FACILITATING JUDICIAL COOPERATION IN THE EU

A Computable Approach to Mutual Recognition in Criminal Matters

Edited by
Giulia Lasagni
Giuseppe Contissa
Michele Caianiello

BRILL | NIJHOFF

Facilitating Judicial Cooperation in the EU

Facilitating Judicial Cooperation in the EU

A Computable Approach to Mutual Recognition in Criminal Matters

Edited by

Giulia Lasagni
Giuseppe Contissa
Michele Caianiello

BRILL | NIJHOFF

LEIDEN | BOSTON

This volume is the result of a research funded by the European Union. The research was conducted within the framework of the Justice Programme (2022) and is subject to the conditions of Grant Agreement No. 101089634. The views expressed herein are solely those of the authors and do not necessarily reflect those of the European Union.

Funded by
the European Union

The Library of Congress Cataloging-in-Publication Data is available online at https://catalog.loc.gov
LC record available at https://lccn.loc.gov/2025022890

Typeface for the Latin, Greek, and Cyrillic scripts: "Brill". See and download: brill.com/brill-typeface.

ISBN 978-90-04-70578-4 (hardback)
ISBN 978-90-04-70579-1 (e-book)
DOI 10.1163/9789004705791

This book is printed on acid-free paper and produced in a sustainable manner.

Contents

List of Figures and Tables IX
Notes on Contributors XI

Introduction 1
Giulia Lasagni, Giuseppe Contissa and Michele Caianiello

PART 1

1 Effective Rights and Remedies in the Computable Era: Facing Informative Asymmetry When AI Adds to Transnational Cooperation 11
Giulia Lasagni and Giuseppe Contissa

2 International Judicial Cooperation and the EU Principle of Mutual Recognition – towards a Convergence of Systems? 29
Michele Caianiello

3 Large Language Models in the Justice Domain 55
Giuseppe Contissa and Galileo Sartor

PART 2

4 Bulgaria: the EAW, EIO and Regulation 1805/2018 in the Bulgarian Legislation and Case Law 69
Miroslava Manolova and Ekaterina Salkova

5 Croatia: Effective Enforcement of Mutual Recognition Instruments and Cases Exposing Political Influences on EU Judicial Cooperation 102
Zlata Đurđević, Elizabeta Ivičević Karas, Marin Bonačić and Zoran Burić

6 France: Cooperation in Criminal Matters between Mutual Recognition and Protection of Fundamental Rights – the Contribution of France 148
Eleonora Cervellera

7 Germany: a Clash of Systems between EU Mutual Legal Assistance Instruments and National Law 182
Anna H. Albrecht and Anne Schneider

8 Italy: the EU Criminal Cooperation Instruments at the Test in Italy – Procedures and Critical Profiles 218
Isadora Neroni Rezende, Antonio Pugliese, Nicolò Gibelli and Anna Piovan

9 Poland: EAW, EIO and Freezing and Confiscation Orders – Implementation and Transposition Process and Its Deficiencies 271
Wojciech Jasiński, Karolina Kremens and Agnieszka Frąckowiak-Adamska

10 Portugal: Recognition of European Warrants and Cooperation Orders in Law and Practice 303
Miguel João Costa, Raquel Cardoso, António Vaz de Castro and Pedro Caeiro

11 Spain: Critical Profiles in the Transposition of European Orders in Criminal Matters 339
Ana Maria Neira Pena

12 The Netherlands: Implementation and Application of the EAW, EIO, and Freezing and Confiscation Orders 372
Camila Ugaz Heudebert, Teddy Zwackhalen, Gijs van Dijck and Menno Dolman

PART 3

13 Comparative Remarks on Mutual Recognition Instruments of Judicial Cooperation in Criminal Matters 427
Giulia Lasagni, Michele Caianiello and Isadora Neroni Rezende

14 Piercing the Veil of Ignorance of Fundamental Rights Protection. What Is Transnational in EU Judicial Cooperation? 454
Mariavittoria Catanzariti

15 Mutual Recognition and Double Criminality in EAW: Comparative Challenges and Future Prospects 487
Alessandra Santangelo

PART 4

16 Access to Justice through AI 507
Marco Billi and Alessandro Parenti

17 Harmonizing Legal Terminology and Case Law Retrieval in European and National Legislation 528
Davide Audrito, Ivan Spada, Rachele Mignone, Emilio Sulis, Luigi Di Caro, Eduard-Raul Kontos and Rohan Nanda

Conclusion 548
Giulia Lasagni and Giuseppe Contissa

Index 551

CHAPTER 1

Effective Rights and Remedies in the Computable Era: Facing Informative Asymmetry When AI Adds to Transnational Cooperation

Giulia Lasagni and Giuseppe Contissa

1 Judicial Cooperation and AI Technology: a Complexity Challenge

Numerous contributions in the last years have dealt with identifying the advantages brought by the AI potential to the criminal justice systems, and perhaps even more authors have raised their voices about the risks posed by such technology for the integrity of fundamental rights in this domain.[1] These authors have also entered the debate by stressing the complexity of ensuring the effectiveness of remedies where algorithmic and AI decisions are in place. On that occasion, we had discussed how, to be able to challenge an individual decision effectively, the data subject must have access to all the information relevant to the decision, and in particular to the datasets, the data processing methods, and the source code expressing the algorithms underlying the functioning of the system.[2]

However, AI systems often present significant challenges for transparency: information on the dataset is usually not available to the parties or the judge using the system, and a similar consideration may be made with regard to the information on the data processing methods and algorithms. In fact, in many cases, they depend on the accessibility of the source code, the disclosure of

* The chapter is a joint reflection of the authors, but its drafting is broken down as follows: Contissa §§ 2, 4 (technological part), 5; Lasagni §§ 1, 3, 4 (legal part).

