imposed sentence. In this case, the authenticity of the collected data was not questioned because the methods of the examiner himself were not found forensically sound.

The main practical issues in the second case[45] concerned in the lack of verification of electronic evidence and the unlawful method of securing it. The analysis of the phone loggings does not show who had possessed and used the phone. In addition, a forensic report in the field of telecommunications had not been ordered. The court of first instance based its findings on materials from operative surveillance which was conducted unlawfully - as a result, incorrect assessment of evidence occurred and a failure to take into account circumstances in favour of the convicts. This directly infringed this presumption of innocence as it is the court's obligation to consider evidence proving both the accused innocence and guilt.

The core dispute in the third case[46] concerns the way of handling electronic evidence by the authorities and ensuring transparency for the parties in the chain of custody. The court, however, pointed out that the electronic evidence was gathered and preserved in forensically sound manner. What was of practical, but also legal relevance, is the way of securing electronic device: using sailing wax, limiting access to the device, and appointing forensic expert. Since all these steps were carefully and adequately implemented, the appeal of the defendant regarding the authenticity and integrity of the data was not justified. This case is a strong example of the level of competence of the investigators and their readiness to deal with electronic evidence.

In the fourth case[47] the main practical obstacle is the court's reluctance to deal with electronic evidence which could be due to the lack of training, knowledge, and appropriate procedural rules. Nevertheless, this could not have been relevant

[44] Polish Supreme Court judgment of June 20, 2013. III KK 12/13, LEX No. 1341691.
[45] Judgment of the Court of Appeal in Warsaw of 30 January 2015. II AKa 238/14, LEX No. 1651984
[46] Judgment of the Regional Court in Gliwice of December 21, 2016 VI Ka 832/16, LEX No. 2274146.
[47] Judgment of the Warszawa-Praga District Court in Warsaw of June 6, 2019. VI Ka 1392/18 LEX No. 2712607.

reasoning for neglecting evidence that might greatly impact the outcome of the case and hence the conviction or acquittal of the defendant.

5.5. Victims and defendant – two sides of a criminal proceeding

None of the cases explicitly mentions the treatment of the defendants or of the victims and if they were questioned. However, a significant part of the cases concerns the court treatment in regard to the defendants' rights, in particular the presumption of innocence. There are examples presented of the court's negligence to evaluate evidence that might be of exonerating nature. Nevertheless, there are also examples that show the complete opposite – respect for the presumption of evidence and no infringement of the defendants' rights.

The first case[48], although not explicitly, aimed at strengthening the presumption of innocence by making sure the evidence upon which the judgement is based is thoroughly verified according to the most recent forensic knowledge and, thus, complexity of e-evidence does not limit the procedural rights of the accused. The lifting of the judgment showed that, although the courts at lower instances are not fully prepared to deal with cases involving electronic evidence, the Supreme Court does not tolerate the incompetent examination of evidence that might harm the integrity of the proceedings.

In the second case[49], the first instance court considered only incriminating evidence and not such in favour of the defendants, which directly affected the presumption of innocence. In addition, a forensic report on the electronic evidence was not ordered which further infringed defendants' procedural rights.

The presumption of innocence in the third case[50] was fully respected. The courts of both instances, as well as the investigation made a lot of effort to thoroughly and carefully secure and verify the electronic evidence. The appointed forensic expert performed his duties according to best practices and knowledge. Therefore, the authorities involved in the case operated in line with the presumption of innocence principle. In addition, the defendant's claim regarding the fact that the information was part of a private conversation between him and a third party was examined and found that was not infringing any of his fundamental rights since the recording had not been altered or falsified.

In the fourth case[51] the court of first instance fully neglected the electronic data which, while the court of second instance correctly pointed out as crucial in determining the defendant's criminal responsibility. Therefore, the complexity and novelty of e-

[48] Polish Supreme Court judgment of June 20, 2013. III KK 12/13, LEX No. 1341691.

[49] Judgment of the Court of Appeal in Warsaw of 30 January 2015. II AKa 238/14, LEX No. 1651984.

[50] Judgment of the Regional Court in Gliwice of December 21, 2016 VI Ka 832/16, LEX No. 2274146.

[51] Judgment of the Warszawa-Praga District Court in Warsaw of June 6, 2019. VI Ka 1392/18 LEX No. 2712607.

evidence discouraged the court from investigating it which resulted in a judgement based on fragmented evidence. In other words, omitted electronic data may have proven the person's innocence had the court of first instance made any effort to investigate it.

5.6. Conviction rates

Only in one of the four cases, the sentence was upheld by the higher instance court. In two of the cases, the conviction was lifted due to concerns regarding the methods used for the examination of electronic evidence, while in a third case, the defendants were either acquitted or a lighter sentence was imposed. This shows that the electronic evidence has a significant role in the decision-making process and that its faulty examination may lead erroneous sentences.

In the first case[52] the Supreme Court clearly pointed out that the analysis of electronic evidence requires a special approach and that its evaluation has to be extremely careful due to the volatility of data by using the most recent knowledge. Due to the fact that the court of appeal did not examine the claims concerning the methods of dealing with electronic evidence, and the latter was of significant importance for the outcome of the case, the sentence was lifted.

In the second case[53] the court of appeal (second instance) changed the judgment. As a result, some of the defendants' acts were acquitted and for others lighter sentences were imposed. The change of the judgment was due to the inadequate examination of the electronic evidence and the lack of consideration of exonerating facts.

The court disagreed with the appeal's arguments in the third case[54], namely that the evidence was collected in violation of the basic principles of securing electronic evidence in the form of e.g. failure to put the carrier in an electrostatic foil bag, incorrect labelling, or failure to consider evidence in favour of the accused (contrary to the presumption of innocence). The statements in the appeal of improper method of securing the recording were not justified, therefore, the sentence was upheld. This is the only case from Poland with a confirmed sentence, while the data on the proceedings show sufficient respect for the defendant's rights.

The court of appeal in the fourth case[55] lifted the sentence as the lower instance court did not evaluate the core evidence presented by the prosecutor, namely the electronic data. This contradicted the basic principles of the criminal trial such as the principle of the free assessment of evidence and the principle of truth. In particular, the higher instance court found that there are significant gaps in the chain of evidence which can only be filled by a proper analysis of subscriber and traffic data.

---

[52] Polish Supreme Court judgment of June 20, 2013. III KK 12/13, LEX No. 1341691.

[53] Judgment of the Court of Appeal in Warsaw of 30 January 2015. II AKa 238/14, LEX No. 1651984.

[54] Judgment of the Regional Court in Gliwice of December 21, 2016 VI Ka 832/16, LEX No. 2274146.

[55] Judgment of the Warszawa-Praga District Court in Warsaw of June 6, 2019. VI Ka 1392/18 LEX No. 2712607.

6. Croatian case law analysis

CASE	CASE 1	CASE 2	CASE 3
Type of crime	5 OFFENCES CONCERNING CHILD SEXUAL ABUSE	8 OFFENCES CONCERNING CHILD SEXUAL ABUSE AND EXPLOITATION	OFFENCES CONCERNING CHILD SEXUAL ABUSE AND EXPLOITATION
Collaborations	NO EXPLICIT COLLABORATION	NO EXPLICIT COLLABORATION	NO EXPLICIT COLLABORATION
Legal issues	LEGALITY OF THE COLLECTED EVIDENCE	LEGALITY AND CREDIBILITY OF THE COLLECTED EVIDENCE	CREDIBILITY OF THE VICTIM'S STATEMENT
Practical issues	COLLECTION OF ELECTRONIC EVIDENCE	COLLECTION AND CREDIBILITY OF ELECTRONIC EVIDENCE	COLLECTION OF ELECTRONIC EVIDENCE
Presumption of innocence	DEFENDSNT'S RIGHTS RESPECTED DURING THE PROCEEDINGS	CONSIDERINGED DURING THE PROCEEDINGS, NO INFRINGEMENTS FOUND	NO INFRINGMENTS FOUND
Convictions	JUDGEMENT UPHELD	JUDGEMENT UPHELD	CONVICTION ISSUED

6.1. Investigation methods and identified issues

Three cases under the Croatian jurisdiction were presented, all of which concerning sexual offences of children. The cases allow the observation that electronic evidence could play a major role in such types of crime. Most of the accused have stored incriminating media files that were consequently found on their devices which allowed for their guilt to be established in front of the court. Another important aspect is the fact that in two of the cases the victims have actively cooperated by giving statements and providing additional electronic evidence which has resulted in conviction. The authorities have also contributed with active examination of electronic evidence, although several errors have been identified and described in the sections below.

The first Croatian case[56] includes 5 offences in total - two criminal offences of sexual abuse of a child under the age of fifteen, the criminal offence of enticing children to meet sexual needs, the criminal offence of introducing children to pornography and the criminal offence of exploiting children for pornography. The defendant claimed that the charges were exceeded and that the judgments were based on unlawful evidence, which violated the right to fair trial. He claimed that the evidence from the social media were collected without a proper search warrant. During the investigation, the home of the defendant and other premises were searched in the presence of two

[56] III Kr 120/2020-3

adult citizens as witnesses. A laptop, tablet, several mobile phones, a USB stick and two CDs were taken. In addition, based on the order of the investigative judge, additional search was also ordered of the defendant's cell phones and the Facebook profile of another person.

In the second case[57] the defendant was found guilty of eight criminal offences against the sexual freedom and sexual morality and one criminal offence of possessing child pornography on a computer system or network, three criminal offences of introducing children to pornography, including other criminal offences of sexual abuse and exploitation of children. He claimed that that the judgment was based on unlawful evidence as the laptop was the only subject of the search, and that illegal search of the SD memory card was conducted, because the contents of that card were examined precisely on the seized laptop. He also stated that before opening the files on the computer, a forensic image[58] was not done, which made impossible for the evidence authenticity to be verified. The defendant also claimed that since the memory cards were examined on his laptop, it allowed the transfer of files from the memory cards to the computer and vice versa, which means that neither the computer nor the memory cards can be credible evidence due to doubts of their contamination.

The third case[59] deals with the crime of sexual abuse and exploitation of a child, sexual abuse of a child under the age of fifteen, gratifying lust in front of a child under the age of fifteen, exploiting and introducing children to pornography. During the investigation, two mobile phones of the victim were temporarily seized. Also, the phone, tablet, laptop, desktop computer, camera and USB stick was temporarily confiscated from the defendant. From the testimonies of the victim and other witnesses, including the insight into the record of the search of movable property (phones, laptops and etc.), it was found that in the mobile phones used by the victim there was no correspondence between her and the defendant, nor any photos, since she always deleted the pictures from the respective mobile phones.

6.2. Collaborations

Although the judgments in all three cases do not explicitly mention collaboration with a forensic expert, such could be assumed on the pre-trial stage of the proceedings. According to the relevant legal provisions, the police may order to technical experts to examine the collected e-evidence. It is the Cyber Security Service responsibility, established within the Ministry of Interior, to conduct forensic analysis of digital evidence.

6.3. Nature of legal issues

The legal issues in two of the cases concern the defendant's claim of the legality of the evidence. Although some errors have been identified during the investigation stage,

[57] III Kr 165/11-5

[58] A bit for bit copy of the source device and is stored in a forensic image format; for further information please consult: https://www.bileckilawgroup.com/court-martial-defense-blog/what-is-a-forensic-image/

[59] Kzd-3/2019-29

the courts concluded that the collected evidence in both cases is lawful. In regard to the third, the electronic evidence, in addition the victim's statements, was the main source of evidence which resulted in the conviction of the defendant.

The Supreme Court in the first case[60] has determined that the appealed judgement is not based on data obtained from a review of the Tinder profile as it is claimed by the defendant but from data obtained by the search of Facebook profile upon the order of the investigative judge. The only evidence obtained without the order was "correspondence between profile L. K. i P. M. i M. K.", because the victim herself provided consent, handed over her phone and gave up the password to search her profile. Therefore, in this case, the evidence was gathered lawfully in contrast with the claims of the defendant.

