E-capsules Report

VR-DigiJust Project

Digitalising Justice via combined Virtual Reality Training

Project Number: ***101046477***

JUST-2021-JTRA

D2.5 – e-Capsules Report

Version 0.1

The content of this document represents the views of the author(s) only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

1. Change Control

1.1 Document Properties

Deliverable No.		D2.5	
Work Package No.	WP2	Work Package Title	CoP Methodology
Author/s		Robert Ranquet (EEEI)	
Contributor/s		All consortium partners	
Reviewer		Sergio Bianchi, Marina Caneva, Pietro Suchan	
Name			
Date		09.08.2023	
Dissemination Level		SEN	

1.2 Revision History

Version	Date	Comments
0.0	09.08.2023	Initial draft
0.1	05.09.2023	Completed draft
1.2	06-09-2023	Revision
1.3		
1.4		

1.3 Table of Acronyms

AFSJ	Area of Freedom, Security and Justice
Art.	Article
cf.	confer
CJEU	Court of Justice of the EU
CoP(s)	Communities of Practice
ECHR	European Convention on Human Rights
EU	European Union
GA	Grant Agreement
i.e.	id est
Rec.	Recital
TFEU	Treaty on the Functioning of the EU
VR	Virtual Reality
WP(s)	Work Package(s)

1.4 Table of Figures

n/a

2. Executive Summary

With Deliverable D2.5, project VR DigiJust has taken an important step in the process to establish a regional network of virtual training centres to facilitate the effective and coherent application of specific EU cooperation instruments. Six training topics have been identified and described in 6 e-capsules: definition of digital justice; online perquisition, trojan and investigative hacking; gathering, preservation and transmission of e-evidence in the framework of the existing supranational and national legislation; digital investigations, proportionality and respect on privacy and data protection; training on EU law; suggestions for training development).

3. e-Capsules methodology

3.1 Contextualisation of D2.5

Deliverables D2.2 and D2.3 have dealt respectively with designing a multidimensional CoP methodology for the intended interdisciplinary training, and with the actual tenue and outcome of the 4 Cops which were organised during 2023 second term in Italy, Greece, Germany and France/Belgium. During these CoPs, practitioners form various specialties (prosecutors, judges, lawyers, …) have exchanged their experiences and their views on practical difficulties arising when implementing the different European cooperation instruments for transborder criminal procedures.

These experts have been able to engage in open dialogue to define good practice training strategies in the selection of cooperation instruments in relation to their specific competences.

CoP participants have sought to understand the relationship between different judicial systems when confronted with ‘cascade investigations with a wide EU impact’, technologies used in court cases, and instruments of European legal cooperation from an andragogic training perspective.

Deliverable D2.3 has provided a comprehensive report on the tenue and outcome of the 4 CoPs.

3.2 Outcome of CoPs

Several key findings were identified, as shown below (extract from D2.3 conclusion):

"I. In all CoPs, the common denominator and main concern of every participating country was the issue of data collection and the safety of personal data. Despite each country having focused on different aspects of the digitalisation of justice, the ethical and legal management of personal data was a key discussion point. For Italy, the use of the Trojan horse software is a potential risk to privacy and personal data, which is why legislation is set up in a way to only allow authorisation in certain instances, i.e., substantial evidence of organised crime. For Greece, the participants of the CoP were both concerned for the data management of their own personal data during the VR trainings, as well as GDPR being followed during the introduction of new technologies in the criminal justice system, such as the use of AI. France and Belgium highlighted the need for multidisciplinary and diverse groups that would create a cross-regional network with respect to GDPR and personal data. Germany focused on the contradictory role of the GDPR and Directive EU 2016/680 regarding protection of fundamental human rights when it comes to specific categories of crimes.
II. The CoPs of Italy and Greece both mentioned that EU legislation and local legislation for new technologies in the criminal justice system is currently not on the same page. More specifically, Italy highlighted the issue of other countries not recognizing the use of Trojan horse software as admissible evidence, making cross-regional collaboration difficult.
The French, German and Greek CoPs all discussed the topic of practical training on new technologies in the justice system. More specifically, they highlighted a need for more vocational training on the tools, as well as tailored training based on each participant's profession and position within the criminal justice system. The issue of older professionals versus newer ones was also mentioned, about familiarity with new technologies and a need for a more hands-on approach to learning. Furthermore, France and Greece also underlined the need for multidisciplinary trainings on the grounds that professionals will learn from each other and elevate the quality of the meetings. France also mentioned diverse groups and a larger number of professionals to be trained, as well as the need for easier accessibility to resources, such as specialised hardware that will be used for the training. Another aspect that was present in Greece's and France-Belgium's CoPs is the language barrier.
IV. All countries' CoPs dealt with the need for a stronger and synchronized collaboration between countries for the introduction of new technologies in the criminal justice system to be smooth and effective. Moreover, they stressed the need for EU protocols and legislation to take into consideration the regional equivalents of each country.
Lastly, Germany and Greece mentioned the need to set up a specific schedule long in advance, so that the participants can arrange their agendas accordingly. Due to their professions, they need to be made aware of the timeslots and dates for the meetings as soon as possible, to achieve a smooth and effective group training."

3.3 Emerging topics from the CoPs

It has been an upfront consideration for the VR-DigiJust project that principle needs for formation are related to the:

- Council Regulation (EU) 2018/1805 on mutual recognition of freezing orders and confiscation orders
- Council Framework Decision 2002/584/JHA on the European Arrest Warrant
- Directive 2014/41/EU on the European Investigation Order
- Council Regulation (EU) 2017/1939 of the European Public Prosecutor's Office
- Regulation (EU) 2016/679 on (general) data protection
- Directive (EU) 2016/680 on law enforcement specific data protection
- Framework Decisions 829 909, 947 on alternative measures to prison

and their interplay in the framework of the case law of the CJEU and of the ECHR. This is the whole topic-related purpose of implementing project VR DigiJust; these instruments are the cascade instruments.

The CoP methodology has helped to identify more precisely several topics which will be further elaborated in the following of the project, namely:

TOPIC ONE: DEFINITION OF DIGITAL JUSTICE, "digitalization", "digitization", contents, data, metadata, cloud, etc. and their judicial implications.

TOPIC TWO: ONLINE PERQUISITION, TROJAN AND INVESTIGATIVE HACKING. Specific exercises should be considered for online perquisition and the use of EIO.

TOPIC THREE: GATHERING, PRESERVATION AND TRANSMISSION OF E-EVIDENCE IN THE FRAMEWORK OF THE EXISTING SUPRANATIONAL AND NATIONAL LEGISLATION

TOPIC FOUR: DIGITAL INVESTIGATIONS, PROPORTIONALITY AND RESPECT ON PRIVACY AND DATA PROTECTION

TOPIC FIVE: TRAINING ON EU LAW

Topic two and three have been merged into one single e-capsule comprising both aspects of the e-evidence within the procedural dimension.

3.4 e-Capsules

Each of the 5 topics identified above is detailed in an e-Capsule which succinctly presents the context, nature and issues of the topic. Designed to constitute a self-supporting document, each capsule presents the points which justify the need for associated training.

4. Conclusions and further steps

With Deliverable D2.5, project VR DigiJust has taken an important step in the process to establish a regional network of virtual training centres to facilitate the effective and co-herent application of specific EU cooperation instruments. The 5 training topics which have been identified in the present step will be further developed into actual training cases and scenarios (D4.2– Case selection from training scenarios) to feed the training catalogue (D3.5 - Catalogue of digitalised e-training Capsules)

The annexes I-VI are detailing the contents of the 5 topics.