1 See, *ex m*ultis, Aleš Završnik 'Criminal justice, artificial intelligence systems, and human rights' (2020) 20 ERA Forum 567–583, https://doi.org/10.1007/s12027-020-00602-0; Serena Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal* (Springer, 2020); Brandon L. Garrett, Cynthia Rudin, 'The Right To A Glass Box: Rethinking The Use Of Artificial Intelligence In Criminal Justice' (2024) 103 (3) Cornell Law Review.

2 Giuseppe Contissa, Giulia Lasagni, 'When it is (also) algorithms and AI that decide on criminal matters: In search for an effective remedy' (2020) 28 3 European Journal of Crime, Criminal Law and Criminal Justice, 290.

which may be limited by intellectual property rights. Moreover, as displayed by the *black box* image, in several AI systems based on machine learning, there are structural limits to the ability to provide information for reconstructing the system's functioning and the reasons for its decision.

This Chapter builds on those studies by focusing on the notion of effectiveness in the multi-layer context of judicial cooperation.

Such dimension, as known, presents its own specific challenges, especially in the European Union, where the procedural divergences among Member States may come to represent an obstacle to smooth cooperation. Indeed, the minimum harmonization realized with the Stockholm Programme, though extremely significant in approximating domestic systems,[3] only concerned a few aspects of procedural rules. In particular, the lack of common regulation persists regarding the performance of investigative measures, for instance, in relation to the need for judicial authorization or to the standard of proof that needs to be met to activate the measure itself. This lacuna grants the principle of mutual recognition not only a theoretical role as the "cornerstone" of judicial cooperation[4] but also a practical pivotal position in determining the effective functioning (or malfunctioning) of the cooperation game. While the limits and potential of this principle have been widely studied in the last decades[5] and are the subject of an increasing number of judicial decisions of the Court of Justice,[6] the growing technological dimension of the investigation calls for a specific reflection on the impact of this element not only for the efficiency of the cooperation mechanisms but also for the fairness of the whole procedure.

This calls for an integrated approach toward the deployment of AI technology in the criminal justice field that puts together, since the design of the

3 Giuseppe Contissa, Giulia Lasagni, Michele Caianiello, Giovanni Sartor (eds.), *Effective Protection of the Rights of the Accused in the EU Directives. A Computable Approach to Criminal Procedure Law* (Brill, 2022).

4 Tampere European Council, 15 and 16 October 1999, Presidency Conclusions, § 33.

5 With regard to different application fields, within the criminal matter see, *ex multis*, Hannah Brodersen, Vincent Glerum, André Klip, 'Improving Mutual Recognition of European Arrest Warrants for the Purpose of Executing in absentia Judgments' Funded by the European Union's Justice Programme (2014-2020); John A. E. Vervaele, 'The ne bis in idem principle as a domestic general principle of law' (2005) 1 (2) Utrecht Law Review 100-118; Helmut Satzger, 'Is mutual recognition a viable general path for cooperation? (201) 10 (I) New Journal of European Criminal Law 44-56; and, with a broader perspective Gisèle Vernimmen-Van Tiggelen et al., *The future of mutual recognition in criminal matters in the European Union / L'avenir de la reconnaissance mutuelle en matière pénale dans l'Union européenne* (Bruxelles 2009).

6 See CJEU Stefano Melloni v Ministerio Fiscal, 26 February 2013, Case C-399/11; Pál Aranyosi and Robert Căldăraru v Generalstaatsanwaltschaft Bremen, April 2016, Joined Cases C-404/15 and C-659/15 PPU; E.D.L., 18 April 2023, Case C-699/21.

tools, lawyers, computer scientists, and legal informatics. These are also the objectives of the FACILEX project, where a platform has been built and some AI applications have been developed by considering the requirements for transparency and explainability.[7]

With this perspective, the Chapter proceeds as follows: in section 2, an overview will be provided on the uses of AI systems in criminal justice, including investigations and judicial decision-making. In Section 3, a specific application of AI technology will be put in the context of the European Investigation Order cooperation mechanism. Looking at the EncroChat/Sky ECC transnational investigation that involved most EU Member States in recent years, the practical and systemic difficulties in ensuring fair trial rights will be highlighted when cooperation issues add up to technological challenges. Against such analysis, Section 4 stresses some proposals on how to approach the informative asymmetry typical of transnational technological investigations.

Last, Section 5 concludes by focusing on the policymaker perspective, examining the recently adopted AI act in light of the highlighted problematics, and proposing some corrective recommendations on better addressing such a complex state of affairs.

2 Potential Uses of AI in Criminal Justice

In recent years, a paradigm shift has occurred in AI: transitioning from human-made representation of knowledge to machine learning. Machine learning refers to a system that "improves its performance on future tasks after making observations".[8]

In machine learning-based systems, knowledge about the domain and the activities to be carried out is no longer provided by humans. Still, it is instead built by the system itself, applying a learning algorithm to vast datasets. Using this model, the system generates classifications, evaluations, and predictions for new cases submitted. Updating and expanding the dataset automatically improves the model and the system's predictive capabilities.