The main legal question in the second case[61] refers to what extent the search of the SD memory card without an investigative judge's order could "contaminate" with its contents the computer for which such order existed. The first and second instance courts found that the search of the laptop was carried out on the basis of a previously issued search warrant by investigative judge, and therefore the defence's motion to set aside that evidence as unlawful was duly rejected. The two searches each by a separate unit and the fact that one record was drafted of both searches did not result in a different qualification of these actions. In addition, a search warrant for the SD memory card was subsequently issued and the fact that its contents were first determined on the basis of an illegal search did not result in unlawfulness of the SD memory card as evidence itself. Moreover, the Supreme Court concluded that the first and second instance courts found that the above might lead to possible objection to the credibility of the evidence, but not a basis for submitting an extraordinary judicial remedy for an extraordinary review. Therefore, the defendants' objections were aimed at the credibility of the evidence, and not at its legality.

The court in the third case[62] confirmed that the victim's statement is credible by the record of the search of movable property, i.e. from the defendant's mobile phone and computer. Namely, it is clear from the aforementioned record that 128 photos were taken with an explicit representation of the victim, 441 photos with an image of the victim, and 12 photos with an image of the victim and the defendant were found in the mobile device. On the basis of the evidence presented, the court established beyond doubt that the defendant committed the criminal acts charged against him.

6.4. Nature of practical issues

In all three cases the practical issues are related to the collection of electronic evidence. In two of them the practical issue is in the context of how to lawfully collect this type of evidence, while in another, the challenge was connected to finding evidence if one of the persons involved have deleted them. Nevertheless, in all cases,

[60] III Kr 120/2020-3
[61] III Kr 165/11-5
[62] Kzd-3/2019-29

the electronic files have been of great contribution to the establishing of the defendants' guilt.

One of the main practical issues in the first case[63] concerns the collection of electronic evidence. A basic principle is the lawfulness of such gathering, namely, law enforcement officials, acting in a specific case, are responsible for ensuring that the law, forensic rules and procedural principles are applied. Those who carry out the actions must be appropriately educated so that they can find and seize the electronic evidence. The issue in this case was whether the general rule for a judge order sanctioning the seizure of evidence, applies to the collected information from the victim's mobile phone. However, since the victim herself signed consent and voluntarily with the presence of the legal representative - her father, handed over her mobile phone and gave up the password to search her profile, an investigative judge order was not necessary.

In the second case[64] the principles and provisions in relation to the collection and use of e-evidence are concerned. If those principles were not respected, the obtained e-evidence would be unlawful. During the first instance proceeding, the credibility of the evidence was disputed or rather the method how the evidence was assessed. There are no legal provisions in the Croatian legal framework, nor protocols regarding the assessing of e-evidence. However, it such case the forensic rules need to be applied and respected.

In the third case[65] no correspondence was found between the victim and the defendant as well as no photos, since she always deleted the pictures from the mobile phone. However, at a later stage such photos were found on the defendant's devices in addition to the victim's statements that have proven enough for a sentence to be delivered.

6.5. Victims and defendant – two sides of a criminal proceeding

All victims in the presented cases are children, which makes them vulnerable[66]. Nevertheless, in two of them the victims have actively participated in the collected of incriminating evidence either by giving statements or by providing evidence themselves. The defendants in two of the cases have claimed that their rights have been breached. However, such infringements have not been established by the court and their objections have been found groundless.

In the first case[67] the defendant claimed that there was a violation of his right to fair trial due to a number of procedural actions that "*diminished the right to defence*". He had found this infringement in the fact that the expert associate at the evidentiary hearing, during the examination of the injured party, asked capsizing, unprofessional

[63] III Kr 120/2020-3
[64] III Kr 165/11-5
[65] Kzd-3/2019-29
[66] Pursuant the Victims' Rights Directive, Art. 22, par. 3
[67] III Kr 120/2020-3

and suggestive questions, and the first instance court had failed to determine the relevant facts in a valid and credible manner. However, the interrogation of the victim was audio-video recorded and the court concluded that the defence was not prevented from asking questions to the witness. It was evident that the defence asked questions, objected to the testimony of the victim, requesting that the court, if it deems it necessary, to prohibit some questions, which the court did not do, after which the defence asked no further questions. Therefore, such violation was not found by the court. In regard to the victim in this case, during the investigative stage she had consented to provide evidence herself, by providing her phone, that has proven to be of incriminating nature to the defendant.

In the second case[68] the respect for the defendant's rights was questioned as he claimed that the evidence presented before the court was unlawful. The higher instances courts did not support this claim as, despite the omissions during the collection of evidence, the evidence itself was not deemed unlawful. Therefore, it could be claimed that the defendant's rights have not been infringed during the proceedings and the court had carefully considered the applicable principles in order to conduct a fair trial.

The third case[69] outlines that in the Croatian legal framework there are no explicit provisions on the collection of e-evidence when the victim is a child. However, children at the age of 16 or older are allowed to make statements and initiate actions in the proceedings on their own. In addition, there are provisions that are of importance to children who are victims of a criminal offence since they enjoy additional rights in the criminal proceedings, such as the right to an attorney at the state's expense, the confidentiality of personal data and the right to exclude the public to the proceedings entirely or partially. Furthermore, the court, the prosecution, and the police must treat children with diligence having in mind their age, personality, and other circumstances so as to avoid harmful consequences on their personal development and education.

6.6. Conviction rates

In all presented cases, convictions have been issued. Although some of them have been through several judicial instances, there are no sentences revoked. In all cases the main instrument for the establishing the guilt of the defendant was electronic evidence.

In the first case[70] the defendant's appeal to a violation of the right to a fair trial was not founded. Consequently, his request for an extraordinary review of the final judgment was not granted. The presumption of innocence in this case is applied through the employment of the defendant's privilege against self-incrimination. The defendant was not obliged to provide the authorities with access to his computer or to give them the password/encryption code or to help them in any way that could result in self-incrimination.

[68] III Kr 165/11-5
[69] Kzd-3/2019-29
[70] III Kr 120/2020-3

The court in the second case[71] ultimately concluded that the search of the laptop was carried out upon order of the investigative judge and is considered as lawful evidence, even though the search of the SD memory card was executed without a separate order issued at that time. However, the court concluded that this does not mean that the search record constitutes unlawful evidence in its entirety. Therefore, the court refused the request for an extraordinary review of the final judgment as unfounded.

The sentence in the third case[72] was based greatly on electronic evidence. In addition to the victim's statements, media files were found on the defendant's devices that made it possible for the court to establish his guilt beyond the reasonable doubt.

7. Slovakian case law analysis

CASE	CASE 1	CASE 2	CASE 3
Type of crime	DANGEROUS PERSUIT OF A PERSON	VIOLATION OF SERVICE OATH AND ASSISTING ILLEGAL SMUGGLING	SEXUAL ASSAULTS AND PHYSICAL AND EMOTIONAL ABUSE
Collaborations	ASSUMABLY WITH THE VICTIM	DEFENDANT	TELECOMMUNICATION SERVICE PROVIDER
Legal issues	LEGALITY OF THE DECISION	CLARIGY OF THE ELECTRONIC EVIDENCE	AUTHENTICITY AND INTEGRITY OF THE ELECTRONIC EVIDENCE
Practical issues	CHANGE IN CLASSIFICATION OF THE CRIME	INCLARITY OF THE ELECTRONIC EVIDENCE	SENSITIVENESS OF THE CASE CIRCUMSTANCES
Presumption of innocence	NO INFRINGEMENT WAS FOUND	RESPECTED DURING THE PROCEEDINGS	INFRINGED DUE TO NEGLIGENCE TOWARDS THE EVIDENCE
Convictions	JUDGEMENT UPHELD	NO DECISION ISSUED DUE TO LACK OF EVIDENCE	CONVICTION REVOKED

7.1. Investigation methods and identified issues

The three presented cases concern crimes of significantly different nature. Despite the fact that in all of them electronic evidence has been collected and examined, only in one it has proven the guilt of the defendant beyond reasonable doubt. In addition, the negligent examination of the evidence in one of the cases led to the erroneous decision by the court. The sections below show examples of legal and practical issues

[71] III Kr 165/11-5
[72] Kzd-3/2019-29

that arise in case where the collected electronic evidence in not of sufficiently conclusive nature.

The first case[73] concerns the dangerous pursuit of a person. The defendant was threatening the victim via phone calls, SMS and messenger chat, and followed her. The electronic evidence offered a clear time frame with specific and detailed messages supporting the claims of the victim.

The second case[74] reviews the offences of violation of the service oath of a policeman by sharing information about the state border with an unauthorised person and thereby assisting illegal smuggling activities. The electronic evidence in this case (content of social media messages, text messages), provided by the defendant in order to prove his innocence, revealed information regarding the network of smugglers. Even though the defendant was sharing confidential information, it was obvious from these messages that he did not do it for enrichment or any further benefits.

The third case[75] concerns the associations of sexual assaults and physical and emotional abuse. The victim was proven to suffer from psychological issues which had led to her accusing her father of the above-mentioned acts. She provided messages as evidence to the authorities that were supporting her accusations. However, during the proceedings via cooperation with the respective telecom operator, it was found out that she was sending violent messages to herself, and the accused was acquitted.

7.2. Collaborations

In the three cases collaboration was established either with the victim or the defendant. However, while the provided electronic evidence by the victim in one of the cases was enough for the defendant to be convicted, the evidence presented by the defendant in another case was not clear enough, therefore, deem as inconclusive. The circumstances in the third case significantly distinguished as it was found that the assumed victim have falsified the evidence that she presented to the authorities. In this case, it was the collaboration with a service provider that contributed to solving the case, although it was not done in a timely manner.

As the physical evidence was not convincing in the first case[76] as all defendant's attacks were without witnesses, or the current boyfriend of the victim was present, deemed as potential bias, the electronic evidence significantly contributed to the proceedings' outcome. Although there is no clear statement how the electronic evidence was collected, it could be assumed that they were provided voluntarily by the victim. The electronic evidence also proved that even though the case was erroneously classified at the start, the results and the decision of the court still would have remained the same.

[73] SR 5Tdo/67/2021 3520010073 28.02.2022
[74] (2018)
[75] (2021)
[76] SR 5Tdo/67/2021 3520010073 28.02.2022

There was no established collaboration in the second case[77] with external providers or forensic experts as all electronic evidence was provided by the defendant who willingly shared the content of his messages from social media and also text messages. However, such an approach is not to be supported, since evidence tempering should be always subject of a review, while the court should always examine such a hypothesis, regardless of who has provided the evidence.

The cooperation with a telecommunication service provider in the third case[78] has proven vital as it revealed that it was the victim who was sending threatening messages to herself. It could be argued that there could have been a better cooperation with the telecommunication service providers at the start. The request of a statement from the call records and messages was only considered in the appeal. If this was done at the start, it could have saved lots of time, resources and stress to the parties' family.

7.3. Nature of legal issues

The legal issues in the three cases are of significantly different nature. While one of them concerns the alleged infringement of the fair trail principles, the other two concern the examination and usage of electronic evidence. In one of them the electronic evidence was falsified by the victim which has been found at a later stage of the proceedings, while the first instance court had already issued an erroneous sentence. This case is a clear example of the importance of the proper understanding and usage of electronic evidence, even in cases concerning sensitive matters, as potential negligence may result in innocent persons being unfairly convicted.

The defence in the first case[79] claimed that the court's decision was erroneous because the defendant's actions were not described properly, the decision was delivered to defendant very late, and that the actions for which he was prosecuted were not the same which were stated in the sentence. Therefore, the defendant did not have a fair chance to defend himself and provide evidence that would have changed the opinion of the court. He also objected to the fact that the hearing of the victim was done only in the presence of his lawyer which did not allow him to defend himself. The Supreme Court did decide that the defendant did not have the right to appeal in this case as the statements made are deemed irrelevant. The indictment did not change at any point as the electronic evidence was the main source of facts demonstrating the behaviour of the offender.