5. Annex I –

TOPIC ONE: DEFINITION OF DIGITAL JUSTICE, "digitalization", "digitization", contents, data, metadata, cloud, etc. and judicial implications. Responsible partner: EPLO

Digital Justice in the EU

Digital justice in the EU is a broad term referring to the activities and policies to modernize the justice system and improve its efficiency using new technological tools, such as VR training. Digitalisation provides easier access to justice for individuals and organizations, faster proceedings by digitalising data that was still on paper, as well as enhancing cross-border collaboration. From 2009, three consecutive Action Plans have been implemented for the digitalisation of justice, while the EU also took measures to combat the impact of the COVID-19 pandemic on justice systems (European Commission, 2020a). Moreover, in order to improve cross-border judicial cooperation, the EU has designed and created a computerized system for communication between member states in civil and criminal proceedings – the e-CODEX system (European Commission, 2020b).

Digital justice processes and regulations were designed with respect to fundamental human rights, and certain technological tools proposed, such as the mindful use of AI applications for more efficient justice systems, IT tools, more accessible information for citizens and easier information exchange for judicial professionals, as well as a monitoring procedure of the digitalisation of justice (European Commission, 2020a).

Digitalisation and digitization

Digitalisation and digitization may sound similar, however there are core differences between them. Digitization is the process of transcribing and/or transforming physical and paper data to digital, i.e., making the analog digital (Dieffenbacher, 2023). Furthermore, it includes the transformation of EU data within a judicial framework from paper to a digital condition, so that it can be easily accessible, transferrable, and travel faster. On the other hand, digitalisation has to do with integrating new technologies and digital processes into

the EU justice system (in this case) to improve efficiency, accessibility and quality (Kimachia, 2022). Examples of the digitalisation of justice in the EU include but are not limited to the e-CODEX system, policies created to integrate new technologies in the judicial system, such as AI systems, as well as training judicial practitioners in new technologies using technology (e.g., VR training).

Another close term to digitisation and digitalisation is the "digital transformation", which can be defined as the future outcome of the digitisation and digitalisation processes (Bloomberg, 2018), that will shape and transform the EU justice system by integrating digital justice.

Data and metadata

The difference between data and metadata is very important, as they are used in different contexts and include different forms of data. Data can be any form of information, either raw or processed and can be used to examine trends and patterns. On the other hand, metadata have to do with context and include details that can assist in working with large data sums. Essentially, metadata is used for global data management systems and can be considered as a tool to extract data from data. Metadata also tend to have a more qualitative nature (Metadata management, 2019; Chilvers & Feather, 1998).

The EU is attempting to collect, process and archive large-scale data using metadata. One example is Eurostat, that uses 2 types of metadata, structural and reference. Structural data is used to identify statistical data and reference data is used to describe concepts, methodologies and determine data quality[1]. This is also used in the judicial system, within the framework of digitalising justice.

Cloud

In order for the EU to expand the justice system within the digital sphere and enrich it with new technologies and tools, cloud services and infrastructures are necessary to sup-

[1] For more information, see: https://ec.europa.eu/eurostat/web/metadata (Accessed 28/08/2023).

port data exchange, management and archival. Cloud services provide a secure space for collected data and will most likely be used in the digitalisation of justice.

Implications to the digitalisation of justice

The digitalisation of justice is a process that will make justice in the EU more efficient, as it tackles crime in modern technological societies. Some implications to consider would be the data security issue, since the data collection and exchange withing the digital justice framework needs to be conducted with respect to GDPR and other regulations. Furthermore, especially regarding the use of AI software and systems, the EU has developed an approach that includes policies to enforce trustworthiness, security, transparency and safety for humans and personal data (European Commission, 2021; European Commission for the Efficiency of Justice, 2019). This ensures the ethical use of new technology for the digitalization of justice and the mindful processing of personal data.

References

Bloomberg, J. (2018) Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril, Forbes, 29th of April [online]. Available at: https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/?sh=7e64525c2f2c (Accessed: 28/08/2023).

Chilvers, A., Feather, J. (1998) "The management of digital data: A metadata approach", *The Electronic Library*, 16(6): 365-372). Available at: https://doi.org/10.1108/eb045663 (Accessed: 28/08/2023).

Dieffenbacher, S. F. (2023) Digitization vs Digitalization: Differences, Definitions, and Examples, 4th of March [online]. Available at: https://digitalleadership.com/blog/digitization-vs-digitalization/ (Accessed: 28/08/2023).

European Commission (2021) Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Fostering a European approach to Artificial Intelligence, 21st of April [online]. Available at: https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review (Accessed: 28/08/2023)

European Commission (2020) Proposal for a regulation of the European Parliament and of the council on a computerised system for communication in cross-border civil and criminal Proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726, 2nd of December [online]. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:c3415d45-3587-11eb-b27b-01aa75ed71a1.0003.02/DOC_1&format=PDF (Accessed: 28/08/2023).

European Commission (2020) Communication from the commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions. Digitalisation of justice in the European Union. A toolbox of opportunities,

2nd of December [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0710 (Accessed: 28/08/2023).

European Commission for the Efficiency of Justice (2019) Possible actions to be taken to ensure a wider dissemination and implementation of the European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment, 5th of March [online]. Available at https://rm.coe.int/cepej-gt-qual-2019-1-en-possible-actions-to-promote-ethical-charter-on/168097a351 (Accessed: 28/08/2023).

Kimachia, K. (2022) What Is Digitization vs Digitalization vs Digital Transformation?, 26th of September [online]. Available at: https://www.channelinsider.com/business-management/digitization-vs-digitalization/ (Accessed: 28/08/2023).

Metadata Management (2019) What is the difference between Metadata and Data?, 3rd of September [online]. Available at: https://zeenea.com/the-difference-between-metadata-data/ (Accessed: 28/08/2023).

6. Annex II –

LegalTech Applications for Justice Authorities' Administrative Support

Large-scale investigations are resulting in large-scale criminal proceedings, i.e. investigations that are characterised by a longer investigation period and that significantly exceed the human and material resources required for average investigations by the police (and public prosecutor's office) are to be considered large-scale investigations. Indicators for this can be, for example, the large number of crimes to be prosecuted, the number of suspects, the number of injured parties, or the amount of evidence to be evaluated. Reference can be done to cases like Enchrochat or Sky ECC, as an example.

The size of such proceedings, both in terms of personnel and data, can lead to a situation in which the rights of those involved in the proceedings, especially the accused, are not sufficiently guaranteed or protected.

In addition, there is a not inconsiderable risk that the available evidence has not been or will not be collected, evaluated and used in the process with sufficient justification, so that special process and project management is required due to the complexity of such proceedings.

Here, it can be helpful to use a system that is supported by artificial intelligence applications during the administrative process; but not when it comes to decision-making (Art. 11 Directive 2016/680).

Use of Evidence deriving from investigation characterised by Profiling

In EU Law, the term 'profiling' refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Art. 3 No. 4 Directive 2016/680).

The use of information collected by means of profiling is generally deemed inadequate before Member States' courts and thus constitutes a threat as to admissibility of evidence. However, law enforcement makes use of profiling methods a strategic level.