This direction has led to a large number of successful applications in many fields, including the judicial, enforcement, and investigations, enhancing the capabilities of law enforcement agencies, judges, and legal professionals.

---

7 For a detailed explanation of the technologies deployed in the FACILEX project, see *infra*, Chapter 15 and 16.

8 Stuart J. Russell and Peter Norvig, *Artificial Intelligence. A Modern Approach* (Prentice Hall, Englewood Cliffs, N.J., 3 edition, 2010).

AI applications in the judiciary can be classified into two main areas:[9] document-oriented and case-oriented approaches.

Document-oriented approaches are focused on the analysis of individual documents. The main goal of such systems is to extract information, that is, to identify named entities such as places, persons, organisations, dates, and claims, as well as to extract more complex information, such as events and narratives. Automated summarisation aims at creating summaries of case facts, decisions, and other legal documents by selecting phrases appropriate to a summary, combining and possibly rephrasing them into a coherent text. The automated parsing of statutory texts aims at the automated conversion of the original, natural language legislative documents into machine-interpretable rules.

Predictive retrieval aims at the automated selection of legal texts relevant to a specific legal task, such as drafting a new law or deciding a case. The entire corpora of documents can be analysed to discover correlations, extract implicit information, and organise cross-references between documents and parts of them.

Such systems may support identifying and selecting the most significant bits of previous cases and thus facilitate the reuse of portions of previous documents in new ones.

Document-oriented systems may benefit legal practice, enabling judges and other legal experts to be more efficient and accurate in doing legal analyses and generating legal documents. They can, therefore, also improve the quality of legal sources, such as judicial decisions and statutory texts.

Case-oriented approaches to legal machine learning typically rely on models extracted from vast sets of cases. They provide aggregate statistical information about such cases. Still, they may also be used to predict specific aspects of new instances, such as their duration, costs, and potential awards or punishments, as well as to calculate the probability that claims, motions, or other pleadings succeed.

The models constructed by such systems embed correlations between (sets of) features of cases on one side and decisions and/or factual forecasts on the other. One of the areas of primary interest is litigation assistance (i.e., systems providing information to increase the likelihood of success at trial). Based on an analysis dealing with factors related to the merit of the case (such as lexical features, events, narratives, and procedural history), but often also on the basis of factors not related to merit (such as the nature of the suit, the attorneys, the venue, the judge, and the parties), such systems can make predictions about the behaviour of the parties to a proceeding (e.g., under what conditions a

9 L. Karl Branting, 'Data-centric and logic-based models for automated legal problem solving' (2017) 25(1):5–27 Artificial Intelligence and Law.

settlement may be accepted) or the behaviour of judges (the decisions they may take).

Besides directly supporting the decision-making activities, Case-oriented AI systems can have a range of additional uses. Firstly, in the preparation of litigation: being prepared for litigation or an investigation involves having access to high-quality information about the potential outcome of the case, including the conditions or arguments that could enhance the chances of a positive result, the anticipated penalties or damages that might be assigned, and the expected time and expenses involved in resolving the matter. This type of information is crucial for a party's strategic planning in approaching the case.

Secondly, in analysing past decisions, AI systems can be used to analyse past decisions to uncover patterns in how judicial decisions have been made over time. These patterns might involve the method of judgement (the approach judges take to make their rulings), the nature of the decisions made (how these rulings differ based on variables like time and location), and through the use of network analysis, the connections between decisions (identifying which court opinions have the most impact on others and the reasons for this influence).

Thirdly, in enhancing the quality of the judiciary: like any professional, judges are fallible, and the quality of their work would benefit from using AI tools that can assist in analysing how judges arrive at decisions or in identifying any inherent biases in those decisions. Moreover, judges can make use of the insights gained from these technologies to assess and possibly enhance their decision-making skills.[10]

Systems that correlate the features of new cases with their possible future decisions may enable lawyers to get a sense of their chances of success (possibly reducing litigation), select or search for aspects of the case that increase their chances of success, and better develop their arguments. Such systems may also be helpful for judges, enabling them to gain a better sense of case law trends and see how a possible decision would stand in the context of case law.

A recent innovation is the development of legal applications for cognitive computing.[11] These applications aim at bridging the analysis of legal texts through machine learning with the relevant legal sources and rationales: the portions of texts that contain applicable provisions, judicial holdings, and

10 Examples of predictive systems for legal advice are Lexmachina, which aims at predicting the behaviour of courts, judges, lawyers, and parties in IP Law; Premonition, which focuses on analysing judicial tendencies and attorneys' performance and outcomes before judges; and Luminance, a platform that applies supervised and unsupervised machine learning to the process of document review and enables the automated annotation of legal documents and the detection of possible anomalies.

11 Kevin D. Ashley, *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age* (Cambridge University Press, 2017).

findings of facts; the arguments that justify the proposed conclusions; and the legal and factual reasons in favour or against the proposed outcome. A cognitive computing approach may support judges and other legal experts in investigating and answering legal questions, providing explanations for their legal decisions or assessments, making arguments for and against legal conclusions, and improving predictions about case outcomes.

Cognitive computing in the legal domain can profit from argument mining, which includes a set of techniques and technologies focused on identifying and analysing argument-related information in text corpora, such as premises and conclusions, relationships between arguments and counterarguments, the substantive strengths or weaknesses of claims, and the rationale for legal decisions. An example of machine learning that includes elements of cognitive computing is Claudette (CLAUse DETecTEr),[12] a platform enabling machine learning analysis of consumer contracts and privacy policies. The system combines ML approaches and knowledge-based approaches to deliver explanation functionalities.