As the investigation in the second case[80] concerned a sensitive matter that involved policeman, there was a mix between disciplinary proceedings - firing a policeman, and criminal proceedings - smuggling goods through the border. There was an issue in the pre-trial proceedings as the defence lawyer could not question witnesses due to security reasons. The e-evidence was very unclear as the respective messages did not show to what extend the policeman knew about the illegal activities. It was also not

[77] (2018)
[78] (2021)
[79] SR 5Tdo/67/2021 3520010073 28.02.2022
[80] (2018)

clear who the unauthorised person with whom he shared information with is as it had not been specified that the defendant cannot share information with the other policeman. The first instance court decided that the policeman should be fired. However, after an appeal, the case was returned to the district court as the evidence was not conclusive enough to make a decision.

The proceedings in the third case[81] were expedited due to the weak mental health state of victim, which was assumed due to the mistreatment from her father. Therefore, the case was closed even despite existing gaps in the evidence chain. However, it was noticed at a later stage of the proceedings, that the evidence was illogical - there was never any victim, the victims had been already treated by psychiatrists many times before, and she has voluntarily visited the household where her father was present on several occasions etc. The cooperation with the respective service provider allowed the alleged perpetrator - her father, to actually prove that there is no harm being done to her from his side.

7.4. Nature of practical issues

The practical issues described in the sections below concern different aspects of the proceedings, yet all are connected to the defendant's rights. While one of them directly submitted a claim that his rights have been infringed due to the improper information that he had received from the court which affected his defence, another defendant's presumption of innocence was clearly infringed as the authorities and judiciary put no efforts in verifying the electronic evidence that was submitted against him. The other defendant was providing electronic evidence in order prove his innocence, while it is a clear legal principle that the burden of proof falls on the prosecution to prove his guilt.

One of the practical challenges in the first case[82] was the fact that the there was a change in classification of the offence. Initially it was classified slightly differently, and the defence claimed that the indictment included scarce information. Nevertheless, the court stated that the outcome still would have been the same, and that the difference in the charges was due to a stenographic error. However, such practices should be avoided, and it is required to inform the offender in detail how the offence is classified.

The most problematic aspect in the second case[83] is that it was not clear who the unauthorised person was and to what extent the policeman could communicate information to other colleagues about activities on the state border. The policeman clearly had known that there were illegal activities going on which he reported, but continued to share confidential information. Another question which arises in this case is why when the policeman reported that W.S. was engaging in illegal activities, he was not investigated. In this particular case the electronic evidence brings more

[81] (2018)
[82] SR 5Tdo/67/2021 3520010073 28.02.2022
[83] (2018)

confusion than facts as the defendant and W.S. were communicating through SMS and Facebook, and the messages were short and easily could be taken out the context.

One of the main practical issues in the third case[84] was the fact that electronic evidence was only examined during the appeal. If this was done earlier, it could have been confirmed that defendant was not guilty. In addition, it was not noticed that the victim's evidence - text messages, was always presented as screenshots without showing the sender's number - just the name "Dad". This might have pointed out that anyone could have sent them. The weak mental state of the victim also played a crucial role as the court tried to deliver a decision as quickly as possible not to add to the stress and cause another emotional breakdown. Another important fact is that the victim had already accused her father of inappropriate behaviour towards her in another instance. However, this report dismissed as social services visited their household and did not find anything alarming.

7.5. Victims and defendant – two sides of a criminal proceeding

The two cases involving a victim showcase appropriate victims' treatment. The victim in the dangerous pursuit case had not been questioned in the presence of the defendant which showed understanding of victim's rights by the respective authorities'. The special treatment of both the authorities and the court regarding the other victim, however, greatly affected the defendant in the case. Although the erroneous sentence is due to the fact that the court had expedited the proceedings in order to avoid any further harm to the victim, this approach does not explain the negligent examination of the provided evidence and the lack of adequate investigation that would have easily proved the innocence of the defendant. The defendant in the other case was collaborating with the authorities trying to prove his innocence, however, the fact that he committed the offence in his capacity as a policeman contributed with aspects that additionally complicated the circumstances of the case.

The defendant in the first case[85] claimed that his right to defence had been infringed due to the incomplete and inaccurate information regarding the classification of the crime he had received. The court held that this had not affected the case outcome, therefore could not be claimed to have infringed the right to defence. The victim's statements in this case were greatly supported by the presented electronic evidence as there have not been other evidence upon which to rely on. There is no explicit information regarding how the victim had been treated during the proceedings; however, it could be assumed that she had cooperated with the authorities by providing the evidence herself.

The fact that the defendant in the second case[86] was a policeman further complicated the case. During the proceedings he had to be proven guilty in two aspects – violating his police oath and assisting to illegal smuggling. The fact that a colleague of his was

[84] (2021)
[85] SR 5Tdo/67/2021 3520010073 28.02.2022
[86] (2018)

involved also brought the questions whether he was allowed to share such information and to what extent. The defendant in this case cooperated fully to prove his innocence. The latter proved insufficient to reach a conclusive decision.

The electronic evidence in the third case[87] was collected during the appeal upon the request of the defendant's lawyer. The whole case was built upon very unclear evidence and one-sided statements of the victim, which were not supported by her family, friends or medical professionals. Due to the sensitivity of the case the court tried to protect the victim both from further abuse and from prolonged proceedings. However, this resulted in the infringement of the defendant´s presumption of innocence as without carefully considering the authenticity and integrity of the evidence against him, the lower instances court issued a erroneous decision.

7.6. Conviction rates

The electronic evidence contributed to the issuing of a sentence in one of the cases where it clearly proved the guilt of the defendant. In the other case, however, the evidence was not clear enough in order for conclusions to be based solely on it. Nevertheless, the other case was greatly affected by the presented evidence in electronic format, which led to the issuing of an erroneous sentence due to the negligent examination of the presented electronic evidence.

The court in the first case[88] held that the electronic evidence clearly proved all signs of dangerous pursuit even though this was not the prosecutor's original indictment. the court stated that the indictment remained the same and it was just a technical mistake in the case file that did not influence the outcome.

In the second case[89] the Supreme Court was returned to the competent lower instance court due to lack of conclusive evidence. In this instance, although there was full cooperation from the defendant's side in regard to the provision of evidence, it was not sufficient in order for a decision to be established.

The decision of the court in the third case[90] was repealed after evidence from the respective telecom operator was provided, which clearly proved that the defendant was innocent. This case is an example of considerable negligence of the presumption of innocence as a sentence was delivered based on unclear and not adequately examined electronic evidence.

[87] (2021)
[88] SR 5Tdo/67/2021 3520010073 28.02.2022
[89] (2018)
[90] (2021)

8. Czech case law analysis

CASE	CASE 1	CASE 2	CASE 3	CASE 4
Type of crime	COUNTERFEITING OF DOCUMENTS AND MONEY	INCITING TO ILLEGALY INTERFERE ADMINISTRATIVE PRODEEDINGS	FRAUD	ILLEGAL DISTRIBUTION OF COPYRIGHTED CONTENT
Collaborations	LACK OF COLLABORATION WITH EXPERT WITHNESSES	LACK OF COLLABORATION WITH EXPERT WITHNESSES	LACK OF COLLABORATION WITH EXPERT WITHNESSES	INTERNET SERVICE PROVIDER
Legal issues	RELIABILITY AND INTEGRITY OF ELECTRONIC EVIDENCE	DEFECTS OF THE EVIDENCE	EVIDENCE ADMISSIBILITY, PROPORTIONALITY, AND INTEGRITY	EVIDENCE RELIABILITY AND CLARITY
Practical issues	SECURING AND EVALUATION OF THE EVIDENCE	PRIVACY INVASIVE ACTONS	SECURING AND EVALUATION OF THE EVIDENCE	EVIDENCE EXAMINATION METHODS
Presumption of innocence	LACK OF REFLECTION OF RELEVANT OBJECTIONS	FUNDAMENTAL RIGHTS AFFECTED	NO BREACH FOUND	INSUFFICIENTLY IMPLEMENTED
Convictions	ANNULED DECISION	OVERTURNED DECISION	ESTABLISHED CONVICTION	RETURNED FOR EVALUATION

8.1. Investigation methods and identified issues

Four cases under the Czech jurisdiction were presented that dealt with various offences including counterfeiting of tax documents and appropriation of sums of money, fraud, incitement to illegal influence of witnesses in criminal proceedings and to illegal interventions in administrative proceedings related to traffic offences, and illegal distribution of copyright-protected content.

In all of the aforementioned cases e-evidence has served as an essential such as accounting system reports, wiretaps and audio-recordings, peer-to-peer DC++ networks and identification of IP addresses. Furthermore, three of the four cases were held before the Czech Constitutional Court in connection to the occurring procedural errors originating from the use of e-evidence that supposedly affect the right to fair trial, the presumption of innocence and the principle of *in dubio pro reo*.

The first case concerned the alleged counterfeiting of tax documents and appropriation of sums of money by a junior sales assistant in charge of issuing invoices and managing the cash register. The employee was supposedly making additional changes to invoices and the cash register documents for a year and appropriated the differences between the declared and the billed amounts. The primary evidence consisted of (i) the data from the accounting system in which the complainant's employer kept its accounts and recorded the tax documents issued; and (ii) a ledger (book of accounts) sent by email without an electronic signature. The defendant

argued that the data from the accounting system had been scorched in a way which undermined its accuracy, reliability and integrity, thus requesting an expert witness to establish the reliability of the system.

In the second case the defendant was accused of inciting the head of the Department of Transport and Road Management of a Municipal Authority to illegally intervene in administrative proceedings related to traffic offences, thus influencing the legality of the administrative proceedings. The incitement was recorded by a wiretap ordered by the Public Prosecutor's Office. The wiretapping was not ordered directly concerning the defendant's alleged criminal activities but rather on suspicion of the activities of an unknown organised group importing vehicles and manipulating their roadworthiness. The defendant brought forward that he had been convicted erroneously in violation of the fundamental principles of fair trial and solely upon the evidence of the wiretap, thus questioning the integrity and authenticity of the recordings.

The third case deals with the alleged crime of fraudulent activities done by a lawyer for promising to reopen a retrial and to influence witnesses in the criminal proceedings of his client. Once again, the communication between the lawyer and his client was recorded via wiretap. During the course of the proceedings, the defendant argued that the wiretaps should have been excluded as evidence since (i) they were unconstitutional on the grounds that they recorded conversations between a defense counsel and a client; and (ii) there have been procedural errors in the ordering the wiretapping by the prosecution.

The fourth case dealt with the matter of illegal distribution of copyrighted content via a DC++ peer-to-peer network and the identification of person within a household who committed the activity based on the IP address from which the crime has occurred.

8.2. Collaborations

None of the cases feature any cross-border collaboration. Furthermore, no collaboration has been established with any Internet or other electronic service providers. An exception exists with respect to the proceedings overseen by the Czech Supreme Court where for the purposes of the identification of an IP address and tying it to a specific physical address/subscription where the expertise of an Internet Service Provider has been sought.

In all cases an emphasis had been stressed by the court on the need to bring in an expert witness during the proceedings. The defence in the various proceedings had argued that failure to appoint an expert witness constitutes a main procedural error. While the Constitutional Court never stipulated that courts must always appoint expert witness during all proceedings, the Constitutional Court did rule that courts need to comply once the defence raises such objections. A possible way to deal with such objections is by actually summoning an expert witness. When doing so, the respective expert witness needs to be selected based on their knowledge of the specific operating procedures and tools used. Otherwise, such expert reports will be reported as flawed as done by the Czech Constitutional Court.

8.3. Nature of legal issues

The legal issues in the four cases mainly cover three major topics concerning 1) the indisputability of e-evidence by courts, 2) the hesitance of courts to collect or appoint additional evidence and forensic expert assessments, and 3) basing judgements on insufficient e-evidence.

As provided in the first case, lower courts rarely question electronic evidence in a manner which leaves no doubt that it could have been altered or changed in any way (intentionally, negligently, or accidentally). As such, courts often fail to comply with their obligation to deal with all raised doubts about the evidential reliability of the evidence used. In the present case the lower courts had failed to provide an independent verification of the accounting system in accordance with the objections to the accuracy, reliability, and integrity of the evidence. Furthermore, when the defendant offered a logically consistent justification for the submitted data from the accounting system, the courts did not supplement the evidence to establish the truth in view of the charges against the defendant. And thus, breached their duty to examine the reliability of the incriminating evidence.