It must be clarified to what extent strategic profiling is considered adequate and up from which point in an investigation strategic profiling methods turn into individual profiling.

Technology-supported Predictive Judiciary Decision-making

Predictive tools are regularly used in the judicial sector. These are applications such as VERA2, which are used to conduct individual risk analyses of radical individuals in order to determine their conditions of imprisonment and parole eligibility. Such systems are also used – or: could be used – to determine adequateness of alternative sanctions

However, often these systems are neither partially nor fully automated – the underlying process of prognostic reasoning is still carried out by personnel trained in psychology and criminalistics. Consequently, the quality of decisions, especially related to alternative sanctions, depends too much on the evaluator's knowledge and competences.

The use of standardises technology-driven tools could improve the quality, at least when capitalised on for supporting measures.

7. Annex III – e-EVIDENCE

Table of Contents

1. THE CONTEXT

The technological evolution, the opportunities offered by virtual universes, the quantity and quality of available data, as well as the extension of social networks that make use of the digital world and the internet, in its stratifications, constantly challenge criminal law, trial, and practice, as well as the investigative methodologies of the police forces.

Virtual spaces have opened a new dimension parallel to the physical and territorial ones on which, until now, the jurisdiction has been based to protect national sovereignty. According to the definition given by ISO 27032:2012, the document that "provides guidance for improving the state of Cybersecurity", cyberspace should mean that "complex environment resulting from the interaction of people, software and services on the Internet, by means of technology devices and networks connected to it, which does not exist in any physical form".[2]

On the one hand, technological evolution seems to work positively in the field of penal-processing practice, with new approaches to the management, protection, and exchange of information, i.e., the so-called "digital process". In this area, technological and network development is continuously evolving and affecting the digitalisation of justice and, above all, criminal trial, and practice. On the other hand, the emergence of the need to collect, preserve, and share digital evidence, which goes beyond the territorial boundaries of jurisdictions and traditional criminal law concepts such as those of the *locus commissi delicti*, to which criminal law and trial continue to be anchored, pose unprecedented problems that national legislators have not always been able to foresee. Some data visually illustrate the importance of the virtual phenomenon in terms of security: the EU Council estimates there are more than 10 Terabytes of data stolen monthly with ransomware being one of the largest cyber threats in the EU[3]. Moreover, phishing is identified as the most common initial vector of such attacks. DDoS (Distributed Denial-of-Service) attacks are also among the most common threats. At the end of 2020, the annual cost of cybercrime is estimated to have reached EUR 5500 billion, twice as high as in 2015.[4]

[2] International Organization for Standardization, "ISO/IEC 27032:2012," 2012, https://www.iso.org/standard/44375.html.
[3] "Top Cyber Threats in the EU," February 2, 2023, https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/.
[4] "Top Cyber Threats in the EU."

To fully understand the importance of the intrusion of cyberspace in the field of justice, it should be highlighted that digital evidence is not only relevant for cybercrime, but also for a very high number of other crimes outside the cyberspace. "This explains why e-evidence is relevant in about 85 % of total criminal investigations; in addition, in almost 65 % of surveys where the need to acquire electronic evidence is highlighted, a request to a service provider across borders (based in other jurisdictions) is required. Combining the two percentages shows that 55 % of all surveys include a request for cross-border access e-evidence".[5]

In summary, the biggest challenges facing criminal investigations and justice in the cyber world today refer to data localisation and meta-data, including for the proper preservation of the evidence acquired and the perimeter of 'digital domicile'; the relationship with a universe of private operators who manage technological processes and are holders of static or transit data, from Internet Service Providers (ISPs), to cryptocurrencies managers through complex blockchain chains, to forensic operators who have the technologies to perform pre-investigative analysis, from the use of OSINT systems to forensic experts able to inoculate Trojans or carry out forensic extractions or drones and computer forensics.

There is therefore a need to define the proper transnational characterisation of the crime in which police forces require access to highly innovative investigative tools is often relevant. Moreover, it is important to ensure the balance of interests between fundamental rights and the technological capabilities of technical tools today capable of collecting data in a massive, "trailing" form, according to the rulings of the European Court. Finally, critically evaluating the opportunities and risks of new investigative tools, such as those related to the profiling and use of Artificial Intelligence, becomes essential.

These are all factors that pour their burden of novelty on our ordinary conceptual and regulatory paradigms of criminal cooperation, both judicial and police. In particular, the latter is called for by the new models of multi-agency cooperation, where the private sector plays an increasing role and the police forces as well as the judiciary are called to new forms of collaboration.

[5] Intelligence, F, Cyber Threat and New Paradigms of International Judicial Cooperation: The Role of Eurojust, Criminal System, 2023

2. THE NEW CHALLENGES

Alongside an endemic lack of culture and investigative tools adapted to the evolution of digital evidence, the challenges generated by cloud computing, encrypted communications, and the network distribution of IT services, propose unprecedented problems for justice, still very much set on territorial jurisdiction.

Below we list some of these, which are of great importance for the future of police and judicial cooperation at European level:

2.1 Digital domicile

Digital space often does not coincide with the physical space to which criminal law is accustomed. It follows that the legal category of "domicile", which is essential for defining procedural and substantive aspects of criminal law, takes on a new profile in the digital space compared to the territorial one. The digital domicile is "liquid", in the sense that content with the value of clues or evidence in a criminal investigation can be distributed in very different spaces both from the physical home of the person, but also from where the technological infrastructures to which they are connected, be it a virtual server or a cloud, are "domiciliated".

In addition, virtual domiciles can also consist of social network systems, cloud storage or virtual server distributions that operate on blockchain transmissions. These IT infrastructures are partially present in real homes but have ubiquitous characters and are deperimetralised, therefore becoming attributions that raise the challenge for the judiciary and the police. This is the case for multi-user virtual assets, for example, with a ledger that contains cryptocurrencies found during a physical search in the suspect's home and in the presence of the defender. In this case, the acquisition of the physical proof - the ledger - is easy, but the acquisition of the digital content is much more difficult, since, during the physical search, it is necessary to simultaneously activate mechanisms to access the digital domicile, beyond where it is located (probably in another European country or in a third country) to confiscate the asset, i.e., cryptocurrencies. Moreover, this process needs to be done very quickly to prevent a third party from transferring funds or erasing data with access from yet another location. As complex is the access to multitenant domiciles, where both the virtual spaces and the documentary contents of an IT evidence are managed by several people, in geographical areas also very different from each other, without the service providers knowing where they are located, where the

operators are domiciled, and which components of the IT asset the individual operators have affected.

Therefore, the question of digital domicile has a pivotal impact not only on the procedural aspects, but also on the substantive level of proof and its acquisition and preservation. Similarly, the rights of the person take on a central position too, since it is likely that the acquisition of digital evidence located in a ledger, for example, takes place in an unusual manner compared to the usual physical search procedures, as it is carried out in secret form, without prior authorisation from the judge and without defensive guarantees.

As a consequence, one of the recurring problems related to digital domicile is to determine the competent judicial authority: the judicial authority of the place where the investigations are carried out, the one where the data are allocated, that of the place where the server is located, or where the authority controlling the data is located or, again, according to the nationality of the holder of the data. The whole subject raises, even more upstream, the need to identify a necessary balance between investigative needs, freedom of access to the network, and protection of privacy.