What is concerned with law enforcement activities, AI's most notable change is the ongoing shift from being reactionary to being proactive in their efforts to prevent crime.

In this context, an important and widespread application is that of predicting policing. The term refers to using data analytics, algorithms, and AI technologies to analyse historical crime data to anticipate future criminal activities. This approach enables law enforcement agencies to allocate their resources more effectively by predicting where and when crimes are more likely to occur. It involves analysing patterns in past crime data, including time, location, and other relevant factors, to identify potential risks and trends. The goal is to prevent crime proactively rather than responding reactively, allowing agencies to allocate their scarce resources to high-risk areas better before crimes happen, thus enhancing public safety and efficiency.[13] Similar AI systems aim to predict potential victims or categories of victims rather than crimes.[14]

12 Marco Lippi et al., 'CLAUDETTE: an automated detector of potentially unfair clauses in online terms of service' (2019) XXVII Artificial Intelligence and Law 117–139.

13 The perhaps most known being PredPol, now Geolitica (www.geolitica.com – accessed: 18/04/2025) but similar tools are today developed and deployed by most law enforcement agencies worldwide. For a comprehensive overview of predictive policing tools, see Albert Meijer, MartijnWessels 'Predictive Policing: Review of Benefits and Drawbacks' (2019) 42(12) International Journal of Public Administration, 1031–1039. https://doi.org/10.1080/01900692.2019.1575664.

14 For example, this research presents the use of AI to predict feminicide victims: Esperanza Garcia-Vergara, Nerea Almeda, Francisco Fernández-Navarro *et al.,* 'Artificial intelligence

A third category of AI applications that has raised many ethical and legal concerns is that of the systems making individual assessments, usually on the likelihood of risk of recidivism. Utilizing vast datasets – some of which may not be immediately accessible to law enforcement – these tools employ mathematical algorithms and machine learning capabilities to link statistical risk indicators with specific individuals. One of the most prominent examples of such predictive analytics tools is COMPAS, created by Northpoint Inc. (now known as Equivant), a private entity headquartered in California. This system is widely employed across various US states for estimating recidivism rates to inform alternative sentencing or probation decisions and has been widely analysed (and criticized) by legal scholars worldwide.[15]

Other systems that use AI predictive capabilities (that is, to predict and recognise anomalous patterns and to learn to recognise new patterns) are those aimed at detecting fraud risks in various fields and cybersecurity threats. Perhaps less known than those aiming at predicting recidivism, these systems find however a broad application in several countries.

Financial fraud detection applications are based on AI systems that can analyse and filter vast amounts of financial transactions to identify patterns indicative of fraudulent activities, such as money laundering or identity theft, much quicker and more accurately than human investigators.[16]

Healthcare fraud detection applications can analyse billing and clinical data across healthcare systems to detect unusual patterns and discrepancies that may indicate fraudulent claims or unnecessary medical procedures.[17]

---

extracts key insights from legal documents to predict intimate partner femicide' (2023) 13 18212 *Sci Rep*, , https://doi.org/10.1038/s41598-023-45157-5.

15 See, *ex multis*, 'Eric L. Loomis, Petitioner v. State of Wisconsin, on Petition for a Writ of Certiorari to the Supreme Court of Wisconsin: Brief for the United States as Amicus Curiae' <https://www.scotusblog.com/wp-content/uploads/2017/05/16-6387-CVSG-Loomis-AC-Pet.pdf> (accessed: 18/04/2025); Iñigo De Miguel Beriain, 'Does the Use of Risk Assessments in Sentences Respect the Right to Due Process? A Critical Analysis of the Wisconsin v. Loomis ruling' (2018) 17 Law, Probability and Risk 45–53; critics have been raised also from civil society, see for all Julia Angwin, Jeff Larson, Surya Mattu, Lauren Kirchner, 'Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks' (ProPublica, 23.05.2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (accessed: 18/04/2025).

16 Johan Perols 'Financial statement fraud detection: An analysis of statistical and machine learning algorithms.' (2011) 30.2 Auditing: A Journal of Practice & Theory 19–50; John O. Awoyemi, Adebayo O. Adetunmbi, Samuel A. Oluwadare, 'Credit card fraud detection using machine learning techniques: A comparative analysis' (International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, 2017) 1–9, doi: 10.1109/ICCNI.2017.8123782.

17 Jing Li, et al. 'A survey on statistical methods for health care fraud detection.' (2008) 11 Health care management science 275–287.

Regarding cybersecurity threats, AI systems are employed to monitor network traffic in real time, identifying anomalies that could indicate a cyber-attack, phishing attempts, or malware infiltration. Moreover, AI systems are also used for cybersecurity incident response to help determine the scope and scale of a breach and recommend containment strategies.[18]

Coming closer to the investigation, AI systems are deployed in a vast set of tasks, ranging from eDiscovery to digital analysis of evidence to recognition of crime scenes, gunshots, and bombs. In eDiscovery, AI tools help investigators to analyse thousands of documents to find relevant case material, significantly reducing the time and cost associated with manual reviews.

In forensics, the main field of application is the digital analysis of videos and images. The typical case is facial recognition, which identifies suspects or finds missing persons by comparing faces against a database of known individuals. Recent developments have enhanced the accuracy of identifying individuals from images of low quality, taken from suboptimal angles, or where the face is partially concealed.[19] Another case in this area is the interpretation of radiological images to assist medical examiners with establishing causes and manner of death.