The main dispute in the second case focused on the argument that the lower courts did not sufficiently reflect the objections directed to the defects of the primary evidence, i.e., the wiretaps, upon which the defendant was sentenced. It has been explicitly pointed out that the prosecutor's order, authorising the wiretap, did not contain any information that would specify the defendant's identity. Thus, no suspicion was established that the person under surveillance had a specific relationship to a particular criminal activity, thus neglecting the necessity of making audio and visual recordings. Despite these circumstances, however, the lower courts did not deal with the legitimacy of the wiretap recordings in a constitutionally compliant manner as they rejected the evidentiary claims, played the audio recordings and considered the wiretaps as a reasonable intrusion of privacy. Thus, they made conclusions about their acquisition contradicting the evidence on file.

As part of the third case, the Constitutional Court dealt with two issues in parallel: (i) the admissibility and proportionality of the deployment of wiretaps; and (ii) the integrity of recordings. Due to the specific method of recording and the classified nature of operational procedures and tools, anomalies were caused that required for an officer of the ÚZČ (the technical unit of the Police of the Czech Republic providing wiretaps) to be summoned. During his testimony a number of contradictions have been identified. Despite the shortcomings of his testimony, the courts were satisfied with its conclusions and no options were provided to the defendant to argue the procedure, thus interfering with his fundamental rights. In the constitutional proceedings it was emphasised that a recorded person must always have the opportunity to argue not only the legality but also the quality, testimonial value and authenticity of the recordings. Therefore, the lower courts must reasonably dispel any doubts regarding the authenticity of the recordings. This must be done by reviewing the raised objections against the prosecution's indictment (especially if expert witnesses support them) and then declassify disputed facts or exclude evidence that lack certainty. Despite the room for improvement in terms of the expert witness, it

remains of the defendant's responsibility to raise objections that are not superficial but to challenge in detail the respective e-evidence. Once such complaints are raised, the proof of burden shifts to the state authorities to prove that the e-evidence is properly collected and verified.

In the fourth case it has been established that the findings of the courts of inquiry lacked a reliable basis for a precise and unquestionable determination of the perpetrator. For the perpetrator to be individualised, it was necessary for an expert assessment to be done on the device and the IP address and on the respective skillset necessary to operate the respective DC++ networks. Due to the nature of IP addresses more than one person had access to the respective computer and committed the copyright infringement. The lower courts never appointed additional expert assessments but rather assumed that the defendant is the perpetrator based on his previous work experience rather on an appointed expert assessment. Since he had previous experience working in a computer manufacturing company, the defendant was assumed to be more qualified to use DC++ networks than the other persons with access to the computer. As concluded by the Czech Supreme Court such question cannot be resolved with the necessary certainty by mere general assertions about the defendant's employment, the absence of formal training with his companion or the pornographic nature of one of the audio-visual works shared.

8.4. Nature of practical issues

All cases seem to focus on the aspect of the lack of taking into consideration the option for manipulation of e-evidence, the need of an expert assessment, the procedural imperfections of the investigative and prosecution authorities and the insufficiently collected evidence for delivering a judgment on the matter.

Due to the lack of awareness of the specifics of the respective evidence concerning its integrity and credibility, the prosecuting authorities did not adequately assess whether it was necessary to use a forensic expert to secure and evaluate the evidence. Thus, the law enforcement and the public prosecutor made the initial assessment of the evidence which proved to be insufficient and potentially inaccurate.

The second case examined the use of wiretaps and recordings as e-evidence and the use of wiretaps as stand-alone evidence proved problematic and without sufficient justification for its use since such e-evidence could have been obtained unlawfully. Despite the objections of the defence, the lower instance courts did not sufficiently address the potential invasion of privacy associated with the use of the respective electronic evidence and did not reasonably doubt the potentially unlawful conduct of the prosecuting authorities.

The third case continues to build upon the use of recordings as e-evidence. When challenged by the defendants, the respective tools and operational procedures for the collection of the recordings must be examined, for example by expert witnesses, despite them not being public. In such cases, the defence needs to make specific claims regarding the integrity of the recordings since not all breaches are relevant to the presumption of innocence. Furthermore, when assessing classified procedures, forensic experts' conclusions cannot be rejected on the premise of being flawed due

to lacking knowledge of the respective procedures. Rather, the prosecution must address them sufficiently and the court must review them exhaustively.

The final case emphasised on the fact that courts cannot rely on assertions and assumptions when assessing situations for which they are not qualified but must rely on expert witnesses. Expert assessments are required when a crucial practical aspect is confirming the circumstantial (indirect) nature of electronic evidence and emphasising proof (and achieving a high standard of certainty) to create a closed chain of circumstantial (direct) evidence.

8.5. Victims and defendant – two sides of the criminal proceedings

No specific peculiarities were present with respect to the parties, save for one of the cases where the defendant had the capacity of a lawyer. These circumstances additionally troubled the review of the wiretaps. The e-evidence, however, was successfully included despite the recording of communication between the parties that would constitute attorney-client privilege.

Other than the raised complaints by the defendants in the respective cases, no other procedural errors and violations seem to have occurred. As per the judgements of the Czech Constitutional Court, the procedural violations against the respective parties have been nulled and voided.

8.6. Conviction rates

Most of the judgments delivered by the Czech Constitutional Court upheld that violations were committed against the respective defendants, thus affecting their fundamental rights such as the principle of *in dubio pro reo* and the right to fair trial. As such the respective charges against the defendants have been nulled and voided. Only one of the cases has resulted in a judgment due to the superficial objections to the integrity of the e-evidence. The defendant was convicted of fraud and sentenced to twenty-five months' imprisonment, suspended for forty months, a fine of CZK 100,000 and compensation for damages of CZK 550,000.

In addition, the proceedings before the Czech Supreme Court have also resulted in the annulment of the contested decisions and the return of the case to the lower instances for a proper review of the proceedings and the defendant’s objection.

9. Slovenian case law analysis

CASE	CASE 1	CASE 2	CASE 3	CASE 4
Type of crime	USE OF MALICIOUS CODE	MURDER	BRIBERY	OWNERSHIP AND DISTRIBUTION OF CHILD PORNOGRAPHY
Collaborations	CROSS-BORDER AND EXPERTS COLLABORATION	EXPERT WITNESSES, SERVICE PROVIDER	CROSS-BORDER COLLABORATION	CROSS-BORDER COLLABORATION, SERVICE PROVIDER
Legal issues	NATURE OF PRIVATE COMMUNICATION	EXAMINATION OF ELECTRONIC EVIDENCE	EVIDENCE COLLECTION AND VERIFICATION	LAWFULNESS OF ELECTRONIC EVIDENCE
Practical issues	DEFENDANT'S LACK OF ACCESS TO EVIDENCE	MISINTERPRETATION OF EVIDENCE	ACQUISITION OF DATA FROM SERVICE PROVIDER	AUTHORITIES MALPRACTICE
Presumption of innocence	AFFECTED BY THE DEFENDANTS' LACK OF ACCESS	AFFECTED BY THE COURT'S MISINTERPRETATION	AFFECTED BY THE LEVEL OF SUSPICION REQUIRED	AFFECTED BY THE AUTHORITIES ACTIONS
Convictions	CONVICTION ESTABLISHED	NO CONVICTION DUE TO INCONCLUSIVE EVIDENCE	CONVICTION ESTABLISHED	CONVICTION ESTABLISHED

9.1. Investigation methods and identified issues

Four cases under the Slovenian jurisdiction were presented that dealt with various offences including unlawful access and damage to information system using malicious software, alleged murder, bribery as well as displaying, manufacturing, possessing, and distributing of pornographic material. In all cases the use of e-evidence proved to be essential to the determination of guilt of the respective defendants and to the respect to the fundamental and procedural rights of the defendant.

The first case concerns the use of malicious code, which automatically and covertly was spread to IT systems via USB sticks, MSN instant messaging and file-sharing networks. The malicious code was used to carry out distributed attacks against infected computers, resulting in the control and management of large numbers of computers, the inoperability of their services, the extraction of personal data and passwords, and the concealment of the identity of the network holders of the code. As such distribution and unauthorised access to numerous information systems can easily be established. It was argued that the e-evidence should be excluded due to it being inadmissible and access to it restricted despite the numerous repeated motions to inspect the electronic evidence.

The second case is focused on the use of mobile tracking data and security camera recordings as evidence and the violation of the defendant's constitutional rights and the procedural rules concerning the trial for murder of a public figure, namely the director of the National Institute of Chemistry (NIC) in Slovenia. Furthermore, during the investigation activities, a search of the defendant's computers resulted in the lack of recorded activities on the hard drives during the critical time which was as one of the facts indicating the absence of an alibi at the time of the victim's murder. Certain issues were present, connected to the service provider's inability to provide the court with information about the base station to which the defendant's phone was connected and his exact location at the time of the crime that essentially were not fully reflected by the court. An objection was also raised with respect to the possibility of identifying the respective culprit of the crime through the presented video recordings. As such the negligence by the court on these circumstances was stated by the defence to have violated the defendant's right to defence, right to equal protection and right to be treated impartially.

The third case deals with bribery received by a District Court judge with the intervention of two accomplices (co-defendants) in order to carry out numerous acts within the scope of his position for the benefit of a person who was a subject of criminal proceedings. The criminal act has been carried out by requesting and accepting a gratuity in the amount of nearly EUR 100,000 for himself as a District Court Judge of the District Court in Celje, and thus in acting in a public function, in order to abuse his position within the limits of his official prerogatives. Certain objections were raised in connection to the range of the electronic data that can be collected and used by the court or investigative authorities at a moment when the defendant is not yet suspected of criminal offences, as well as to the possibility of post factum re-examination of the orders for carrying out covert investigative measures.

The fourth case concerns ownership and distribution of child pornography in the form of pictures or videos on public networks. The files containing illegal content were exchanged through the so-called peer-to-peer file sharing network. Among the Dynamic Internet Protocol (IP) addresses of the users of the network was also a certain dynamic IP address, which was assigned by a Slovenian internet service provider. Based on the obtained data, the Slovenian police requested the internet provider to disclose personal data regarding the respective user to whom it assigned an IP address. Additionally, an order was issued requesting the internet provider to disclose both the personal and traffic data regarding the IP address in question. Furthermore, during a carried-out house search four computers were also seized and copies were made of their hard disks that revealed that one of them contained files with pornographic material involving minors using a file sharing program, eMule. The program allowed to download different files from other users and automatically to distribute personal files to third parties. Objections were raised with respect to the fact that every computer in the network acted as a client and a server was also the main drawback of the network, since there existed the risk of transferring unwanted

files due to the lack of any effective control over the content of the files available for transfer.

9.2. Collaborations

National and/or foreign court experts and expert witnesses were involved at different stages of the proceedings and different instances. In addition, on some occasions, collaboration was established with the local telecom operators with respect to the collection of traffic data.

In the first case the investigation and prosecution authorities were notified by foreign FBI agents and undercover agents that have allegedly communicated with the defendant by email, documented such communication, and forwarded the recordings to the authorities of the Republic of Slovenia. In addition, the Slovenian District Court appointed a Forensic Expert on IT, Software and Computer Science during the proceedings.

In the second case the first instance court considered the opinion of multiple expert witnesses and court experts, both national and foreign, however none of them were appointed to examine the technical aspects concerning the e-evidence. There were however appointed forensic telecommunication experts. In addition, the court has collaborated with a local Slovenian telecom service provider for the obtaining the traffic data of the defendant's mobile phone. A representative of the telecom service provider was also questioned regarding the coverage area of the respective base stations that were collecting and tracking the traffic data.

In the third case the Slovenian court made cross-border inquiries with Interpol Zagreb (Croatia) to establish the circumstances of the police proceedings relating to the cancellation of the arrest warrant, which was also among the criminal offences the accused was charged for. Information on the procedure at the Gunja border crossing point between Bosnia and Herzegovina and Croatia was obtained as well. Outside of this no other cooperation with regard to any electronic service providers in connection to the examination of the call records between the parties.