2.2 The e-evidence

The second challenge for judges and investigators is to define what is a useful information element for the purposes of 'digital proof'6, to be consolidated in a debate. The Budapest Convention defines "computer data" as "representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function" (Art. 1, par. b) Budapest Convention)7. Considering the complexity of "computer systems", as defined by the Budapest Convention8, digital evidence may consist of stored data, i.e., information stored on their devices by the individuals under investigation, or computer systems managed by service providers9 or, finally, "traffic

[6] Spiezia, F., Cybernetic Threat and New Paradigms of International Judicial Cooperation: The Role of Eurojust, Criminal System, 2023, pg. 15, footnote 15: Digital evidence is the "complex of digital information that is able to determine whether a crime has been committed or that may represent a link between a crime and its perpetrators." In essence, it is any data or information of a digital nature capable of taking on a probative value.'

[7] Council of Europe, "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data," International Legal Materials, November 23, 2001, https://doi.org/10.1017/S0020782900032873.

[8] Ibidem, Art.1, par. a): "computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".

[9] Ibidem, Art.1, par c): ''service provider' means: any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service."

data"10, that are data in transit between different computer systems, often through multiple digital domiciles and multitenant assets.

It should be noted that in the digital world the concept of "data" is different from that of "content". The data, in fact, in addition to the content (for example of a telephone conversation), also include so-called "metadata", for example basic subscriber information, the type of service used, the identity of the subscriber, the associated telephone number, the IP address used for the registration of the service, the postal address or other geolocalisation metadata, other information relating to the payment of the service, the registration data of the computer domain, the telephone traffic data (date, time, source, and destination of the communication, links to the telephone cells, the direction of the service, the volume of traffic data, and the metadata of the documents uploaded to the service).

Therefore, there are various procedures to follow to acquire these different digital data, depending on their configuration (non-content data, stored content data, real time communications) and the methods of storage, based on the need to maintain the forensic chain in its integrity.

Finally, further complexity is given by the fragmentation of European legislation in relation to the acquisition of so-called "traffic data", where these take place on encrypted computer systems, which therefore require the use of investigative tools such as "Trojan Horses", GPS tracking or digital humint systems, which, in theory, would not require the assistance of police forces and the judiciary in the executing countries and have a very large data collection capacity, beyond the individual target.

2.3 Public-Private Cooperation

In the virtual space there are many actors who can have digital evidence or have access to it. In addition, the technological evolution in digital and virtual universes is very fast, and this requires police forces and the judiciary to collaborate with companies and digital forensics experts to keep up with the techniques used by criminal organisations and their "DaaS" (Digital as a Service) services available on the highly advanced market. This implies the ability to collaborate with Internet Service Providers and various other third parties, with an extension of our investigative perspective that can take into account a plurality of acquisition areas. As

[10] Ibidem, Art.1, par. c): "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Spiezia indicates "Beyond diversity and the need for regulation, public base or private basis, dialogue with internet service providers puts a strain on principles on which we have been accustomed to confronting each other since 1999 and which have become the central pillar of judicial cooperation under the Lisbon Treaty: the principle of mutual recognition, understood as a direct relationship between judicial authorities".[11]

In addition, new actors are entering pre-investigative mechanisms, since online sources of information are changing the ways, people understand and interact with the state and the criminal justice system[12]. Online practices enable new kinds of digital agency[13]. There are newfangled types of justice emerging, including cybersecurity vigilantes[14] who seeks to expose wrongdoing and facilitate justice in non-traditional ways or in ways that usually work outside of the formal criminal justice system. For example, voluntary non-government groups such as Creep Catchers or investigative journalists are now established in dozens of countries. Group members posed as online youth and try to catch people engaged in online/internet sex crimes. Sometimes cyber vigilantes operate at the nexus of policing and the entertainment industry in ways that can alter police practices and justice outcomes[15]. Public police struggle to keep up with these shifting digital and online practices[16]. As a result, the governance of crime in online and digital realms can foster complicated relationships between public police,

[11] Spiezia, F, op.cit., pg. 13.

[12] Sean Patrick Roche, Justin T. Pickett, and Marc Gertz, "The Scary World of Online News? Internet News Exposure and Public Attitudes Toward Crime and Justice," Journal of Quantitative Criminology 32, no. 2 (2016): 215–36.

[13] Kenneth Kernaghan, "Digital Dilemmas: Values, Ethics and Information Technology," Canadian Public Administration 57, no. 2 (2014): 295–317, https://doi.org/10.1111/capa.12069; Lara Karaian, "Policing 'Sexting': Responsibilization, Respectability and Sexual Subjectivity in Child Protection/Crime Prevention Responses to Teenagers' Digital Sexual Expression," Theoretical Criminology 18, no. 3 (2013): 282–99, https://doi.org/10.1177/1362480613504331; Nicholas J. Long, "Utopian Sociality. Online," The Cambridge Journal of Anthropology 30, no. 1 (2012): 80–94.

[14] Mark Wood, Evelyn Rose, and Chrissy Thompson, "Viral Justice? Online Justice-Seeking, Intimate Partner Violence and Affective Contagion," Theoretical Criminology 23, no. 3 (2019): 375–93, https://doi.org/10.1177/1362480617750507; K. K. e Silva, "Vigilantism and Cooperative Criminal Justice: Is There a Place for Cybersecurity Vigilantes in Cybercrime Fighting?" International Review of Law, Computers & Technology 32, no. 1 (January 2, 2018): 21–36, https://doi.org/10.1080/13600869.2018.1418142.

[15] Steven A. Kohm, "Naming, Shaming and Criminal Justice: Mass-Mediated Humiliation as Entertainment and Punishment," Crime, Media, Culture 5, no. 2 (August 1, 2009): 188–205, https://doi.org/10.1177/1741659009335724.

[16] Benoît Dupont, "Darkode: Recruitment Patterns and Transactional Features of 'the Most Dangerous Cybercrime Forum in the World,'" American Behavioral Scientist 61, no. 11 (2017): 1219–43; Lara Karaian and Katherine Van Meyl, "Reframing Risqué/Risky: Queer Temporalities, Teenage Sexting, and Freedom of Expression," Laws 4, no. 1 (March 2015): 18–36, https://doi.org/10.3390/laws4010018; Karaian, "Policing 'Sexting.'"

telecommunications, tech companies, private citizens, and NGOs.[17] It is also important to note that although technologies are changing, these processes remain normative and moralized.[18]

2.3.1 Basic Principles Guiding Public-Private Cooperation in Investigations[19]

2.3.1.1 Do not harm:

It is crucial for civil society organizations (CSOs) to prioritize the safety and well-being of individuals providing information. This involves conducting risk assessments, adhering to professional standards, obtaining informed consent, and protecting sources. CSOs should ensure that their documentation activities do not inadvertently harm individuals or communities involved in the process.[20]

- **Informed Consent**: Individuals should receive a comprehensive explanation regarding the nature and purpose of the activity, the anticipated procedures, the intended use of the gathered information, and potential security risks. It's crucial that individuals comprehend this information to provide valid consent.
- **Voluntary Consent**: Respect for an individual's free will is essential. The environment should be non-coercive, allowing individuals to freely express their opinions.
- **Consideration of Social Context**: Always account for social factors that may hinder an individual's ability to give consent freely. These factors can include cultural influences, gender dynamics, age-related considerations, as well as pressures from their community or family.