However, current AI technology provides law enforcement with capabilities that extend far beyond mere recognition of individuals and objects. For instance, it enables the analysis of accident and crime scenes, both as they occur and post-event: combining the information captured in crime scene photos with the analysis of gunshot pattern signatures, AI algorithms are used to differentiate each explosive shockwave and assign shots to a specific firearm and within a particular moment. Increasingly, AI technology is also used to decipher encrypted content, as illustrated below.

---

18 Javier Martínez Torres, Comesaña Carla Iglesias, Paulino J. García-Nieto, 'Machine learning techniques applied to cybersecurity' (2019) 10 (10) International Journal of Machine Learning and Cybernetics 2823–2836; Anand Handa, Sharma Ashu, K. ShuklaSandeep, 'Machine learning in cybersecurity: A review' (2019): 9.4 e1306 Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery .

19 Justin Norman, Hany Farid, 'An Investigation into the Impact of AI-Powered Image Enhancement on Forensic Facial Recognition (Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops', 2024) 4306–4314.

3 An Automated Approach to Mutual Recognition? The Cooperation Case of EncroChat and Sky ECC

A recent case, or better, a series of recent cases, present well the complexity of matching the use of AI techniques during criminal investigations with the application of cooperation mechanisms based on mutual recognition.

The reference goes to the EncroChat and Sky ECC affair, which involved a significant number of EU Member States and whose facts are so well-known that it is enough here to recall some of the main traits.

It was 2020 when the French and Dutch authorities, together with Eurojust and Europol, announced the official dismantling of the EncroChat server. Based (also) in France, EncroChat was one of the world's most extensive encrypted communication services, a parallel operating system to traditional ones (such as Android), with thousands of users in Europe alone. The service provided a 'secure' communication network, thanks to the deactivation of microphones, cameras, and GPS in the devices, the possibility of remotely wiping the contents of the hardware, and finally, encrypted software specifically for forwarding messages anonymously.

Having discovered the exploitation of such a network by several organised crime groups active in drug trafficking, in 2018, France and the Netherlands, with the support of the European agencies, set up a Joint Investigation Team (JIT). With the authorisation of the French judiciary, the investigators, thanks to an unspecified 'technical device', captured messaging for about two months until the platform, realising the hacking, alerted its users, informing them that a public authority had obtained access to the system and suggesting they dispose of their phones.[20] From a legal perspective, the operation was carried out in France using a specific investigative technique, which requires, in a similar way to the regime of wiretapping in most systems, an authorisation by a judge for its performance.[21]

The data collected, amounting to hundreds of thousands of messages, were first shared within the investigation team, giving rise to numerous criminal proceedings in the two countries. Subsequently, with the support of Eurojust

20 Eurojust/Europol, 'Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe', joint press release, 2 july 2020, <https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe> (accessed: 18/04/2025).

21 Specifically, the *captation des données informatiques* (Article 706-102-1 of the French Criminal Code, on which more *infra*, Chapter 6 – France).

and Europol, they were made available to other states through requests for judicial cooperation, precisely via the European Investigation Orders (EIOs).

After dismantling the EncroChat network, the French and Dutch investigators, joined by the Belgian ones, noted a shift of communications relating to international drug trafficking to the Sky ECC platforms. This was an encrypted messaging network boasting hundreds of thousands of users worldwide, based on the sale of smartphones that had been modified (deactivation of the video camera, microphone and GPS; impossibility of making calls outside the Sky ECC circuit) and equipped with unique security settings, such as the automatic deletion of messages received after a period of time predetermined by the users (even a very short one, such as 30 seconds) and the possibility of remotely deleting the contents of the device with a special password (so-called distress password/kill switch) in case of need. Sky ECC's complex hacking operation, once more carried out via the establishment of a JIT between France, the Netherlands, and Belgium, again with the support of Europol and Eurojust, resulted in the capture of at least one billion encrypted messages and the seizure of 70,000 cryptophones.

As in the EncroChat case, from a legal point of view, the inoculation into the encrypted platform was carried out in France (where the Sky ECC servers were also located) through the same investigative measure, with authorisation by the competent court. Technically, according to what has been disclosed, the operation was developed in three phases (not necessarily all clearly distinct, from a temporal point of view): a) use of a software to break into the server of reference; b) application of an AI tool to decrypt the content acquired, and attribute the content of the selected messages to specific defendants; and finally c) storage and analysis of the data collected through digital forensics platforms. All these technologies were developed within the JIT, with the fundamental contribution of the Dutch National Forensic Institute and Europol. Again, once collected, the data were also made available to third countries through international cooperation requests, which, within the EU, took the form of EIOs.[22]

The sharing of information in the EncroChat and Sky ECC cases gave rise to hundreds of criminal proceedings in Europe alone, in which several

22 For a more comprehensive analysis of the cases, see *ex multis*, Jan-Jaap Oerlemans, Sofie Royer, 'The future of data-driven investigations in light of the Sky ECC operation' (2023) 14 (issue 4) *New Journal of European Criminal Law* 434–458; Georgios Sagittae, 'On the lawfulness of the EncroChat and Sky ECC-operations', (2023) 14 (issue 3) New Journal of European Criminal Law 273–293; specific national aspects are also highlighted in Part 2 of this volume.

critical aspects related to the use of the collected data at trial were immediately apparent.