In the fourth case there was a cross-border collaboration between the Slovenian and the Swiss police in obtaining electronic evidence relevant to the criminal proceedings. In addition, both the Swiss investigation authorities and the Slovenian judicial authorities have collaborated with a Slovenian internet service provider regarding the disclosure of data connected to the user to whom it assigned an IP address which was recorded by the Swiss police. In response, the internet service provider gave the police the requested data (such as name, address, and telephone number) of the owner of the respective assigned IP address.

9.3. Nature of legal issues

The legal issues in the four cases mainly cover several major topics concerning the collection of e-evidence without an issued order by the court and its admissibility, the

re-examination of e-evidence gathering through covert investigative measures along with the range that can be obtained of such data, the right of privacy when collecting various data during investigations and the interpretation of e-evidence.

In the first case the examined legal issues were mainly focused on the dispute of whether subsequent communication by e-mail following advertisement of sales on the Internet constitutes as private communication and whether such communication should be protected under the privacy of communication as part of the fundamental rights provided for in the Slovenian Constitution. It was maintained that if this is to be the case, the respective e-evidence obtained through these measures should be considered as inadmissible. It was essentially found by the Constitutional Court that such subsequent communication by e-mail is to be interpreted differently to the public advertisement of sales and it does constitute private information. It was emphasised that merely by making his or her email address public, an individual does not necessarily relinquish his or her reasonable expectation of the privacy of the contents of subsequent communication via the email address in question. Therefore, the Constitutional Court held that a reasonable expectation of the privacy of such communication by email exists, and therefore the surveillance of the latter entailed an interference with the right to communication privacy. On the matter of the inadmissibility of the evidence, it was maintained that such evidence should not be examined in court since a significant extent on the evidence from the United States of America was obtained by a breach of the defendant's communications privacy. The FBI agents were engaged in a covert operation which was based solely on a letter from the US General Attorney's office and monitored communications on internet forums which are not publicly accessible. Furthermore, the respective FBI agents also allegedly communicated with the defendant through a fictitious identity in respective communication platforms, which are also not publicly accessible. These communications were documented (producing a "print screen") and provided to the authorities of the Republic of Slovenia, all without a court order. These actions conflict the respective constitutional rights of the Slovenian Constitution, thus violating the privacy of the defendant. It is therefore argued that the expectation of privacy, as it considers that the mere publication of an e-mail address on a publicly accessible website does not necessarily mean that the individual does not thereby also waive the right to privacy with regard to the content of online communications. The defendant also opposed the courts' view that foreign authorities are not required to respect those provisions of the Constitution which is only applicable to the authorities of Slovenia. It was further submitted that a state which allows evidence obtained by a violation of constitutionally guaranteed human rights, or evidence obtained contrary to the rules in force in the state in which the evidence was obtained, fails to protect the human rights as well as fails to ensure that the consequences of violations thereof.

The legal issues in the second case were raised in connection to both the security camera recordings and the data used for the determination of the accused party's location. The assessment of the e-evidence was done by considering all recordings at

the same, thus basing its grounds on approximate time lags of different cameras which essentially led to the inability to determine the defendant's identity during the time of the criminal act. In addition, the court also did not take into account the fact that a possibility existed for the defendant to be located at its home, rather than at the scene on the crime as provided by telecom operator.

The main legal issues in the third case considered (i) the possibility of ex-post verification of judicial decisions during the phase of carrying out covert investigative measures; and (ii) the very range of electronic data that can be obtained by the court or investigative authorities and which exists even at a time when they are not suspected of criminal offences. In this respect, it was concluded that courts essentially require reasons for issuing an order and that the basis for intervention with the defendant's privacy of communication can be found in the decision to initiate an investigation, which contains the proposal and the indications as to the grounds for suspicion. The statement of reasons for the decision to initiate the investigation is, however, allowed when they are based on objective criteria for access to data based on the intention to commit a crime which was already being monitored by other Secret Surveillance Measures at the time of the orders. In such circumstances, neither the retention of such data, which is limited, as regards the categories of data stored, the means of communication used, the persons involved and the duration of the retention, to what was strictly necessary for the criminal proceedings, nor the measure of obtaining such data contravenes the constitutional requirement of proportionality of the interference with the privacy of communications. In respect to the range of electronic data, it was pointed out that the protection of privacy of communication covers both the content of the communication and the circumstances and facts related to the communication, i.e. traffic data. In addition, such protection is also granted over the information on the frequency of communications, as well as the analytical information showing the density and timing of the communications between the telephone numbers under observation and with other telephone numbers.

The fourth case examined legal issues regarding the right to privacy and the right to fair trial when collecting (during criminal investigation) and using (during a trial) electronic evidence. More particularly, it referred to the question whether electronic evidence (i.e., pornographic pictures and videos involving minors) obtained by the police by way of acquiring from an internet service provider the data on the user of the dynamic IP address without a court order, should have been excluded as evidence, in order to ensure the accused person a fair trial. The development of the case included proceedings both before the local Slovenian courts as well as before the ECtHR which seemed to conflict each other. It was maintained by the local courts that the data concerning the IP address and the name of its owner or user represented data that can be obtained without a court order and that such information should not be considered private and protected. Moreover, the Slovenian police had not acquired traffic data about the defendant's electronic communication, but only data regarding

the user of a particular computer through which internet had been accessed. Finally, it was held that, given that the defendant's house search had been ordered precisely for the purpose of seizing his computer and its contents, no additional court order was required for the review of his computer files. The assessment of an Information Commissioner was also requested on the issue of providing data on subscribers of electronic communication to the police on their request who was of the view that it is impossible to separate traffic data from subscriber data, as traffic data alone do not make any sense if one does not ascertain who the person behind these data is, which is an extremely important element of communication privacy. Such traffic data processed for the transmission of communications in an electronic communications network or for the billing thereof, which included the IP address is therefore protected, provided that the applicant hides in any way the IP address through which he accessed internet, and neither was access to the peer-to-peer network used by him in any way restricted. On the contrary however, the defendant had established an open line of communication with an undetermined circle of strangers using the internet worldwide who have shown interest in sharing certain files. Therefore, the expectation of privacy was not legitimate and no interference with his right to communication privacy has occurred, thus leading to the conclusion that a court order was not necessary.

The position of the ECtHR however was essentially the opposite and determined that the defendant's interest in preserving his identity with respect to his online activity protected falls with the scope of the notion of "private life" and that the right to privacy and family life was therefore applicable. As such, it was found that the law in accordance with which the contested measure was ordered lacked clarity and did not offer sufficient safeguards against arbitrary interference with the defendant's rights. Following this conclusion, the ECtHR found that the interference with the defendant's right to respect for his private life was therefore not "in accordance with the law" as required by the Convention.

9.4. Nature of practical issues

The practical issues raised in the cases seem to focus on multiple aspects concerning the procedural and fundamental rights of the defendant including provision of access to e-evidence, misinterpretation of e-evidence, as well as classification and prerequisites for surveillance measures related to privacy of communication.

In the first case the practical issues were mainly connected with the fact that the defendant was essentially denied access to the evidence. It was appealed that due to the established restrictions in terms of the time and scope of the access to the case file during the proceedings, the defendant could not effectively dispute the charges stated in the indictment because he was not provided unlimited access to all evidence in the case file or he was provided such only at a very late stage of the proceedings, thus violating the defendant's right to adequate time and facilities to prepare his defence. What was additionally elaborated was also the fact that a decision cannot be altered by the fact that a defendant's attorney is granted unlimited access to the case

file, as the latter cannot substitute for the defendant as regards factual questions, particularly if these are very specific, as in the case of the computer crimes at issue.

During the second case it was maintained that the practical misinterpretation of e-evidence by the court essentially constituted a violation of the defendant's constitutional rights to defence, equal protection and right to be treated impartially, as well as the defendant's presumption of innocence. It was established that the burden of proof in regard to the unclear and insufficient e-evidence did not lie with the defendant, but with the prosecution, thus essentially leading to the conclusion that the collected e-evidence did not provide certainty of the guilt.

The third case examined the question whether acquisition of data from internet service providers on suspects' communications represents a central step for the use of more serious covert investigative measures and if the requirement for appropriate analysis can be challenged *ex post facto*. It has been concluded that acquisition of such data requires a relatively low standard of proof of reasonable grounds for suspicion, whereas other measures and interferences with communications privacy require a higher standard of proof – i.e., reasonable grounds for suspicion. This is because the data are used to carry out traffic analyses, which are used to justify proposals for other covert investigative measures and for more severe interferences with communications privacy. As such, analyses are generally not subject to scrutiny on whether they are carried out appropriately and can only be challenged *ex post facto*.

The practical issues of the fourth case where essentially focused on the (mal)practice of the investigating and prosecuting authorities which may constitute a barrier to fair trial due to the violation of the defendant's privacy of communication. The Slovenian police requested an internet service provider to disclose the data regarding the respective user who was suggested of committing the crime. The police required the operators of the electronic communication networks to disclose to the police the information on the owners or users of a certain means of electronic communication whose details are not publicly available. Since a new (i.e., dynamic) IP address was assigned to a computer each time the user logged on, such data should be considered as traffic data and considered as circumstances and facts connected to the electronic communication. Thus, it was subject to protection of privacy of communication and the Swiss police should not have obtained the dynamic IP address and the respective identity of the owner without a court order. It was also maintained that the Slovenian police should not have reviewed the files on the computer without a specific court order allowing such a search to be conducted. In addition, the law regulating such access and retention of such data was also lacking clarity.

9.5. Victims and defendant – two sides of a criminal proceeding

No specific peculiarities were present with respect to parties and the victims under the case law except for two of the cases.

The second case was one of the most outstanding and publicly exposed criminal cases of the last decade in Slovenia due to the victim being a public figure, namely the director of the National Institute of Chemistry. Serious controversy arose over the question of why the prosecution never prosecuted another perpetrator, since there was a legitimate doubt that the perpetrator was not the respective defendant due to the faults and insufficiency concerning the e-evidence.

In the other instance the defendant had the capacity of an active judge which however never led to any additional complications.

9.6. Conviction rates

Most of the Slovenian cases have resulted in the respective defendant found guilty of their crimes. An exception can be found only in the second case where the perpetrator was essentially unable to be identified by the collected e-evidence.

Furthermore, follow-up proceedings were initiated before the ECtHR with respect to the fourth case where it was concluded that due to uncertainty of the local legislation and the interference with the defendant's right to respect for his private life, a breach of his fundamental rights was committed.

10. EU case law analysis

Case law analysis of the decisions of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) was concluded to map relevant court decisions that provide insights on the collection and various uses of electronic evidence pre-trial and trial criminal proceedings and its effect on fundamental rights and freedoms of individuals, namely the presumption of innocent. The identified decisions were addressing the topics of fair trial, collection of data for national security purposes, classification of e-evidence, access to data/documents/evidence, cooperation with telecommunications companies, level of specification of search warrants concerning electronic data.