[17] Yvonne Jewkes and Majid Yar, eds., Handbook of Internet Crime (London: Willan, 2009), https://doi.org/10.4324/9781843929338; Majid Yar, "The Policing of Internet Sex Offences: Pluralised Governance versus Hierarchies of Standing," Policing and Society 23, no. 4 (December 1, 2013): 482–97, https://doi.org/10.1080/10439463.2013.780226.
[18] Susila Gurusami, "The Carceral Web We Weave: Carceral Citizens' Experiences of Digital Punishment and Solidarity," Punishment & Society 21, no. 4 (October 1, 2019): 435–53, https://doi.org/10.1177/1462474518790237; Robert Werth, "Individualizing Risk: Moral Judgement, Professional Knowledge and Affect in Parole Evaluations," British Journal of Criminology 57, no. 4 (February 28, 2016): azw025, https://doi.org/10.1093/bjc/azw025.
[19] European Union Agency for Criminal Justice Cooperation "Documenting International Crimes and Human Rights Violations for Criminal Accountability Purposes: Guidelines for CSOs" (September 21, 2022), DOI: 10.2812/682168.
[20] BIGOSINT Project, "THB Handbook for Online Investigators and Analysts", (2022).

- **Ongoing Information**: Individuals should be consistently informed about the process. They retain the right to refuse cooperation and withdraw their support until the information is shared with competent national or international authorities.

- **Explicit Consent Required:** Whenever feasible, a documented record of informed consent must be generated. This record may take various forms, such as a written statement by the consenting individual, an audio recording, or any other method that identifies the consenting person and incorporates the following practices:

    - By adhering to these outlined principles, our efforts will be fortified.
    - Abstain from making assumptions.
    - Treat incriminating and exonerating evidence with equal weight, while also exploring multiple hypotheses and theories systematically.
    - Organize activities as information is collected, avoiding any attempts to coerce information sources (e.g., refraining from leading questions).
    - Exercise caution against making legal judgments while gathering information (e.g., refraining from inquiring whether an attack was 'indiscriminate') and assess the reliability of information sources.[21]

2.3.1.2 Objectivity, Impartiality, and Independence:

CSOs must carry out their independent activities objectively, impartially, and independently. They should maintain sound information management practices and keep detailed records of their methods while safeguarding data security and confidentiality. Using coded language or encryption helps ensure data security.

2.3.1.3 Accountability and Legality:

[21] Idem.

CSOs should be aware that they are not entitled to any immunity or privileges associated with official accountability mechanisms. They may be called upon to testify regarding the information they have collected. Additionally, they should be conscious of potential legal liabilities under applicable laws, especially in the country where they operate, and protect their employees' rights and welfare.

2.3.1.4 Professionalism and Respect:

CSOs are encouraged to act with professionalism, integrity, respect, and empathy throughout their activities. They should be sensitive to cultural nuances and vulnerabilities that could impact the information collected. Avoiding payments for information is important, and criteria for supporting individuals involved in the documentation process should be established and recorded.

2.3.2 Basic Standards for Digital Evidence:

In the context of digital evidence collection, CSOs should consider legal compliance, potential risks, and online security. Some important steps and considerations include:

- Performing a security assessment of the digital landscape before commencing online activities.
- Ensuring that personnel conducting online research receive appropriate training.
- Verifying data accuracy, as online information can be volatile and easily change or disappear.
- Capturing online information in its native format or as close to it as possible, including web addresses, HTML source code, and screen captures with date and time stamps.
- Gathering additional data like media files, metadata, and collection information.
- Keeping records of pertinent information, including collector details, IP addresses, and timestamps.

- Storing the hash value for each digital item collected securely on a fresh media device.[22]

3. REGULATORY CHALLENGES

The European Union and its agencies, in particular Eurojust, Europol, and Eu-Lisa, have put in place a complex and growing judicial strategy to support and complement the Budapest Convention of 2001 (ETS No. 185) and its Second Additional Protocol of 2022 (CETS No. 224). The latter, in the Third Chapter, provides for a strengthening of the rules on personal data, in line with the European GDPR (Regulation (EU) 2016/679) and with the so-called 'Police Directive' (Directive (EU) 2016/680), which still are an important point of the doctrinal debate together with the principle of proportionality of investigative and judicial actions in the cyber area.

Alongside supranational instruments, the EU has a vast regulatory apparatus, which is at the heart of the VR DIGIJUST project and which training will focus on the problematic issues highlighted herein. This regulatory framework has its focal points in the following instruments of judicial cooperation:

- Directive (EU) 2014/41 regarding the European Investigation Order in criminal matters;
- Council Framework Decision 2002/465/JHA on joint investigation teams;
- Council Framework Decision 2005/214/JHA on the application of the principle of mutual recognition to financial penalties;
- Regulation (EU) 2018/1805 on the mutual recognition of freezing and confiscation orders;
- Council Framework Decision 2009/948 JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings;
- Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

The heart of this European regulation, when entering cyberspaces, which are very unregulated, still requires harmonisation. Drawing on privacy theory, several researchers show that privacy harms constitute a serious and far-reaching consequence of existing and emerging

[22] Idem.

processes of digitisation in the realm of criminal justice. Digitisation risks creating new forms of privacy inequalities that constrains people's everyday lives and choices in important and long-lasting ways, with marginalised groups being particularly affected.

For this reason, among the content of the VR DIGIJUST project, it is central to harmonise the criminal law framework cited so far with the so-called Stockholm's Roadmap, which represents a set of European legislation guaranteeing the procedural rights of accused or suspected persons in criminal proceedings (Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings).

Alongside procedural rights, European jurisprudence has also intervened several times to protect the principles of privacy in the field of data retention. As Spiezia23 rightly pointed out, reference should be made to the judgment of the Court of Justice of 8 April 201424 which annulled the so-called Frattini Directive No. 24 of 2006 on "data retention" because it is considered contrary, in some of its legal provisions, to the fundamental rights of the individual. In its 2014 Digital Rights Ireland judgment25, the Court of Justice of the European Union annulled Directive 2006/24/EC26 (so-called "Data Retention"), on which the internal rules subject to amendment are based through the above-mentioned amendment, considering that the interference it exercised on the right to confidentiality of European citizens for security reasons was disproportionate. The Court of Justice has returned to the subject with the Sent. 21 December 2016, Tele2 and Watson (Joined Cases C 203/15 and C 698/15)27. Following the judgment of 8 April 2014, in which the Luxembourg court declared Directive 2006/24/EC on the retention of telephone and internet traffic data to be invalid because it was contrary to the principle of proportionality, the Court of Justice of the European Union again intervened against the indiscriminate collection of data. According to the Court, Member States cannot impose on providers of electronic communications services a general and undifferentiated obligation to retain traffic and user location data. As a result of these decisions, a complex

[23] Spiezia, F. (2023). Cyber Threat and New Paradigms of International Judicial Cooperation: The Role of Eurojust, Criminal System
[24] European Court of Justice, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, No. Joined Cases C-293/12 and C-594/12 (ECJ April 8, 2014).
[25] Ibidem.
[26] "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC," 105 OJ L § (2006), http://data.europa.eu/eli/dir/2006/24/oj/eng.
[27] European Court of Justice, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, No. Joined Cases C-203/15 and C-698/15 (ECJ December 21, 2016).

situation has arisen, in which 10 Member States declared unconstitutional (and therefore annulled) the national legislation implementing the aforementioned Directive (on data retention). On the other hand, in 16 other Member States, including Italy, the relevant national legislation is still in force. All this contributes to increasing operational difficulties in cross-border acquisition of digital evidence and leaves in limbo the protection of the fundamental rights involved in the matter.

