ARTIFICIAL INTELLIGENCE, LARGE DATASETS AND FUNDAMENTAL RIGHTS IN EUROPEAN CRIMINAL JUSTICE: THE EUROPOL CASE AND THE EMERGING EU REGULATORY FRAMEWORK

Sergio Bianchi
Director of the Department of Technology for Justice, Security and Peace-UPEACE University, United Nations

Abstract

The growing use of artificial intelligence and large-scale data analytics in law enforcement has fundamentally transformed criminal investigations in the European Union. Massive datasets generated through digital communications, encrypted platforms, and cross-border investigative cooperation increasingly serve as the basis for algorithmic analysis supporting investigative and prosecutorial decisions. While these technologies may significantly enhance investigative capacity, they also raise serious concerns regarding the protection of fundamental rights, including privacy, data protection, non-discrimination, and the right to a fair trial. This article examines how data-driven technologies may endanger fundamental rights within the European legal order and analyses the safeguards introduced by the European Union's regulatory framework. Particular attention is devoted to the interaction between the Artificial Intelligence Act, the General Data Protection Regulation, and Directive (EU) 2016/680 on data protection in law enforcement. The article also discusses the implications of the Europol data-governance case and recent developments in the regulation of cross-border electronic evidence.

1. Introduction

The digital transformation of contemporary societies has profoundly altered the role of data within systems of governance and criminal justice. Law enforcement authorities increasingly rely on large datasets in order to detect patterns of criminal activity, identify connections between individuals, and facilitate cross-border investigations. Artificial intelligence systems operate by analysing such datasets and generating predictive or analytical outputs that may influence investigative decisions and prosecutorial strategies.

Within the European Union, the growing reliance on data-driven technologies raises complex legal questions concerning the protection of fundamental rights. The large-scale processing of personal

Co-funded by the European Union
University for Peace
Department of Technologies for Justice, Peace and Security
TJPS Institute
DATA EQUALITY

data has the potential to affect rights such as privacy, data protection, equality, and the right to a fair trial. These rights occupy a central position within the EU constitutional framework and are explicitly protected by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Over the past decade, the European Union has progressively developed a multilayered regulatory framework aimed at addressing these challenges. Key elements of this framework include the General Data Protection Regulation (GDPR), Directive (EU) 2016/680 governing data protection in the field of law enforcement, and more recently the Artificial Intelligence Act. These instruments seek to ensure that technological innovation remains compatible with the protection of fundamental rights.

Against this background, the present article explores the risks associated with data-driven technologies in criminal investigations and analyses the safeguards introduced by the European legal framework. Particular attention is devoted to the role of large datasets and algorithmic analysis in law enforcement and to the implications of the Europol data-governance case for the legality of AI-supported investigations.

2. Data Processing and Fundamental Rights in EU Law

The protection of personal data constitutes a cornerstone of European constitutional law. Articles 7 and 8 of the Charter of Fundamental Rights recognise the right to respect for private life and the right to the protection of personal data as distinct but closely interconnected fundamental rights.

At legislative level, the European Union has adopted two main regulatory instruments governing personal data processing. Regulation (EU) 2016/679, commonly known as the General Data Protection Regulation, applies to the processing of personal data in the private sector and in most areas of public administration. Directive (EU) 2016/680, commonly referred to as the Law Enforcement Directive, regulates the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, and prosecution of criminal offences.

Both instruments establish a series of fundamental principles governing data processing. These include the principles of lawfulness, purpose limitation, data minimisation, proportionality, and accountability. These principles serve as essential safeguards aimed at ensuring that personal data processing remains compatible with fundamental rights.

The Court of Justice of the European Union has repeatedly emphasised the importance of these principles when assessing the legality of legislative measures involving large-scale data processing.

In the landmark judgment *Digital Rights Ireland*, the Court invalidated the Data Retention Directive on the ground that the general and indiscriminate retention of telecommunications data constituted a disproportionate interference with the fundamental rights to privacy and data protection. Similarly, in *Tele2 Sverige AB v Watson*, the Court held that generalised retention of telecommunications data is incompatible with the requirements of EU fundamental rights law.

These judgments illustrate a central constitutional principle of European law: measures involving large-scale collection or retention of personal data must satisfy strict requirements of necessity and proportionality.

3. Data-Driven Investigations and the Transformation of Criminal Evidence

The increasing reliance on digital technologies has fundamentally altered the traditional model of criminal investigations. In the past, investigative activities were typically directed toward specific suspects or defined criminal acts, and evidence was collected in relation to clearly identified investigative hypotheses.

In contrast, modern digital investigations often involve the collection and analysis of massive datasets generated through communication platforms and digital infrastructures. Investigations involving encrypted communication systems such as EncroChat or Sky ECC have produced datasets consisting of millions of messages exchanged between thousands of individuals across multiple jurisdictions.

In many of these cases, data was initially collected in bulk and only subsequently analysed in order to identify potential suspects or criminal networks. This investigative approach represents a significant departure from traditional investigative models. Instead of gathering evidence concerning identified suspects, authorities may first acquire large quantities of digital information and subsequently search for patterns or connections that may reveal criminal activity.

This shift raises important legal questions. The large-scale acquisition and analysis of digital data may challenge established principles governing criminal investigations, including proportionality, legality of evidence gathering, and the ability of defence lawyers to effectively challenge digital evidence.

These issues have increasingly generated litigation before national courts as well as before the Court of Justice of the European Union and the European Court of Human Rights.