INNOCENT

CJEU CASE LAW ANALYSIS

CASE	CASE 1	CASE 2
Type of crime	FUNDING TERRORIST ACTIVITIES AND PARTICIPATION IN CRIMINAL ORGANISATION	RETENTION OF PERSONAL DATA FROM ELECTRONIC COMMUNICATIONS FOR NATIONAL SECURITY
Collaborations	EIO ISSUING COLLABORATION	NATIONAL SERVICE PROVIDERS AND NATIONAL AGENCIES
Legal issues	EIO ISSUING AND VALIDATION	OBLIGATION OF NATIONAL SERVICE PROVIDERS TO COLLECT AND PROVIDE PERSONAL DATA
Practical issues	INCOMPATIBILITY BETWEEN THE LEGAL PROVISIONS AND DOMESTIC CASE LAW	EXCEPTIONS OF PRINCIPLES FOR NATIONAL SECURITY PURPOSES
Presumption of innocence	CONCERNED BY THE EIO ISSUING CRITERIA	ENHANCED BY THE COURT'S DECISION
Convictions	PROSECUTORS' ISSUING RIGHTS ARE LIMITED WHEN SENSITIVE DATA IS CONCERNED	DOMESTIC LEGISLATION CANNOT OBLIGE PROVIDERS UNLESS A SERIOUS THREAT IS PROVEN

INNOCENT

ECHR CASE LAW ANALYSIS

CASE	CASE 1	CASE 2	CASE 3	CASE 4	CASE 5
Type of crime	EMBEZZLEMENT, CREATION OF CRIMINAL ORGANISATION, THEFT, TAKING HOSTAGE	THEFT, FRAUD, EMBEZZELMENT	BREACH OF TRUST OR MARKET MANIPULATION	PRIVACY VIOLATION	CYBERVIOLENCE
Collaborations	LACK OF COLLABORATION BETWEEN THE AUTHORITIES AND THE PROSECUTION	BAR REPRESENTATIVE	FORENSIC DIVISION AND INVESTIGATORS, PROSECUTION AND DEFENCE	ANTI-TERRORISM TASK FORCE WITH SERVICE PROVIDERS	CROSS-BORDER COLLABORATION, SERVICE PROVIDERS
Legal issues	INFRINGEMENT OF ART.3,5,6 OF ECHR	EVIDENCE LAWFULNESS, LEVEL OF REASONABLE SUSPICION	ACCESS TO INFORMATION	SURVELLIANCE CONDITIONS	ELECTRONIC EVIDENCE SECURING, THREAT LEVEL
Practical issues	POLITICAL FACTORS AND PUBLIC AWARENESS	WARRANT UNCLARITY, DEFENDANT'S POSITION AS LAWYER	VAST AMOUNT OF DATA	BALANCE BETWEEN PRIVACY AND NATIONAL SECURITY	LACK OF CONSIDERATION FOR ELECTRONIC EVIDENCE AND ONLINE CRIMES
Presumption of innocence	INFRINGED BY PUBLIC STATEMENTS	INSUFFICIENT LEVEL OF REASONABLES SUSPICION	AFFECTED BY THE EVIDENCE COLLECTION METHODS	AFFECTED BY SURVELLIANCE METHODS	OVERLY RELIED ON
Convictions	BREACHES OF ART.3,5,6 ECHR HAVE BEEN ESTABLISHED	VIOLATION OF ART.8 ECHR	VIOLATION OF ART. 6.1 ECHR DUE TO LACK OF OBJECTIVE IMPARTIALIT	VIOLATION OF ART.8,ESTABLISHED, CONNECTED TO ART.6	VIOLATION OF ART.8 ECHR

10.1. Investigation methods and identified issues

10.1.1. CJEU

The identified issues by the CJEU mainly concern the disclosure of information from telecommunication companies and the criteria for lawfulness of data retention.

I. One of the identified issues[91] is related to the lawfulness of a European Investigation Order ('EIO') that requests access to traffic and location data from telecommunications company of other Member States on the grounds that e-communication involving defendants has occurred. Such EIOs request data on the communications from defendants' devices that could determine whether a crime has been committed.

When determining the admissibility of such evidence, a question remains as to whether prosecutors and other investigation authorities can request the gathering of traffic and location data in order for it to be consequently used as part of the indictment against the defendant provided that domestic rules in the respective Member States stipulate such competence only to judges. In some judicial systems, the prosecutor can only ask the respective judge for the issue of such orders and not submit them themselves.

It was therefore inquired whether a decision made by a national authority which is required to issue a request for a telecommunications company of the respective Member State to reveal traffic and location data, can acceptably substitute the decision which should have been issued by the judge of the issuing State in order to guard the legality and inviolability of private life.

II. The other major issue[92] focuses on the lawfulness of an obligation provided by domestic laws stipulating that telecommunication companies are required to provide information for the purposes of national security and its retention by the respective authorities. When determining the lawfulness of such an obligation, a 'strict' proportionality must be established with respect to the person's fundamental rights. In such an event, a review must be conducted by the respective judiciary or administrative authority with obligatory power to prevent abuse of power.

As such, the Court was enquired to rule on whether domestic laws can allow a national authority to oblige electronic communication services' providers to disclose information to security and intelligence agencies for national security. In addition, it was inquired as to whether providers of electronic communications services can be obliged to retain traffic and location data by domestic legislation and use automated analysis and real-time collection of traffic and location data without notification to the persons whose data is being processed.

---

[91] Case C-724/19

[92] Joined Cases C-511/18, C-512/18 and C-520/18

10.1.2. ECtHR

Additional issues have been identified by the ECtHR that that examine aspects of fair trial, classification of e-evidence, access to data/documents/evidence, level of specification of search warrants concerning electronic data.

I. In the case law identified additional issues[93] were assessed regarding cases where e-evidence such as video recordings of statements and log-registers of call records or any other data are not recognized as documents under domestic legislation and thus not presented to the defendants. Such e-evidence was however presented on the premises of the Special Prosecutor and could be seen if requested. In addition, the defence was also delayed with receiving access to the transcripts due to the vast volume of evidence available. The applicants repeatedly complained that their right of access to documents had been violated.

II. In addition, issues[94] have been raised concerning the lack of appointed additional forensic expert assessment or collected evidence by national courts despite the lack of decisiveness of electronic evidence such as calls records and alert reports from electronic tracking devices.

III. Furthermore, questions[95] have been raised relating to the level of detail that a search and seizure warrant must contain so it does not appear too vague. The case law examines a scenario where the warrant in respect of the premises of a practicing lawyer was not confined to data likely to be related to the alleged offences but extended to all data in the office. Following the search, a review chamber authorised the examination of all the materials after noting that the data had been seized in the context of preliminary investigations and that a lawyer could not rely on his duty of professional secrecy when he himself was the suspect.

IV. Another aspect addressed is how much secret surveillance[96] can be used during criminal proceedings. It remains uncertain as to how detailed and precise should the secret surveillance be and what sufficient guarantees are required against abuse and arbitrariness so that it does not violate the Convention since in such events public authorities interfere with citizens' rights of private life, home and correspondence when they search and keep under surveillance homes secretly, monitor electronic communications and computer data transmissions and make recordings of any data acquired through these methods.

V. The final case glances over the question[97] of effective and timely investigation by authorities against recurring acts of cyberviolence. In the examined case, authorities failed to protect a citizen from recurring acts of cyberviolence for approximately three years. This included disseminating intimate photographs

[93] Sigurdur Einarsson and Others v. Iceland
[94] Korban v Ukraine
[95] Robathin v. Austria
[96] Szabó and Vissy v. Hungary
[97] Volodina v Russia, Volodina v Russia (No.2)

without consent, impersonation through the creation of fake social-media profiles and tracking with a GPS device. Authorities have been accused of failing to conduct an effective investigation into these acts.

10.2. Collaborations

All identified cases have different collaboration aspects, while none concern cross-border collaboration. In most of the CJEU and ECtHR case law national service providers had been collaborating with the respective national authorities regarding the retention of relevant data. This collaboration, however, was of obligatory nature as they were required by their respective domestic laws to provide such information.

In the CJEU case law, the principle of mutual trust is discussed regarding the acceptance and execution of an EIO. The CJEU outlined that even though an executing state cannot refuse to accept an EIO without valid ground, it can propose as an alternative less intrusive measure if it serves the same purpose. In addition, the grounds of non-recognition and non-execution are also clearly provided for in the EIO Directive or as well as the rules so the Member State are able to follow these guidelines and not violate the existing mutual trust.

The main topics covered in the ECtHR case law focus on the procedural consequences of collaboration at local level:

I. The investigation team was collaborating with the respective computer forensics division of the police on tapping the applicant's phone call and its examination and relevance to the case. During this collaboration process, however, aspects related to lawyer-client confidentiality have not been accurately assessed and certain calls have not been deleted as they should have been, thus leading to additional procedural difficulties.

II. Information was requested by national social network platforms regarding fake profiles and the disseminated personal data and photos. One of the many factors that led to the delayed investigation was due to the year-long late response from the respective service providers. In addition, the tracking devices that were found have been sent to the special technical measures bureau in order to be reviewed in more detail. However, technical means were not fully used to determine the number of the SIM card installed on the device using the service provider's network infrastructure.

    Records of phone communications have also been requested from the Azerbaijani authorities in connection to the Azerbaijani number used for the creation of the fake accounts. They managed to identify the name of the owner of the number. However, the connection between him and the suspect was never investigated, thus showing that the collaboration with the Azerbaijani representatives could have been of use if the investigative authorities have investigated the received data into more details. The data collected from phone and Internet providers was also not entirely examined for the necessary evidence to be compiled by the prosecution.

III. Various flaws could be found also within the formal indictment prepared by the prosecution since not all of the investigator's suspicions were communicated to the prosecution. An example of that was the fact that the alerts from the electronic tracking device were presented to the prosecution as technological errors, while there were suspicions that they were due to the applicant's interference with the device.

10.3. Nature of legal issues

10.3.1. CJEU

The nature of the legal issues analysed by the CJEU investigates two main legal questions regarding the disclosure of information from telecommunications companies and the criteria for data retention lawfulness.

I. The first question is focused on whether a public prosecutor has the competence to issue an EIO under Article 2(c)(i) of Directive 2014/41 during the pre-trial stage that requests the access to traffic and location data, while another national case outlines that this competence is exclusively granted to the judge. The CJEU had to investigate if the interpretation of "issuing authority" defined under Article 2(c). Article 6(1)(a) obliges the issuing authority to evaluate the necessity and proportionality of the EIO and the evidence requested. In addition, the Directive also requires further reasonings on the need for issuing an EIO, especially in cases of financial data request. Therefore, the CJEU concludes that to conduct the assessment and provide the necessary reasoning, the issuing authority should be investigative. Also, to issue the EIO, this authority must be allowed to do so under national law. This means that if under domestic legislation the public prosecutor does not have the right to order an investigative measure to receive traffic and location data, then they could not be acting as an issuing authority under Article 2(c)(i). Therefore, in the current case, even though the Bulgarian law outlines the public prosecutor as the competent authority to issue an EIO, domestic legislation grants the power to request traffic and location data from a telecommunication company exclusively to the court. This leads to the conclusion that the power of the public prosecutor in Bulgaria does not extend to the gathering of such type of data by way of EIO's issue.

II. The second legal question before the CJEU is whether an executing country's approval of an EIO requesting traffic and location data can substitute the wrongful validation of the same EIO by the issuing state. Article 6 of Directive 2014/41 outlines the conditions for an EIO and states that if the executing country has concerns, it could consult with the issuing state. In addition, the executing authority can also reject the EIO on the grounds of non-recognition or non-execution described under Article 11. Considering these aspects, the CJEU concludes an executing State cannot compensate for the infringement of the criteria under Article 6(1). However, an executing state could not refuse to execute the EIO on other grounds but only to suggest a less intrusive measure if possible.

10.3.2. ECtHR

Regarding the ECtHR cases identified, no specific common link can be established. The cases, however, provide vast insight into how e-evidence should be dealt with so that the defendants' interests are duly secured.

I. One of the legal issues concerns the issues of collecting documents, their classification, and the establishment of access limits. In connection to this, a question was raised as to whether the defence had the right to examine the vast amount of data the prosecution collected arbitrarily and not included in the investigation file, as well as "tagged" data found through system searches, in order to find material that would be exculpatory. During the proceedings documents/data have been collected in several categories, as following:

- "full collection of data" which encompassed all the material obtained by the prosecution and which included tagged" data as a sub-category "as resulting of searches using specified keywords but not subsequently included in the investigation file;
- "investigation documents", identified from that material by means of further searches and manual review as being potentially relevant to the case; and
- "evidence in the case", that is the material selected from the "investigation documents" and actually presented to the trial court by the prosecution.

The defence was given access to the "evidence in the case" during the hearings and was given a chance to review the "investigation file," which contained information that had not been filed with the domestic court. However, the defence was not given access to the "full collection of data".

(i) The "full collection of data" inevitably included a mass of data which was not *prima facie* relevant to the case. Moreover, for the purpose of identifying relevant data, it is legitimate for the prosecution to sift through the vast volume of unprocessed material to identify and to reduce the file to manageable proportions. Nevertheless, in principle an important safeguard in such a process would be to ensure that the defence was provided with an opportunity to be involved in the laying-down of the criteria for determining what might be relevant. Therefore, in this respect the data in question were more akin to any other evidence which might have existed but had not been collected by the prosecution at all, than to evidence of which the prosecution had knowledge but which it refused to disclose to the defence.