REFERENCES

Ashworth, L., & Free, C. (2006). Marketing Dataveillance and Digita Online Privacy Concerns. Journal of Business Ethics, 67(2), 107-123.

Atif, Y., & Chou, C. (2018). Digital Citizenship: Innovation in Education, Practice, and Pedagogy. Journal of Educational Technology & Society, 21(1), 152-154.

Atkinson, R., & Rodgers, T. (2016). Pleasure Zones and Murder Boxes: Online Pornography and Violent Video Games as Cultural Zones of Exception. British Journal of Criminology, 56(6), 1291-1307.

Barbosa Neves, B., Fonseca, J. S., Amaro, F., & Pasqualotti, A. (2018). Social Capital and Internet Use in an Age-comparative Perspective with a Focus on Later Life. PLoS ONE, 13(2), 1-27.

Baudrillard, J. (1995). The Virtual Illusion: Or the Automatic Writing of the World. Theory, Culture & Society, 12(4), 97-107.

BIGOSINT Project, “THB Handbook for Online Investigators and Analysts”, (2022).

Bogard, W. (1996). The Simulation of Surveillance: Hypercontrol in Telematic Societies. Cambridge: Cambridge University Press.

Capurro, R. (2017). Digitisation as an Ethical Challenge. AI & Society, 32(2), 277-283.

Casey, E. (2000). Digital evidence and computer crime, in Academic Press, 2000

Castells, M. (1996). The Rise of the Network Society. Oxford: Blackwell.

Chan, J., & Bennett Moses, L. (2016). Is Big Data Challenging Criminology? Theoretical Criminology, 20(1), 21-39.

Christians, C. G. (2016). Social Justice and Internet Technology. New Media & Society, 18(11), 2760-2773.

Couldry, N., Gray, M. L., & Gillespie, T. (2013). Culture Digitally: Digital In/Justice. Journal of Broadcasting & Electronic Media, 57(4), 608-617.

Council of Europe. "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." International Legal Materials, November 23, 2001. https://doi.org/10.1017/S0020782900032873.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 105 OJ L § (2006). http://data.europa.eu/eli/dir/2006/24/oj/eng.

DuPont, B. (2017). Bots, Cops and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a way to Control Large-scale Cybercrime. Crime, Law and Social Change, 67(1), 97-116.

Dupont, Benoît. "Darkode: Recruitment Patterns and Transactional Features of 'the Most Dangerous Cybercrime Forum in the World.'" American Behavioral Scientist 61, no. 11 (2017): 1219–43.

European Council. "Top Cyber Threats in the EU," February 2, 2023. https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/.

European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, No. Joined Cases C-293/12 and C-594/12 (ECJ April 8, 2014).

European Court of Justice. Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, No. Joined Cases C-203/15 and C-698/15 (ECJ December 21, 2016).

European Union Agency for Criminal Justice Cooperation "Documenting International Crimes and Human Rights Violations for Criminal Accountability Purposes: Guidelines for CSOs" (September 21, 2022), DOI: 10.2812/682168.

Gurusami, Susila. "The Carceral Web We Weave: Carceral Citizens' Experiences of Digital Punishment and Solidarity." Punishment & Society 21, no. 4 (October 1, 2019): 435–53. https://doi.org/10.1177/1462474518790237.

Hannah-Moffat, K. (2019). Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates. Theoretical Criminology, 23(4), 453-470.

Huffman, S. (2018). The Digital Divide Revisited: What is Next? Education, 138(3), 239-246.

Hui, Y. (2012). What is a Digital Object? Metaphilosophy, 43(4), 380-395.

International Organization for Standardization. "ISO/IEC 27032:2012," 2012. https://www.iso.org/standard/44375.html.

Jewkes, Yvonne, and Majid Yar, eds. Handbook of Internet Crime. London: Willan, 2009. https://doi.org/10.4324/9781843929338.

Johnson, J. (2016). The Question of Information Justice. Communications of the ACM, 59(3), 27-29.

Jones, L. M., & Mitchell, K. J. (2016). Defining and Measuring Youth Digital Citizenship. New Media & Society, 18(9), 2063-2079.

Karaian, Lara. "Policing 'Sexting': Responsibilization, Respectability and Sexual Subjectivity in Child Protection/Crime Prevention Responses to Teenagers' Digital Sexual Expression." Theoretical Criminology 18, no. 3 (2013): 282–99. https://doi.org/10.1177/1362480613504331.

Kernaghan, Kenneth. "Digital Dilemmas: Values, Ethics and Information Technology." Canadian Public Administration 57, no. 2 (2014): 295–317. https://doi.org/10.1111/capa.12069.

Kernaghan, K. (2014). Digital Dilemmas: Values, Ethics, and Information Technology. Canadian Public Administration, 57(2), 295-317.

Karaian, Lara, and Katherine Van Meyl. “Reframing Risqué/Risky: Queer Temporalities, Teenage Sexting, and Freedom of Expression.” Laws 4, no. 1 (March 2015): 18–36. https://doi.org/10.3390/laws4010018.

Kohm, Steven A. “Naming, Shaming and Criminal Justice: Mass-Mediated Humiliation as Entertainment and Punishment.” Crime, Media, Culture 5, no. 2 (August 1, 2009): 188–205. https://doi.org/10.1177/1741659009335724.

Kim, D., Russworm, T. M., Vaughan, C., Adair, C., Paredes, V., & Cowan, T. L. (2018). Race, Gender, and the Technological Turn: A Roundtable on Digitising Revolution. Frontiers: A Journal of Women Studies, 39(1), 149-177.

Long, Nicholas J. “Utopian Sociality. Online.” The Cambridge Journal of Anthropology 30, no. 1 (2012): 80–94.

Marx, G.T. (1985). The Surveillance Society: The Thread of 1984-style Techniques. The Futurist, 6, 21-26.

McDonald, L. W., Tait, D., Gelb, K., Rossner, M., & McKimmie, B. M. (2015). Digital Evidence in the Jury Room: The Impact of Mobile Technology on the Jury. Current Issues in Criminal Justice, 27(2), 179-194.

Monahan, T. (2016). Built to Lie: Investigation Technologies of Deception, Surveillance, and Control. The Information Society, 32(4), 229-240.

Monahan, T., & mokos, J. (2013). Crowdsourcing Urban Surveillance: The Development of Homeland Security Markets for Environmental Sensor Networks. GeoForum 49, 279-288.

Mosco, V. (2015). To the Cloud: Big Data in a Turbulent World. London: Routledge.

Mosco, V. (2019). Becoming Digital: Toward to Post-Internet Society. Bingley: Emerald Publishing Limited.

Roche, Sean Patrick, Justin T. Pickett, and Marc Gertz. “The Scary World of Online News? Internet News Exposure and Public Attitudes Toward Crime and Justice.” Journal of Quantitative Criminology 32, no. 2 (2016): 215–36.

Silva, K. K. (2018). Vigilantism and Cooperative Criminal Justice: Is There a Place for Cybersecurity Vigilantes in Cybercrime Fighting? International Review of Law, Computers & Technology, 32(1), 21-36.

Smith, G., Bennett Moses, L and Chan, J. (2017). The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data Driven Approach. British Journal of Criminology, 57(2), 259-274.