Of all the problems related to these affairs,[23] one is crucial for the focus of this paper: the AI-based tools used to (probably) hack the server and analyse the collected communications were not disclosed to the parties. This occurred not due to typical 'black box' technical issues but because the investigative authorities involved in the JIT made clear their interest in reusing the software for future repressive actions.[24]

Similarly, the data collected by the investigators was made available to the parties only to a limited extent. Expressly, parties within a given criminal proceedings were granted access to the so-called 'tertiary dataset', that is, the bulk of information relevant to that specific case, per the national law regulating access to file. However, no access was generally allowed to the raw dataset of all seized information ('primary dataset'), nor the data considered relevant for criminal investigations ('secondary dataset').[25]

Requests to access the AI tool and the dataset were also raised – and denied – in other Member States, where the information seized had arrived via EIO, reaching up to the highest instances in the respective court systems. The problems were also brought before the Court of Justice, which famously ruled on the application of the Landesgericht Berlin with judgment *M.N.* of 30 April 2024.[26]

In all such contexts, the question thus arose of whether these impediments could be regarded as an infringement of the rights of the defence and, if so, of what remedy could be effectively invoked against it. In particular, the problem posed by the defence concerned the alleged impossibility of trusting the reliability of the data contained in the tertiary dataset without the possibility of checking the latter with the bulk of data that have been seized and without knowing how the AI tool was set to operate on such data.

In the countries not included in the JIT, the issue was further complicated by the layer given by the transnational dimension of the investigation in light of the limited rules posed by the EIO Directive in this regard.

---

23 Among which whether the acquisition of the data, carried out in France according to forms of collection that do not necessarily find a correspondence in the domestic system, can be an obstacle to the use (or admissibility, in European States where the two profiles are not autonomous) of the data in domestic proceedings; and whether it is necessary to add, in the system that receives the data, a further measure of the judicial authority, certifying the usability of the data for domestic purposes, or whether it is sufficient to check that the French court has already carried out the acquisition at the time of the data.

24 Jan-Jaap Oerlemans and Sofie Royer (n 22) for the reference to the relevant domestic case-law.

25 Idem, ft 105.

26 CJEU, C-670/22.

Article 1(1) of the Directive provides that an EIO may be issued "for obtaining evidence that is already in possession of the competent authorities of the executing State". While this hypothesis was likely conceived as relatively unproblematic in origin, its recent application in the context of interceptions shows all the limits of the legal basis, especially in light of the principle of mutual recognition. In particular, the regulation of this type of EIO does not seem to consider the fact that when the bulk of evidence is remotely gathered in real-time investigating measures, the phase of data selection becomes crucial. Accordingly, the possibility for the defence to participate in such a selection is also essential, for instance, by contributing to defining the parameters (e.g., keywords) adopted to do so. This operation, however, occurs in the Member State where the investigative measure has been carried out (or, where relevant, in the countries involved by the JIT).

Defendants of further Member States that received the data via EIO, on the other side, did not have a chance to participate in the selection procedure and had to deal with packages of relevant data ('tertiary dataset') passively received in their case file. In such circumstances, the EIO Directive does not provide any specific safeguard to reinstate the right to be heard in the issuing Member State. This gap is then often examined at the national level in light of the principle of mutual recognition. The problem then emerges of whether or to what extent the principle of mutual recognition can compensate for the lack of access to information on both the selection process and the deployment of AI systems during the investigation.

4 Effective Rights and Remedies in a Transnational Computable Era

The question raised in the EncroChat and Sky ECC cases is exemplificative of a more general issue concerning the informative asymmetry that belongs both to the deployment of AI technology and to the transnational dimension of criminal investigations. In other words, in transnational technological investigations, there is a proliferation of information asymmetries that heavily impact the effectiveness of fundamental rights.

This makes the identification of effective remedies a highly complex task. On the one hand, total and detailed transparency in how the technology deployed or the foreign legal system works seems difficult to achieve for several reasons. Conferring to the defendant the right to know in detail how the AI technology works would likely impair the possibility of efficiently reusing that technology in the future, as it would enable strategic behaviours and ways to circumvent the use of the systems. In any case, detailed knowledge about an AI system would need to encompass not only the source code, not only the data set used by the investigators, as argued above, but also likely the user

manual, i.e., the instructions on how the system works – an element that is also often covered by copyright or secrecy law.[27] Even where copyright or secrecy law would not apply, this amount of information is of such technical complexity that it would seem unlikely for an average defendant to be able to sort it in a meaningful way in the time constraints of a criminal proceeding. Similarly, a detailed knowledge of the functioning of another legal system can only be reached by a certain degree of approximation, given the legal and linguistic discrepancies. Studies that make foreign legislation and case law freely accessible, such as Crossjustice and FACILEX, try to reduce such gap. Still, of course, the specific knowledge required in one particular case is hardly reduced by a schematic approach and needs to be further integrated by direct contact between the two systems.

On the other hand, excluding these complexity factors appears unrealistic and unfeasible. Deployment of AI technology is increasingly necessary to address the challenges posed by encryption and anonymity, and transnational cooperation, especially in the common legal area of the EU, is, at this point, a matter of fact in a significant number of criminal investigations.

How to ensure, then, the effectiveness to both fair trial rights and, at least, the available remedies?

First, the assumption that the AI system, to be effective, must be utterly secret in its operation can be disputed.

