E-CAPSULE N.4
DIGITAL INVESTIGATIONS, PROPORTIONALITY, AND RESPECT ON PRIVACY AND DATA PROTECTION

This project is funded by the European Union

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.

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

1. **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.

2. **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.

3. **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.

4. **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 (Dir. 2014/41/EU)

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

Freezing of assets and confiscation (Reg. 2018/1805)

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

Financial penalties (FD 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 (Dir. 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 (Reg. 2018/1805)

- Prevention of money laundering and terrorist financing
- Disruption of illicit financial transactions
- Recovery of the proceeds of crime

Financial penalties (FD 2005/214/JHA)

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

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.

PROCESSING INFORMATION COLLECTED FROM LEGAL INSTRUMENTS

When collecting data for each instrument, the transmitting agencies gather detailed infor-mation, such as data on wanted persons, evidence (e.g. assets presumed to be linked to crimi-nal 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 consorti-um 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 docu-ments, 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 trans-mission, 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 investiga-tion, 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.

CONCLUSIONS

The rapid development of digital technology has undoubtedly transformed the criminal inves-tigation 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 Fun-damental 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 prosecu-tion.

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 authori-ties, law enforcement agencies and legislators remain vigilant, ready to develop balanced ap-proaches that take into account both the effectiveness of criminal investigations and the safe-guarding 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 socie-ties. 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 pos-sible to continue to evolve in the complex landscape of digital criminal investigations, ensur-ing 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.