Thus, it was not a situation of withholding evidence or "non-disclosure" in the classic sense, since the prosecution had in fact not been aware of what the contents of the mass of data were, and to that extent it had not held any advantage over the defence.

(ii) While the excluded material was *a priori* not relevant to the case, the "tagged" data because of the initial searches had been prepared solely by the prosecution, without being superseded by any judicial authorities and without involving the defence in the process.

The defence had denied the "tagged" documents on the grounds that they had not existed and that there was no obligation to create such documents. It would have been appropriate for the defence to have been afforded the possibility of conducting a search for potentially exculpatory evidence since further searches in the data would have been technically straightforward, even though under the application domestic legislation no obligation exists for the prosecution to create documents which did not already exist. Since the privacy issues were not insurmountable obstacles in that respect, any refusal to allow the defence to carry out further searches of the "tagged" documents would in principle raise an issue regarding the provision of adequate facilities for the preparation of the defence.

II. At another instance, prosecution authorities and national courts had been dealing with the consistency of e-evidence. At the start of the criminal proceedings, one of the offences raised was making threatening calls to an official. This claim was based on the phone calls that the respective official had received from an individual who presented himself as the applicant. The final judgement does not outline what further evidence had been presented in support of this accusation.

Additionally, it was raised by the investigator that during the applicant's house arrest there had been thirty-eight alerts from the electronic tracking device which was pointed out as evidence that the applicant might have tampered with it. Out of the 38 alerts from the tracking device used during the applicant's home arrest, only 3 were explained reasonably by court hearings and a hospital stay. The remaining alerts were claimed to be fault of the technology used by the device. Despite the uncertainty of the collected e-evidence, these suspicions were not presented to the prosecution and no additional evidence or forensic expert assessments have been appointed.

III. The topic of whether search and seizure of the electronic data for the purposes of crime prevention constitutes an interference with the applicant's right of respect for his "correspondence" has been also analysed. The issue of whether the search warrant is too vague to be in accordance with the law raises the question of proportionality. The warrant was, however, couched in extremely broad terms, as it authorised in a general and unlimited manner the search and seizure of documents, personal computers and discs, savings books, bank documents and donation deeds and wills in favour of the applicant. Although the applicant had benefited from numerous procedural safeguards, the review chamber to which he had referred the case had given only brief and rather general reasons when authorising the search of all the electronic data from the applicant's office, rather than data relating solely to the relationship between

the applicant and the victims of his alleged offences. In view of the specific circumstances prevailing in a law office, particular reasons should have been given to allow such an all-encompassing search. In the absence of such reasons, the seizure and examination of all the data had gone beyond what was necessary to achieve the lawful aim.

IV. Another aspect addressed is to what extent secret surveillance could be used during criminal proceedings. It remains dubious as to how detailed and precise the secret surveillance legislation should be and what sufficient guarantees are required against abuse and arbitrariness so that it does not violate the European Convention of Human Rights.

According to the Hungarian legislation only two scenarios could entail secret surveillance:

(i) the prevention, tracking and repelling of terrorist acts in Hungary; and

(ii) the gathering of intelligence necessary for rescuing Hungarian citizens in distress abroad.

In matters affecting fundamental rights the legislation granting discretion to the executive authority in the sphere of national security must indicate the scope of such discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. Under the national legislation, authorisation for interception could be given in respect not only of named persons, but also of a "range of persons", a notion that is overly broad and could pave the way for the unlimited surveillance of a large number of citizens. For this purpose, the need for the interference to be "necessary in a democratic society" must be interpreted as requiring that any measures taken should be strictly necessary both, as a general consideration, to safeguard democratic institutions and, as a particular consideration, to obtain essential intelligence in an individual operation. Any measure of secret surveillance which does not fulfil the strict necessity criterion would be prone to abuse by the authorities. Although surveillance measures are subject to prior authorisation, such supervision is eminently political and inherently incapable of ensuring the requisite assessment of strict necessity. Therefore, supervision by a politically responsible member of the executive did not provide the necessary guarantees.

V. Finally, the last question examined in the identified ECtHR case law is on the timely matter of investigation by authorities and whether authorities, once aware of a cybercrime interference with a citizen's rights, had discharged their obligations to take sufficient measures to put an end to that interference and prevent it from recurring.

(i) On the question of whether an adequate legal framework had been put in place providing the applicant with protection against the acts of cyberviolence, it was held that the authorities' response to the known risk of recurrent violence had been manifestly inadequate and that, through their inaction and failure to take measures of immediate

deterrence, they had allowed him to continue threatening, harassing, and assaulting the applicant without hindrance and with impunity. This finding was also applicable in the circumstances of the present case in which the authorities had not considered at any point in time what could and should have been done to protect the applicant from recurrent online violence.

(ii) As to how the authorities had investigated the applicant's reports: The investigation was opened late, almost two years after the applicant first reported the fake profiles to the police. Before that, the police had sought to dispose hastily of the matter on formal grounds instead of making a serious and genuine attempt to establish the circumstances of the applicant's malicious impersonation on social media. Since state authorities are responsible for delays, whether attributable to the conduct of their judicial or other authorities or due to structural deficiencies in their judicial system, it is immaterial whether the initial delay was caused by a lack of clear rules on jurisdiction for investigating online offences or by the reluctance of individual police officers to take up the case. Delays connected to the unavailability for questioning of the suspect party are also not convincing. In any event, police authorities are required to act promptly and in good faith to secure forensic evidence of the alleged offences, such as the identification of phone numbers and Internet addresses used to create the fake profiles and upload the applicant's photos. This had not been done, however, until two years later, resulting in a loss of time and undermining the authorities' ability to secure evidence relating to the acts of cyberviolence.

10.4. Nature of practical issues

10.4.1. CJEU

I. The fundamental issues in the identified CJEU case law relate to the examination of whether the evidence is obtained on valid legal grounds under the Bulgarian national legislation and whether any rights of the defendant have been breached under these circumstances. The practical problem is that there is a certain incompatibility between the legal provisions and the principles laid down in domestic case law. Under the Bulgarian law, a public prosecutor has the right to issue an EIO. However, case law shows that the power of the public prosecutor is limited to occasions where certain types of data is concerned. An example of this is the data required in the current case concerning traffic and location information. As outlined in Directive 2014/41, if there is a risk of breach of a person's fundamental rights due to an investigative measure prescribed by an EIO, the respective EIO should not be executed. Although in the current case the presumption of innocence had not been directly infringed, it might be argued that the right to fair trial (Art.6 ECHR) had been put under question. The fact that the public prosecutor has issued an EIO that includes investigative

measures which go beyond his prerogatives had put the defendant's rights at risk.

II. The other practical issues focus on the exemption of the right to privacy usually made in the context of national security. It is the obligation of the court to elaborate clear boundaries and state which measures could not be applied on the basis of national security and combatting terrorism as their nature violates the fundamental rights of the citizens and go beyond the necessity to fulfil its lawful purpose.

10.4.2. ECtHR

I. One of the central practical issues in the case is connected to the dissemination of the vast amount of data and filtering the relevant information necessary for the filing of an indictment. Such data needs to be of nature that serves as grounds for indictment. The evidence presented to the court was summarised which may lead to some inaccuracies or incompleteness.

In addition, when the applicants examined some of their tapped telephone conversations which were stored by the Specialised Prosecutor, they found that among the phone calls there were five calls between some of the applicants and their respective lawyers. Thus, they submitted a complaint. The prosecution responded that an error had been made and the phone calls had not been erased immediately and that they had since been deleted. It was explained that the calls had been recorded by the Computer Forensics Division of the Police and investigators evaluated their relevance to the case. The investigators had been commanded to stop listening to recordings when they became aware that the defendant was speaking to his defence lawyer and not to expose whatever they had already heard. However, an employee did not mention the phone calls in question when writing a report which led to neglecting them when deleting the rest of the calls in the report. The Specialised Prosecutor outlined that the calls had not been listened to and that confidentiality had been respected. Since these recordings were not used as evidence, the court noted that the police could not have anticipated that a specific call would be with the defendant's lawyers and the procedure in place was reasonable.

Finally, despite the frequent complaints to the prosecution about lack of access to documents, the applicants had never formally sought a court order to access the "full collection of data" or for further searches to be carried out, nor they had suggested further investigative measures such as a fresh search using keywords suggested by them. This possibility of a review by the court was an important safeguard in determining whether access to data should be ensured. Moreover, among the evidence submitted to the trial court there were overviews of the seized items and an approximate idea of their contents. In those circumstances and bearing in mind that the defendants had not provided any specification of the type of evidence they had been seeking, the lack of

access to the data in question was not such that the defendants had been denied a fair trial overall.

II. The alerts from the applicant's electronic tracking device ran counter to the documents the prosecution had in possession. As such, the lack of additional collected evidence and the appointed forensic expert assessments leads to the impossibility to conclude if an obstruction of the device has been occurring.

III. The fact that the warrant was written in a way that makes its interpretation broad and difficult was one of the most problematic points in this case. The police officers had to follow the judge's orders after the confirmation to seize all files, while at the same time deal with the opposition from the Vienna Bar Association representative.

In addition, the fact that the applicant is a lawyer also led to a more complicated situation as the professional secrecy of a lawyer also had to be considered when examining the files of the rest of his client. In addition, the law firm was owned not only by the defendant but by his partner as well. While this partner was not a suspect, files that were concerning him and his client have also been seized.

IV. The national legislation did not clarify how the notion of a "range of persons" is applied in practice and the authorities were not required to demonstrate the actual or presumed relation between the persons or range of persons concerned and the prevention of any terrorist threat. In such cases it would defy the purpose of government efforts to keep terrorism at bay, and thus restore citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically replaced by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques. In the present case, it could not be ruled out that the domestic provisions could be interpreted to enable strategic, large-scale interception.

V. According to the claims of the police, the delay caused by the investigation was caused by deficiencies of the domestic legislative framework, namely a lack of clear rules on jurisdiction for investigating online offences.

10.5. Victims and defendant – two sides of a criminal proceeding

No specific peculiarities were present with respect to the parties in the examined case law of both the CJEU and the ECtHR with the exception of two cases where the defendants had a unique capacity – a public political figure and a lawyer.

Due to the country's political environment and the defendant's involvement as a politician, the public awareness of the proceedings was significantly raised. As such, on several occasions during the proceedings influential people have claimed that the defendant had committed serious crimes, which strongly influenced the public opinion of the defendant's innocence. As the court outlined, the words that they used

were particularly important. They breached the presumption of innocence by proclaiming a person guilty before his guilt had been established before the court.

In the other instance the fact that the applicant was a practicing lawyer led to the additional circumstances that were never taken into consideration by the investigation authorities, thus infringing the attorney- client privilege which led to procedural violations, invalidity of evidence and infringement of fair trial.

10.6. Conviction rates

10.6.1. CJEU

The CJEU case law held that EU law requires the respective issuing authorities to provide reasonings for the sought investigative measures and to provide a safeguard for the fundamental rights of the individuals concerned. Additionally, domestic legislation is prohibited to oblige] electronic communications services' providers to conduct general and indiscriminate transmission of traffic and location data to national security agencies for the purpose of national security.

I. The criteria for issuing and transmitting an EIO should mitigate the potential abuse of the right to fair trial, right to privacy and the presumption of innocence. In addition, the executing authority is also provided with the opportunity to suggest alternative measures that will not interfere with individuals' rights and serve the same purpose.

II. The CJEU stated that an obligation to conduct general and indiscriminate transmission of traffic and location data affects the protection of privacy and personal data, and it is conflicting with the principle of freedom of expression. Only in cases where there is a severe threat to national or public security such a measure could be imposed; however, they must be 'strictly' proportionate to the purpose sought.