True, it is often helpful to keep some elements of the functioning of an AI system secret, such as the model parameters, the key inputs, or the outcome. Specifically, maintaining aspects of an internal functioning logic secret can help prevent strategic "gaming" of a system.

However, presenting that as a necessity is reminiscent of the idea of "security through obscurity", namely the practice of concealing the details or mechanisms of a system to enhance its security. Experts have strongly criticised this approach and stand in contrast with more modern ones, such as "security by design".[28]

Instead, computer science nowadays offers several advanced techniques to enable the governance of secret decision systems, namely a set of computational methods that can provide accountability and a certain degree of understanding of the functioning of the system, even when some information is

27 Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond' (August 1, 2017). A revised version of this paper has been published in International Journal of Law and Information Technology, 11 January 2019, DOI; 10.1093/ijlit/eay017, Available at SSRN: https://ssrn.com/abstract=3124901 or http://dx.doi.org/10.2139/ssrn.3124901.

28 Peter P. Swire, 'A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Agencies', (2006) 42 Houston Law Review SSRN 842228.

kept secret. Kroll et al.[29] give an overview of some of these methods: software verification, cryptographic commitments, zero-knowledge proofs, and fair random choices.

These methods ensure that the software and inputs meet the requirements for procedural regularity. Specifically, they can verify that the same decision policy was used for each decision, that the policy was established and implemented into the system before the inputs were known, and that the outcomes are reproducible. They can also be coupled with auditing, namely a set of techniques for the analysis of digital records documenting the responses of a computer system to the inputs it receives. The objective of auditing is to verify that proper procedures were adhered to (that is, compliant with the law) and to identify any unauthorized alterations in the system's functionality.

Second, access to the datasets must be addressed systematically, possibly by creating special rules at a centralised level. While access to the primary dataset seems difficult to achieve, for security and privacy issues,[30] structured access to the secondary dataset seems both feasible for the investigators and valuable for the defence.

In this regard, inspiring is the example of the Netherlands, where the defence, in Sky ECC cases, could file a motivated request to access parts of the secondary dataset. Once granted access, the examination of the information was realized via the same platform used by law enforcement authorities on the premises of the national forensic institute (but now also remotely).[31] This model could well be generalized and institutionalized in the various domestic systems. Last but not least, the claim for effective rights and remedies in such transnational and technological investigations can only call for a more conscious approach on the part of the defence. Investigators successfully carried out such a complex operation by creating Joint Investigation Teams and taking full advantage of the EIO cooperation mechanism.

To think, in the shoes of the defence, of countering such an organisation with a single set-up, in which each law firm is confronted with the difficulties of a transnational and technically complex investigation together, appears today to be guiltily naive. In this sense, at least for the more complicated general issues (e.g., how and where to get access to the secondary dataset, how to

29 Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson & Harlan Yu, 'Accountable Algorithms' (2017) 165 U. Pa. L. Rev. 633.

30 As the collected data in its most raw form is both likely used for intelligence purposes and certainly referring to a plethora of subjects, whose confidentiality shall be preserved.

31 As reported by Harm M. van Beek, Erwin J. van Eijk, RuudB. van Baar, Mattijs Ugen, J.N.C. Bodde & A.J. Siemelink 'Digital forensics as a service: Game on' (2015)15 Digital Investigation 27–28; see also Oerlemans, Royer (n 22) 456.

obtain information on the technical operations carried out, how to possibly challenge the use of EIO by the investigating authorities), the European bar has to take a step forward towards a common and more federated approach.

For example, it would seem essential to secure valuable information for an effective defence to present oneself in a unified manner before European agencies such as Europol (where the primary dataset of the EncroChat/Sky ECC data is stored).

5 The Lesson for Policymakers

All the challenges or difficulties outlined in the previous sections seem to be only partially addressed in the most recent legislation, i.e., the novel EU Regulation on Artificial Intelligence – or AI Act. The European Parliament adopted the AI Act on 14 March 2024 and published it on 12 July 2024 in the Official Journal of the EU as Regulation (EU) 2024/1689.[32]

The AI Act adopts a 'risk-based approach' to prevent and mitigate the risks of using AI. A risk-based regulation considers both the level and the characteristics of the risk associated with a practice to determine the applicable rules. At least in principle, legal restrictions should apply only to the extent necessary to prevent or mitigate risks.

Article 5 establishes some prohibited practices that constitute the highest risk associated with AI systems. The Regulation imposes a general prohibition on these practices, with some specific exceptions. Among them, and directly relevant to the uses of AI in investigation and judiciary activities, are the prohibitions of placing AI on the market, putting it into service, or using AI systems in two cases.

The first case is that of AI systems for criminal risk assessment of individuals (art 5(1)(d)): the AIA prohibits systems making risk assessments to predict criminal behaviour based solely on profiling or personality traits, supporting human assessment based on objective facts related to criminal activity. However, "this prohibition shall not apply to AI systems used to support the human assessment of a person's involvement in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity".

32 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, 2016/797/EU and 2020/1828/EU.

The second case is that of AI systems for real-time biometric identification in public spaces (art 5(1)(h)): the AIA prohibits systems using real-time remote biometric identification in publicly accessible spaces for law enforcement purposes. The Regulation provides a set of exceptions, namely when the use of these systems is strictly necessary for one of the following objectives: 1) for identifying victims of serious crimes such as abduction, trafficking, or sexual exploitation, and for locating missing persons; 2) for Preventing substantial and imminent threats to individuals' safety or preventing terrorist attacks; and 3) for Locating or identifying individuals suspected of major criminal offenses referred to in Annex II of the AIA, if also punishable for a maximum period of at least four years, to facilitate criminal investigations, prosecutions, or the execution of criminal penalties.

