E-CAPSULE N.3
E-EVIDENCE

This project is funded by the European Union

THE CONTEXT

The technological evolution, the opportunities offered by virtual universes, the quantity and quality of available data, and the extension of social networks that make use of the digital world and the internet, 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".

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. However, 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.

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.

In addition, 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”.

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.

This e-capsules has been produced as part of the project VR-DIGIJUST - Digitalising Justice via combined Virtual Reality Training.This document is part of the Deliverable 2.5 - e-Capsules Report. VR-DIGIJUST project has received funding from the European Union under Grant Agreement no. 101046477.
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 granting authority can be held responsible for them.

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:

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. Similar-ly, 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 com-pared 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 protec-tion of privacy.

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' , 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) . Considering the complexity of "computer systems", as defined by the Budapest Convention , digital evi-dence may consist of stored data, i.e., information stored on their devices by the individuals under investigation, or computer systems managed by service providers or, finally, "traffic data" , 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 conversa-tion), 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, de-pending on their configuration (non-content data, stored content data, real time communica-tions) and the methods of storage, based on the need to maintain the forensic chain in its in-tegrity.

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 sys-tems, 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 capac-ity, beyond the individual target.

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” (Digi-tal 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 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”.

In addition, new actors are entering pre-investigative mechanisms, since online sources of in-formation are changing the ways, people understand and interact with the state and the crimi-nal justice system . Online practices enable new kinds of digital agency . There are newfan-gled types of justice emerging, including cybersecurity vigilantes 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 . Public police struggle to keep up with these shifting digital and online practices . As a result, the governance of crime in online and digital realms can foster complicated relationships between public police, telecom-munications, tech companies, private citizens, and NGOs. It is also important to note that although technologies are changing, these processes remain normative and moralized.

BASIC PRINCIPLES GUIDING PUBLIC-PRIVATE COOPERATION IN INVESTIGATIONS

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 commu-nities involved in the process.

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.

3. **Accountability and Legality**: 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.

4. **Professionalism and Respect**: CSOs are encouraged to act with professionalism, integrity, respect, and empathy throug-hout 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 establis-hed and recorded.

BASIC STANDARDS FOR DIGITAL EVIDENCE

In the context of digital evidence collection, CSOs should consider legal compliance, potenti-al 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 appropria-te training.
- Verifying data accuracy, as online information can be volatile and ea-sily 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 cap-tures with date and time stamps.
- Gathering additional data like media files, metadata, and collection in-formation.
- Storing the hash value for each digital item collected securely on a fresh media device.
- Keeping records of pertinent information, including collector details, IP addresses, and timestamps.

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 Con-vention 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 Di-rective' (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 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 repre-sents 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 pro-ceedings).

Alongside procedural rights, European jurisprudence has also intervened several times to pro-tect the principles of privacy in the field of data retention. As Spiezia rightly pointed out, reference should be made to the judgment of the Court of Justice of 8 April 2014 which annulled the so-called Frattini Directive No. 24 of 2006 on "data retention" because it is con-sidered contrary, in some of its legal provisions, to the fundamental rights of the individual. In its 2014 Digital Rights Ireland judgment , the Court of Justice of the European Union an-nulled Directive 2006/24/EC (so-called "Data Retention"), on which the internal rules sub-ject 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 rea-sons 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).

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 situation has arisen, in which 10 Member States declared unconstitutional (and therefore an-nulled) 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 acqui-sition of digital evidence and leaves in limbo the protection of the fundamental rights in-volved in the matter.

This e-capsules has been produced as part of the project VR-DIGIJUST - Digitalising Justice via combined Virtual Reality Training.
This document is part of the Deliverable 2.5 - e-Capsules Report.
VR-DIGIJUST project has received funding from the European Union under Grant Agreement no. 101046477.
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 granting authority can be held responsible for them.