10.6.2. ECtHR

Most of the identified ECtHR decisions stipulate that violations were committed against the respective defendants. The decisions do not discuss in detail the electronic evidence in the case. Some of these judgements do not rely on the e-evidence presented in the respective cases due to them being seen as insufficient and unreliable evidence. Mostly the violations result either from the investigation process being faulted or the fundamental rights of the person concerned being affected.

Only one of the cases has resulted in a decision that finds a lack of violation due to the passive behaviour of the defence with respect to their option for requesting data to be included in the case's evidence.

11. Comparative analysis of Eastern Europe National case law and EU case law

Both the analyses at national and European level show the importance of electronic evidence during both the pre-trial and trial phase of the criminal proceedings. Furthermore, the analysis demonstrates that collaboration with expert witnesses/ forensic examiner, and service providers is mainly conducted at national level as the ECtHR and CJEU review cases that have already gone through review by the respective national court. Nevertheless, it could be argued that all identified case law shares common type of both practical and legal issues.

The main trends noted by the researchers which identified the case law is that there are existing issues within the examined jurisdictions in terms of how e-evidence is collected and handled by the investigative and prosecution authorities. This is further exacerbated by the limited capacities of the court to appropriately review and construe the presented electronic evidence, in particularly visible at the lower courts' level where low awareness is observed. The same is likewise applicable to the prosecution as some of the identified case law revealed there is a lack of appropriate understanding how current technologies function which might not only breach the presumption of innocence but to also to erroneous judgement. It was reported that in some cases all electronic evidence is excluded in the materials of the case by the prosecution. It was highlighted that in some of the examined jurisdiction, at the lower courts' level, the involvement of forensic examiners is not sought.

Another major point is the efficiency of the collaboration with electronic service providers, since this is an important element in the evidence collection process. It was reported by the INNOCENT research team that in some of the examined jurisdictions that such collaboration is oftentimes the last resort for the investigation authorities, rather evidence is sought directly from the victim and/ or the defendant. Yet, all partner countries' domestic legislation clearly outlines how such collaboration should be executed.

12. National and European legal gaps in the context of electronic evidence

The identified case law allows for the identification of existing gaps in the applicable legislation when it comes to the use of electronic evidence in the criminal procedure.

In one of the national cases identified, a question before the court was raised with respect to the format in which the evidence should be presented as one of the lower instance courts have established that an electronically provided evidence is only a copy of the actual evidence. This was revoked by the higher court; however, it was established that the format of the evidence in a case could be consistent. Therefore, if the initial evidence is presented as a paper document, then the one discovered at a later stage should not be in an electronic format. This shows that some of the national courts are not entirely prepared to deal dynamically with different forms of evidence, especially when it comes to electronic evidence. What is more, during the focus group organised within the INNOCENT team, researchers have shared that there might be a

need to introduce specific provisions that deal with the handling of e-evidence at both pre-trial and trial stage of the proceedings. It was shared that there is a lack of specific requirements alongside vague statements that all evidentiary rules – search or interception can also be used for collecting e-evidence. Only in one of the partner countries there is legislation that outlines e-evidence handling, introducing temporary seizure and analysis of electronic data as regular investigative measures, as well as all procedural guarantees and special investigative measures.

Every case has its individual circumstances that may often lead to making the collection of evidence in a consistent format impossible. It could also be claimed that presenting of evidence in a coherent manner can contribute to avoiding the negligence of certain pieces of evidence. However, this could also be covered by following certain established guidelines and practices in addition to the careful examination and reporting of every finding.

In another national case, the defence questioned the conclusions presented by the expert witness as he was not following the latest methods for the examination of the electronic evidence. The lower instance court ruled that the professional was not obliged to follow the latest practices, especially in they were not scientifically proved. The higher instance court revoked this decision and obliged the court to follow the latest developments in regard to electronic evidence examination and to implement them. However, this case is an example of the fact that both the investigators, expert witnesses/ forensic examiners and lower instance courts are not competently prepared to collect, examine, and access data in electronic format.

13. Implementation of the presumption of innocence and respect for human rights in the researched countries

The analysis presented herewith shows significant percentage of national cases where both the court and authorities treat with respect the defendants' right to fair trial. In several cases a conviction has not been established due to the lack or inconclusive evidence. However, it could also be claimed that in such cases certain traces stemming from electronic evidence were not followed during the investigation, which might had changed the outcomes of these instances. These are examples of overreliance on the presumption of innocence by neglecting pieces of electronic evidence that might have proven the defendant's guilt. However, some of the analysed cases also show that such negligence has infringed the defendant's rights by not considering exculpatory evidence. Among the identified cases, where the presumption of innocence has been violated, this mainly happened at the first instance stage. On the contrary, a significant percentage of the identified case law decisions which enhance the presumption of innocence are delivered by the respective higher instance court or even the supreme court.

Most of the analysed ECtHR case law established that there has been a violation of the defendant's fundamental rights. The selected case law mostly concerns infringements at the pre-trial stage during the investigation or due to a court decision that did not

consider all the evidence or did not appropriately evaluate it. This shows the clear need for improving the competence of both the law enforcement authorities and judiciary in the context of electronic evidence as they currently lack necessary knowledge and skills to evaluate it in the same way as physical evidence or paper documents. In both ECtHR and CJEU selected case law there are examples using surveillance or collection of personal data. In the ECtHR case it was established that the presumption of innocence was indeed affected, while it could be argued that the CJEU case enhances its practical implementation.

14. Level of professional knowledge in regard to electronic evidence examination

In cases where the main source of evidence is in electronic format, the high level of competence and in-depth understanding by both the investigators and judiciary is of great importance. In order to follow certain evidence traces in an electronic environment, the investigative and prosecution authorities should understand what kind of information could be found in potential devices, what methods should be used and how to examine the authenticity and integrity of this type of evidence. In addition, once this piece of evidence is presented before the court, the judges, prosecutors, and lawyers need to be able to apply the legal principles and rules in regard to the facts presented by the electronic evidence.

It is difficult to draw universal conclusions from the identified case law are as there are examples of complete negligence of e-evidence from either the pre-trial authorities or the lower instance courts, while simultaneously there are cases where all good practices and guidelines have been followed. The main types of devices and mechanisms that the investigation, prosecution and the court needed to consider and examine are mobile phones, personal computers, and location tracking. In several cases, collaboration was established with relevant electronic service providers, yet in some, this was done in an untimely manner which affected the outcomes of the case.

A significant percentage of the analysed case law outlines that one of the central practical issues revolves around the examination of electronic evidence. It is observed that both the pre-trial authorities and judiciary had difficulties with either following good practices or with extracting the necessary evidence from various devices. One of the cases shows that the process is significantly complicated if there is a vast amount of data concerned. This might affect the presumption of innocence as large amount of data may include either exculpatory or inculpatory evidence. Therefore, the prosecutors' and judiciary's knowledge and skills to deal with such challenges are significant as it may affect the outcomes the cases. As outlined in the section above, the need of such competences is most noticeable during the pre-trial stage and at lower instance courts.

15. The influence of the gender perspective and sociological factors in the context of the presumption of innocence

Apart from the legal and practical issues that emerged in the cases presented above, there are also sociological factors that influence the criminal proceedings in the different stages.

The cases identified under the Croatian jurisdiction concern sexual abuse offences against children. Such type of crime creates high public interest while putting on focus a vulnerable victim – a child. Nevertheless, in two of the three cases, the victims were actively participating in the proceedings, providing evidence themselves. The provided electronic evidence was one of the main instruments that consequently led to the conviction of the offenders. Although it was not explicitly mentioned, crimes where the victim is a child are usually of extremely sensitive nature as it is responsibility of all the parties involved (investigators, prosecution, lawyers, judiciary, social workers) to maintain the balance between the child's well-being and protection from further harm and the defendants procedural and fundamental rights.

In one of the Slovakian cases which also concerns sexual abuse, although not against a minor, the treatment of the victim greatly influenced the proceedings. The presumed victim was mentally unstable, which the investigators and judiciary assumed was due to the alleged abuse done to her by her father. In order to protect her from further harm and to avoid prolonged proceedings, the examination of electronic evidence was done quite briefly leading to extreme negligence. This case is an example of how gender stereotypes could significantly affect the presumption of innocence, and hence the right to fair trial. Since the crime in question was of highly sensitive nature, the authorities did not focus on the objectivity of the circumstances and did not carry out a detailed investigation, instead the emphasis was put on the issuing of a sentence and protecting the victim from further psychological and psychical harm. It was only on a later stage of the proceedings when it was discovered that the presented electronic evidence was inaccurate and simulated, and the defendants was declared innocent.

Another type of crime that is significantly influenced by sociological factors is violation of a service oath (Slovakian second case) and bribery committed by a public official (Polish third case). In both cases additional factors such as the high public interest influenced the manner in which the investigation, proceedings, and decision-making have been done. Also, the fact that the breach of the policeman service oath was connected to a potential crime that a colleague of his was suspected of committing added aspects that were very controversial and the court needed to consider.

Among the European case law identified, there is a case which has been most significantly influenced by sociological factors. It concerns a defendant which was acting as a politician, making the case widely presented in the respective national media. Some of his political opponents and other officials made public statements that were directly stating unconfirmed facts regarding the defendant's guilt which constitutes a substantial infringement of his presumption of innocence.

As it can be seen from the selected cases there are a number of sociological factors that may greatly influence the outcomes in the criminal proceedings. It is an essential skill for both the prosecution and judiciary to consider them and assess their impact on a certain case. It is their responsibility to evaluate the individual circumstances in each case and take a competent decision that will both protect the victim but also be of full compliance with the defendant's rights.

16. General conclusions from the collected data and identified gaps

Based on the case law analysis, it could be concluded that whenever presented electronic evidence has a central role in the outcome of a case. However, it could also significantly affect a defendant's fundamental rights and legal principles, such as the presumption of innocence.

There are several key elements which need to be considered in order to strike the balance between the use of electronic evidence and the presumption of innocence:

- Due weight should be given to the evidence collection methods being duly reflected as well as the chain of custody.
- Access to the collected evidence should be provided to all procedural parties.
- Electronic evidence should be assessed according to the most current practices based on scientific research by a qualified expert witness/ forensic examiner.
- Constant efforts should be invested to continuously increase and maintain the competence of prosecution and judiciary but also lawyers in terms of critically examining and evaluating electronic evidence.

Appendix 1 Data Collection Template

Details of the case *(Please, include here information of the parties, the competent court, the stage of the criminal proceedings, the year of start and end of the criminal proceedings)*	
Facts of the case *(Please describe the crime, and the key facts of the case that are relevant to the use of digital evidence and its effect on the right to fair trial from legal and practical standpoint.* *Did the accused/defence made any statements in view of the e-evidence, if yes – please provide a summary?)*	
The relevant legal issues (*Please describe key issues in relation to the interpretation of the right to fair trial when applying e-evidence and application of the applicable legal framework.* *Which provisions were applicable in your opinion/which provisions were invoked in the indictment and which in the court's decision?* *Did the charges change at any point in the course of the*	**During the investigation.** **In the prosecution of the offence(s).** **Before the court (reference separately first instance/appellate/cassation court decisions).**

proceedings? How? Was this influenced by the submitted e-evidence?)	
The relevant practical issues *(Please describe key issues in relation to the practice of the investigating and prosecuting authorities which may have constituted a barrier to fair trial in the effective investigation and prosecution of the case. In your analysis, please emphasise practices in relation to the collection and use of e-evidence during the investigation and prosecution of the offence.)*	
Collaboration *(Please include information whether there was ongoing cross-border collaboration, or collaboration with electronic services' providers/ Internet Service Providers. Information about the appointment and statement by expert witness is highly welcome)*	**During the investigation.** **In the prosecution of the offence(s).** **Before the court (reference separately first instance/appellate/cassation court decisions).**
Outcome of the case *(Please describe the outcome of the case, with reference to the different stages of the proceedings (first instance, appellate, etc.). What crime(s) was*	

the defendant acquitted/convicted for? *Was the right to fair trial discussed in the sentence and how? How was the e-evidence evaluated by the Court?)*	
Other *Please mention any additional barriers or good practices, as well as any other elements you deem to have played an important role in the case and were not mentioned in the previous sections.*	