However, in the cases mentioned above, the adoption of real-time remote biometric identification systems requires the adoption of certain procedural guarantees. These safeguards consist, on the one hand, in assessing the preconditions authorising the use of such technologies and the potential consequences for rights and freedoms; on the other hand, in time, geographical and personal limitations are to be respected in using such systems. In all cases, prior authorisation is required by the judicial authority or an independent administrative authority of the Member State and granted upon reasoned application. Such authorisation, however, in a "duly justified situation of urgency" (Art 5(3)) may also be requested during or after use. The competent authority may only grant authorisation if, based on objective evidence or clear indications presented to it, the use of the system in question is necessary and proportionate to achieve one of the three objectives specified in (art 5(1)(h)). Due to the high risk that real-time biometric identification systems entail for individuals and groups, the prohibition outlined in the AIA is a welcomed choice; however, the exceptions' extension seems too large.

Pursuant to a risk-based approach, the Regulation also identifies high-risk AI systems (Art 6), referring to two lists in Annex I and III. These systems are subject to a series of provisions on their development, sale, and deployment in the EU market. The objective is to ensure the risk to safety, health, and protection of fundamental rights associated with such systems are mitigated without unnecessarily hindering their adoption.

Among the AI systems listed in ANNEX III are AI systems for law enforcement (annex III 7(a, b, c, d)). The reason for their inclusion is explained in recital 59 of the AI Act: "Given their role and responsibility, actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on

fundamental rights guaranteed in the Charter." Among the rights that could be hampered is the exercise of important procedural fundamental rights, such as the right to an effective remedy and a fair trial, as well as the right of defence and the presumption of innocence.

Other systems listed in Annex III that are relevant for our purposes are the AI systems used in migration, asylum, and border control management (annex III 8) since they affect persons who are often in particularly vulnerable positions and who are dependent on the outcome of the actions of the competent public authorities; and the AI systems used in the administration of justice (annex III 9), considering their potentially significant impact on democracy, the rule of law, individual freedoms as well as the right to an effective remedy and to a fair trial.

A core assumption of the AI Act is that risk can be calculated and classified in an objective and predetermined manner. While this may apply to a certain extent when we consider the safety and health of citizens, concerns arise as to whether the risk can be determined concerning fundamental rights: the AI Act is based on the idea that the impact on fundamental rights can be assessed according to a scale of values and that, to a certain extent, it can be deemed acceptable. However, the Act does not indicate how the acceptability judgment shall be made. The danger is that the risk assessment on fundamental rights will essentially be based on a subjective evaluation by the AI system provider and its greater or lesser risk aversion.

Concerning fundamental rights, what raises concerns is the decision by the EU legislator not to rely on a rights-based approach along the same lines as the Data Protection Regulation (GDPR).

Although it pursues the objective of protecting fundamental rights, the AI Act does not introduce any new rights that can be actionable and enforceable by individuals who may be adversely affected by the use of the AI system, other than the right to lodge a complaint with a market surveillance authority (Art 85) and the right – introduced only following an amendment proposed by the EU Parliament – to obtain an explanation "of the role of the AI system in the decision-making procedure and the main elements of the decision taken" (Art 86).

However, it should be noted that the right to obtain an explanation of the role of the AI system in decision-making does not involve a full right to the disclosure of detailed information on the functioning of the system, including all the elements, data and parameters that would be necessary to replicate and possibly challenge the fairness and procedural regularity of the system. Moreover, the right is subject to a significant limitation in the AI Act: Art 86(1), establishing this right, shall not apply to the use of AI systems "for which

exceptions from, or restrictions to, the obligation under that paragraph follow from Union or national law in compliance with Union law." (Art 86(2)). This would leave open the problem of cases such as the EncroChat/Sky ECC mentioned above.

The problematic choice of the EU legislator of not providing actionable and enforceable by individuals who may be affected by AI systems is linked to a bold (but possibly wrong) assumption within the regulatory regime designed by the AI Act: that the use of AI systems may be fully regulated, just like any other product, by designing a set of obligations targeting specifically those persons creating the product (system developers) and using it (deployers). However, such strong assumptions may be rendered inaccurate by the technological peculiarities of an AI system, which, differently from other products, may evolve and learn by itself, sometimes in ways that escape the complete control of their developers and users. Maybe the idea that problems will and shall always be identified and solved *ex-ante* (during the development or deployment) could have been coupled with a regulatory empowerment *ex-post* of the individuals affected by AI, providing them actionable rights.[33]

Moreover, such focus on developers and deployers overshadows the transnational dimension of AI systems application, in particular in the context of criminal justice: no rules or directions are provided by the EU legislator, as highlighted above, to find a viable solution for situations like the Encrochat/Sky ECC cases, which clearly show a problem of compression or limitation of fundamental rights, in a transnational dimension.

In the face of these issues, the multidisciplinary and integrated approach proposed by this research project, in which, albeit with difficulty, law and technology have dialogued together since the design of the reference rules, can perhaps be an inspiring example.

33 On the problem of assumptions in technology regulation, see BJ Ard, Rebecca Crootof. 'Legal responses to techlaw uncertainties' in Bartosz Brożek, Olia Kanevskaia, Przemysław Pałka (eds.), *Research Handbook on Law and Technology* (2023) 28–44.