Spiezia, F. (2023). Cyber Threat and New Paradigms of International Judicial Cooperation: The Role of Eurojust, Criminal System.

Werth, Robert. "Individualizing Risk: Moral Judgement, Professional Knowledge and Affect in Parole Evaluations." British Journal of Criminology 57, no. 4 (February 28, 2016): azw025. https://doi.org/10.1093/bjc/azw025.

Wood, Mark, Evelyn Rose, and Chrissy Thompson. "Viral Justice? Online Justice-Seeking, Intimate Partner Violence and Affective Contagion." Theoretical Criminology 23, no. 3 (2019): 375–93. https://doi.org/10.1177/1362480617750507.

Yar, Majid. "The Policing of Internet Sex Offences: Pluralised Governance versus Hierarchies of Standing." Policing and Society 23, no. 4 (December 1, 2013): 482–97. https://doi.org/10.1080/10439463.2013.780226.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs.

8. **Annex IV** – DIGITAL INVESTIGATIONS, PROPORTIONALITY AND RESPECT ON PRIVACY AND DATA PRO-TECTION

Foreword

At the different CoPs, some questions have arisen concerning the compatibility of legal investigation tools under European Union law and the fundamental principles of privacy and data protection. In two judgments handed down on 25 May 2021, the Grand Chamber of the European Court of Human Rights (ECHR) clarified the conditions for mass surveillance of electronic communications.

This problem is accentuated by the gradual shift from traditional phone interceptions to increasingly sensitive intelligence tools.

Introduction

Technological advances have given law enforcement agencies access to an unprecedented amount of digital data in the course of criminal investigations, opening the way to crucial discoveries, but also raising legitimate concerns about respect for citizens' fundamental rights.

In Europe, the protection of privacy is a major concern, enshrined in several key legal texts.

The Charter of Fundamental Rights of the European Union, which has been legally binding since the Treaty of Lisbon, explicitly enshrines the right to respect for private and family life.

The cornerstone of this protection is the General Data Protection Regulation (GDPR), which came into force in May 2018. The GDPR aims to ensure that the processing of personal data is carried out with respect for the fundamental rights and freedoms of individuals, while providing a robust regulatory framework for criminal investigation authorities.

Nevertheless, the balance between the imperatives of criminal justice and respect for privacy remains delicate. Digital criminal investigations raise crucial questions about the legitimacy of access to sensitive data, the duration of its retention, the procedural safeguards surrounding its collection and use, and measures to prevent abuse and infringement of fundamental rights.

This document examines the principles of proportionality and respect for privacy in the context of digital investigations at European level.

The main legal instruments for digital investigations in criminal matters

The European Arrest Warrant (2002/584/JHA)

Based on a vision of enhanced cross-border cooperation, this mechanism enables the judicial authorities of Member States to request the extradition of suspects between Member States. By facilitating the fluidity of procedures, this warrant strengthens the fight against crime while preserving fundamental rights, thus contributing to a more effective and balanced approach to European justice.

European Investigation Order, Mutual Legal Assistance and Joint Investigation Teams (Directive 2014/41/EU)

It provides a harmonised framework for the collection and exchange of evidence. By encouraging greater cooperation between judicial authorities, this directive improves Member States' ability to investigate complex crimes effectively, while preserving essential procedural safeguards.

Freezing of assets and confiscation (Regulation 2018/1805)

In the fight against money laundering and terrorist financing, this regulation enables national authorities to quickly freeze assets linked to criminal activities. By offering a simplified procedure and a coordinated approach, this mechanism strengthens Member States' ability to disrupt illicit activities and recover the proceeds of crime, thus contributing to a more secure and resilient Europe.

Financial penalties (Framework Decision 2005/214/JHA)

Focused on the effective enforcement of cross-border financial penalties, this framework decision establishes a framework for cooperation between Member States on the recovery of

financial penalties. By simplifying procedures and strengthening the recovery of sums due, this decision promotes the uniform and rapid application of penalties, thereby strengthening deterrence against criminal offences in the European Union.

Principles governing the collection and use of legal instruments

Data collection

European Arrest Warrant (2002/584/JHA)

- Searched person data: names, addresses, telephone numbers, e-mail addresses, etc.
- Evidence of offences
- Information relevant to investigations

European Investigation Order, Mutual Legal Assistance and Joint Investigation Teams (Directive 2014/41/EU)

- Evidence (witness statements, documents, etc.)
- Information relating to an ongoing criminal investigation

Freezing of assets and confiscation (Regulation 2018/1805)

- Asset information: financial assets such as bank accounts, property, investments, etc.
- Evidence of their involvement in criminal activities

Financial penalties (Framework Decision 2005/214/JHA)

- Information on fines
- Data on convicted persons

Purpose

European Arrest Warrant (2002/584/JHA)

- Rapid extradition of suspects between Member States
- Strengthening cross-border judicial cooperation
- Prompt and fair justice despite borders

European Investigation Order, Mutual Legal Assistance and Joint Investigation Teams (Directive 2014/41/EU)

- Facilitating the collection and exchange of evidence
- Strengthening cooperation between judicial authorities
- Tackling cross-border crime more effectively

Freezing of assets and confiscation (Regulation 2018/1805)

- Prevention of money laundering and terrorist financing

- Disruption of illicit financial transactions
- Recovery of the proceeds of crime

Financial penalties (Framework Decision 2005/214/JHA)

- Cross-border recovery of fines
- Uniform and effective enforcement of financial penalties
- Greater deterrence against criminal offences

Processing information collected from legal instruments

When collecting data for each instrument, the transmitting agencies gather detailed information, such as data on wanted persons, evidence (e.g. assets presumed to be linked to criminal activities), testimonies, verifying their relevance and legitimacy for the investigation or procedure in progress. The transmitting agency can then share them with the judicial agencies of other Member States (requested agencies) involved in the investigation.

Data processing means that the requested bodies use the information collected exclusively to carry out specific measures, such as arrest and surrender, stepping up investigations, applying the asset freeze or cross-border recovery of fines, while respecting the principles of law and cooperation between Member States.

To interconnect the IT systems of these judicial bodies in compliance with data protection law, a specific, decentralised technical infrastructure has been created, the result of a consortium of Member States and the Commission's desire to ensure the long-term future of a secure system. In practical terms, e-CODEX (Regulation 2022/850) links the IT systems of judicial authorities and legal professionals to enable the rapid and secure exchange of legal documents, evidence and information essential to proceedings. All these exchanges take place without any personal data being stored by the e-CODEX system. In addition to secure transmission, e-CODEX guarantees that personal data will not be altered. Lastly, only the original and required entities have access to personal data.

Balancing proportionality and respect for privacy

The search for an appropriate balance between digital investigations and individual rights is at the heart of the combination of applicable legislation that reconciles several principles.

Firstly, the collection of data should be limited to what is strictly necessary for the investigation, and the length of time the data is kept should also be restricted.

Prior judicial authorisation is required before intrusive digital investigations are carried out, and the judicial authority must be precisely informed of the nature and scope of the digital investigations, as far as possible.

Access to the data collected is restricted to those authorised and competent to process it, thereby reducing potential risks.

Conclusion

The rapid development of digital technology has undoubtedly transformed the criminal investigation landscape, offering powerful tools for fighting crime, but also raising key concerns about privacy and the protection of fundamental rights.