4. The Europol Case and the Governance of Large Datasets

The legal risks associated with large-scale data processing in law enforcement are clearly illustrated by the case concerning Europol's data-processing practices.

In 2019, the European Data Protection Supervisor launched an investigation into Europol's handling of large datasets provided by Member States and international partners. The investigation revealed that Europol had processed extensive volumes of personal data relating to individuals who had not yet been categorised as suspects or otherwise connected to criminal activity.

In January 2022, the European Data Protection Supervisor issued a decision requiring Europol to delete certain datasets that did not comply with EU data-protection requirements. The decision emphasised that personal data processing in law enforcement must respect strict legal conditions, including the proper categorisation of data subjects and clear limitations on data retention.

The Europol case highlights an important legal principle: the legality of algorithmic analysis depends on the legality of the underlying dataset. If personal data has been collected or retained in violation of applicable legal requirements, analytical outputs generated through algorithmic systems may themselves become legally problematic.

The case also illustrates the broader governance challenges associated with the analysis of massive datasets in law enforcement. When datasets contain information about large numbers of individuals who are not suspected of criminal activity, the risk of disproportionate interference with fundamental rights becomes particularly acute.

5. Risks Associated with AI-Driven Data Analysis

The use of artificial intelligence systems in law enforcement does not merely replicate existing risks associated with data processing; it often amplifies them.

One of the most significant concerns relates to data quality. AI systems rely heavily on the quality and representativeness of the datasets used for training and analysis. Inaccurate or biased datasets may produce unreliable results and may lead to discriminatory outcomes, particularly when algorithmic outputs are used to support investigative decisions.

Another important issue concerns algorithmic transparency. Many AI systems operate through complex statistical models that may be difficult to interpret. When such systems generate analytical outputs that influence criminal investigations, questions arise regarding the ability of courts and defence lawyers to evaluate their reliability. A lack of transparency may undermine the right to a fair trial if algorithmic evidence cannot be meaningfully challenged.

A further concern relates to the phenomenon often described as “function creep.” Data collected for one investigative purpose may subsequently be reused for other purposes unrelated to the original investigation. The principle of purpose limitation, enshrined in both the GDPR and the Law Enforcement Directive, seeks to restrict such practices. However, the availability of large datasets combined with advanced analytical tools may create incentives to expand the use of data beyond its original purpose.

6. The Artificial Intelligence Act and the EU Risk-Based Regulatory Model

The adoption of the Artificial Intelligence Act represents a major development in the European regulatory framework governing digital technologies. The Regulation establishes the first comprehensive legal framework for artificial intelligence within the European Union.

The AI Act adopts a risk-based approach to regulation. AI systems are classified according to the level of risk they pose to fundamental rights and societal interests. Systems that present unacceptable risks are prohibited, while high-risk systems are subject to extensive regulatory obligations.

AI systems used in law enforcement are generally classified as high-risk systems. As a consequence, their deployment is subject to strict requirements concerning data governance, documentation, transparency, human oversight, and post-market monitoring.

These obligations aim to ensure that AI systems used in sensitive contexts operate in compliance with fundamental rights and democratic values. The Regulation therefore represents an important attempt to reconcile technological innovation with the protection of fundamental rights.

7. Cross-Border Data Access and the Regulation of Electronic Evidence

Another major development within the European legal framework concerns the regulation of cross-border access to electronic evidence.

The EU e-evidence package adopted in 2023 introduced new mechanisms allowing judicial authorities to request electronic evidence directly from service providers located in other Member States. The Regulation on European Production Orders and Preservation Orders for electronic evidence seeks to facilitate faster access to digital evidence while maintaining appropriate safeguards.

These new mechanisms represent an important step toward improving the efficiency of cross-border criminal investigations. At the same time, they raise complex questions regarding jurisdiction,

mutual trust between Member States, and the role of private companies in criminal investigations. The growing involvement of service providers in the transmission of electronic evidence also highlights the evolving relationship between public authorities and private actors in the digital environment.

8. Artificial Intelligence and the Future of Criminal Justice

The increasing use of artificial intelligence in criminal investigations cannot be assessed solely in terms of technological efficiency. While AI-driven analytical tools may significantly enhance investigative capacity, they also require a corresponding strengthening of legal safeguards.

The European legal framework has begun to address these challenges through a combination of data-protection law, AI regulation, and rules governing cross-border access to electronic evidence. Nevertheless, important questions remain concerning transparency, accountability, and the protection of defence rights in proceedings involving algorithmic analysis.

Ensuring that AI-supported investigations remain compatible with the principles of the rule of law requires continuous attention to the quality of datasets, the transparency of algorithmic systems, and the possibility for courts and defence lawyers to effectively scrutinise algorithmic outputs.

Conclusion

The growing integration of artificial intelligence into criminal investigations represents one of the most significant transformations of contemporary criminal justice systems. The ability to analyse massive datasets through advanced computational techniques offers important opportunities for improving investigative effectiveness. At the same time, it introduces new risks for the protection of fundamental rights.

The European Union has responded to these challenges through the development of a comprehensive regulatory framework combining data-protection law, AI regulation, and rules governing cross-border electronic evidence. The Europol case illustrates the central importance of robust data governance in this framework and demonstrates that the legality of algorithmic analysis depends fundamentally on the legality of the underlying dataset.

Ultimately, the challenge facing European criminal justice systems is not merely technological but constitutional. The effective use of AI in law enforcement must remain compatible with the principles of proportionality, transparency, and respect for defence rights that underpin the European legal order.