Legal texts such as the General Data Protection Regulation (GDPR) and the Charter of Fundamental Rights of the European Union have set important milestones in privacy protection, defining fundamental principles to guide digital criminal investigations, providing essential safeguards to ensure that individual rights are not sacrificed in the name of criminal prosecution.

However, it is crucial to recognise that emerging challenges cannot be fully anticipated by static legislation. Technological advances will continue to present new dilemmas, requiring laws and regulations to be constantly adapted. It is therefore imperative that judicial authorities, law enforcement agencies and legislators remain vigilant, ready to develop balanced approaches that take into account both the effectiveness of criminal investigations and the safeguarding of individual rights.

Protecting privacy in the context of digital criminal investigations is not an isolated challenge, but a reflection of the fundamental values and principles that underpin our democratic societies. Striking the right balance between the pursuit of justice and respect for individual rights remains an ongoing and collaborative task, requiring the participation of all stakeholders to ensure that our societies remain fair, equitable and respectful of human dignity.

By adopting a considered approach, based on respect for legal and ethical principles, it is possible to continue to evolve in the complex landscape of digital criminal investigations, ensuring that the protection of privacy remains a key priority in the collective quest for security and justice.

The balance between rigorous law enforcement and respect for privacy will remain at the heart of societal and legislative discussions as technology continues to redefine our approach to criminal justice.

9. Annex V –

Data Protection

Provisions of Regulation (EU) 2016/679 and Directive (EU) 2016/680: Similar and complementary, but also hierarchically – superiority and inferiority are not always clearly defined, thus situational and subject to discretionary powers.

European Arrest Warrant

The CJEU's restrictive interpretation of the concept of judicial authority based on fundamental rights raises questions on the concept of public authority found in EU instruments on cross-border cooperation in criminal matters in the Area of Freedom, Security and Justice. This is clearly the case in relation to the Council Regulation 2018/1805 (mutual recognition of freezing orders and confiscation order); Council Framework Decision 2002/584/JHA (European Arrest Warrant); Directive 2014/41/EU (European Investigation Order); Council Regulation 2017/1939 (European Public Prosecutor's Office); Regulation 2016/679 (GDPR); Directive (EU) 2016/680 (criminal justice data protection); and the Framework Decisions 829, 909, and 947.

However, there are additional doubts when other – indirectly related – public authorities are acting in potentially relevant fields, e.g. tax authorities.

Restorative Justice

Opportunities deriving from alternative measure to detention (FDs 829, 947 and 909) and their potential for cross-sectoral multi-agency cooperation mechanisms involving restorative justice instruments are not yet commonly conceptualised and applied. The added value of technology to gather and transfer data and to modernise the interplay of authorities, CSOs, perpetrators and victims is not yet capitalised on.

Requirements for the Collection of Evidence

Domestic criminal procedure law does not recognise any generally applicable principle according to which every violation of evidence collection regulations entails a prohibition of use in criminal proceedings. Whether such a prohibition applies is rather to be decided according to the circumstances of the individual case, considering the type of prohibition and the weight of the violation, weighing the conflicting interests.

It must be noted that the assumption of a prohibition of use of evidence restricts one of the essential principles of criminal procedural law, namely the principle that the court must investigate the truth and, to this end, must extend the taking of evidence ex officio to all facts and evidence that are of importance.

Therefore, a prohibition of the use of evidence is an exception that is only to be recognised according to an explicit statutory provision or for overriding important reasons in an individual case.

A More Exhaustive EU Regulatory Framework

The work of the EU in the Area of Freedom, Security and Justice is by no means exhausted in the legislative activity, which is primarily placed in the foreground here in terms of legal doctrine. Its focus is on activities to promote practical cooperation between the authorities of the member states; from a political perspective and from the point of view of the administration of justice, the creation of new regulations in Union law often appears to be a mere accompanying measure.

For this reason, efforts to ensure effective criminal prosecution have so far repeatedly been given too much priority, to the detriment of the individual rights of the accused (but not only).

European Public Prosecutor's Office EPPO

Art. 6 I EPPO Regulation provides that external instructions are not to be sought or received; advice may, however, be sought. It also requires member states and EU bodies not to influence the EPPO in the performance of its tasks. In addition, helping to ensure independence are the EPPO's own budget, regulatory autonomy and authority to adopt internal guidelines, the process for appointing and dismissing the European Prosecutor General, the European Prosecutors (as well as their non-renewable terms), and the European Delegated Prosecutors, decision-making in panels rather than by individuals, the different levels of supervision, and member state notification of or requesting approval of a disciplinary measure or dismissal to the European Delegated Prosecutors, who must be active members of the national prosecution or judiciary during their term of office.

It is subject to criticism that the responsibility in the investigation and prosecution activities is distributed in such a way that an accountability of the European Chief Public Prosecutor, who as the head of the EPPO bears the overall institutional responsibility and is indirectly democratically legitimized by the participation of organs of the Union in the appointment, can hardly be considered.

Due to the lack of a hierarchically conceived EPPO as well as decision-making in bodies, the European Attorney General cannot significantly influence the activities; thus, he rather degenerates into a representative body to the outside. The EPPO Regulation also only provides for the dismissal of the European Public Prosecutor for serious misconduct; however, this is an ultima ratio and not an appropriate sanction for other misconduct.

Interplay of EPPO and domestic Public Prosecutors

The internal order of EPPO has a direct impact on the judicial system of the member states: Although primarily police, customs and tax authorities are instructed by the EPPO to carry out (investigative) measures, there is in principle an obligation similar to administrative assistance, which is standardized for domestic public prosecutors.

Still unresolved against the background of the CJEU rulings on the EAW are the limits of the authority of the European (Delegated) Prosecutors to issue instructions to domestic prosecutors or other authorities who are subject to a right to issue instructions externally – such instructions are in tension with the independence of the EPPO.

This may happen because there is at least the possibility of a potential abuse (contrary to EU law) of the power to issue instructions by the political bodies with the power to issue instructions vis-à-vis the national authorities commissioned by the EPPO. In which constellations the EPPO can commission national authorities that are externally dependent on instructions will probably have to be decided on a case-by-case basis.

Criteria to be considered are the intensity of the commissioned measure in terms of fundamental rights, the scope of design and discretion exercised in the process, and the extent of supervision of the measure carried out. Consequently, measures that are particularly invasive of fundamental rights and involve a great deal of discretion cannot be delegated to the domestic public prosecutor's offices or other authorities that are bound by external instructions.

This project is funded by the European Union

VRDIGIJUST

Project

Digitalising Justice via Combined Virtual Reality Training

e-Capsules Report

Deliverable No. 2.5

PARTNERS


AGENFOR
INTERNATIONAL


Procura della Repubblica
PRESSO IL TRIBUNALE DI FIRENZE


HfÖ
Hochschule für
Öffentliche Verwaltung Bremen


COMMISSAIRES
DE JUSTICE
CHAMBRE NATIONALE


RES
PVBLICA
1995
ΑΘΗΝΑ


EPLO
European Public Law
Organization


Procura della Repubblica di Rimini


eeei
EUROPEAN
EXPERTISE
& EXPERT
INSTITUTE
Shaping Expertise across European Justice Systems


CORTE DI APPELLO DI VENEZIA


De Nationale Kamer van
Gerechtsdeurwaarders
La Chambre Nationale
des Huissiers de Justice