Artificial Intelligence and Digitalisation of Judicial Cooperation

The Main Provisions in Recent EU Legislation

Katerina Entcheva, Ioana Mazilescu *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

Artificial intelligence (AI) tools are increasingly being used by justice professionals to improve the speed and the efficiency of legal proceedings and to alleviate administrative burdens. Digital and AI tools may be a game changer in enhancing the quality of justice and allowing justice professionals to concentrate on more substantive tasks. Digitalisation and the use of AI in justice bring about significant benefits but can also present certain risks, thus requiring a clear regulatory framework. The last few years have brought about a considerable number of new rules agreed at EU level that cover different aspects of the digital developments experienced by our society and economy.

This article presents the main elements of two of these acts: the AI Act and the Regulation on digitalisation of judicial cooperation, focusing on the aspects with the most relevance for the justice sector. It explains which AI practices are prohibited and the approach to regulating AI systems. It then presents the digital technology tools that will underpin cross-border cooperation between judicial authorities in the EU and will help citizens to access courts more easily and conveniently in cross-border disputes. In a nutshell, the article explains the regulatory framework and the expected benefits of digitalising judicial cooperation and access to justice. The next steps related to these laws are also briefly explained, and the authors conclude that further digitalisation in the justice field is to be expected.

AUTHORS

Katerina Entcheva

Policy officer
European Commission, DG for Justice and Consumers

Ioana Mazilescu

Deputy Head of Unit
European Commission, DG for Justice and Consumers

CITE THIS ARTICLE

Entcheva, K., & Mazilescu, I. (2025). Artificial Intelligence and Digitalisation of Judicial Cooperation : The Main Provisions in Recent EU Legislation. Eucrim – European Law Forum: Prevention • Investigation • Prosecution. https://doi.org/10.30709/eucrim-2024-018

Published in eucrim 2024, Vol. 19(3) pp 202 – 205

https://eucrim.eu

ISSN:

CC BY ND

I. The Artificial Intelligence Act

1. Introductory Remarks

As announced in its White Paper on Artificial Intelligence (AI) of 2020,[1] the European Commission has proposed several pieces of legislation aimed at creating an ecosystem of trust to facilitate the uptake of AI in the European Union. Several of these proposals have amended particularly the EU acquis concerned with the safety of products. In this context, the Commission had proposed a legislative package on liability in 2022: the proposals for the AI Liability Directive (AILD)[2] and the revision of the Product Liability Directive (PLD)[3]. Against this background, this article will focus on describing the provisions of the main legal framework regulating AI systems in the EU: The Artificial Intelligence Act (Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence).[4]

2. Key provisions of the AI Act particularly in relation to the justice sector

Regulation 2024/1689 entered into force on 1 August 2024. The AI Act provides for fully harmonised rules for the following:

- Placing on the market, the putting into service, and the use of AI systems in the European Union;
- Prohibitions of certain AI practices;
- Specific requirements for high-risk AI systems and obligations for operators of such systems;
- Certain transparency rules;
- Rules on market surveillance and enforcement.

The Regulation stipulates **clear requirements and obligations for AI developers and deployers** regarding specific uses of AI. At the same time, the regulation seeks to reduce administrative and financial burdens for business, in particular small and medium-sized enterprises (SMEs). The AI Act follows a **risk-based approach,** i.e., some AI practices are prohibited and some are considered high-risk and are subject to specific requirements; certain transparency rules are applicable to specific situations. Yet, AI systems that do not fall under the categories or uses regulated in the AI Act can be developed and placed on the EU market without being subject to any specific rules. Certain AI tools for the administration of justice are classified as high-risk; therefore, they have to comply with specific requirements.

The AI Act aims to ensure that when AI is used, including in the justice sector and the administration of justice, safeguards and control mechanisms are in place to minimise risks to fundamental rights, safety, and the rule of law, among others.

The legal framework set out by the AI Act follows the objective of boosting the trustworthy use of AI tools across sectors, including in the area of justice. In turn, this would contribute to supporting judges and justice professionals in the administration of justice and to improving the efficiency of judicial procedures. However, national judicial authorities preserve the right to opt for or against the use of AI in the justice sector.

Prohibited AI practices

Overall, the AI Act recognises that certain AI systems are considered too risky and thus **prohibited by law**. For example, in the context of AI in the area of justice, the act bans the placing on the market, the putting into

https://doi.org/10.30709/eucrim-2024-018

service, or the use of an AI system for making risk assessments of individuals in order to assess or predict the risk of committing a criminal offence, based solely on the profiling of this person or on assessing their personality traits and characteristics. The Commission has been tasked with adopting guidelines for the practical implementation of this provision by February 2025.

High-risk AI systems

In addition, the AI Act classifies **certain AI systems used in specific areas as high-risk**. Putting on the market and use of such systems will be subject to strict obligations for both the entities developing them and their deployers (i.e., legal persons or professionals who use AI systems). Additional obligations and requirements for deployers may apply to fulfil EU or national obligations, for instance in the area of consumer law, product liability, and data protection.

AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts are one example of what is considered high-risk AI systems. This is due to their potentially significant impact on the rule of law and on the fundamental rights enshrined in the Charter of Fundamental Rights of the EU, notably the right to a fair trial and to an effective remedy, the presumption of innocence and the right of defence, human dignity, and non-discrimination.

The AI Act therefore recognises and reaffirms the **role of the judge**: while the use of AI tools can support the judiciary, it should not replace the decision-making power of judges. The final decision-making must remain a human-driven activity.

Moreover, the following AI systems are considered high-risk and consequently subject to the requirements explained above:

- AI systems intended to be used by law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups,[5] and
- AI systems intended to be used for the profiling of natural persons in the course of the detection, investigation, or prosecution of criminal offences.

Non-high risks AI systems

At the same time, AI systems for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases are not considered high-risk. This may concern, for example: a) the anonymisation or pseudonymisation of judicial decisions, documents or data, b) communication between personnel, or c) administrative tasks.

Derogations

The AI Act establishes a derogation for the use of certain high-risk AI systems, which is relevant for the use of AI in the area of justice. Such systems should not pose a significant risk of harm to the fundamental rights of individuals, e.g., by not materially influencing the outcome of decision-making. The derogation applies where one of the following conditions is fulfilled:

- The AI system is intended to perform a narrow procedural task;
- The AI system is intended to improve the result of a previously completed human activity;

- The AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review, or;
- The AI system is intended to perform a preparatory task to an assessment relevant, for instance, for AI in justice.

To guide the application and interpretation of the AI Act in general, including the use of AI in the administration of justice, the AI Act empowers the European Commission with issuing guidance in respect of prohibited practices (by February 2025) and of high-risk AI systems (by February 2026).

This guidance will be particularly relevant for those **Member States already using AI** or intending to do so in the justice sector. From the current information available from a number of EU Member States, a range of projects using AI in justice is being developed or starting to be used at national level. In 2023, five Member States were planning to use AI in their justice systems, while in six Member States courts and prosecutors use some AI applications in core activities.[6]

II. The Digitalisation Regulation

1. Introductory Remarks

Regulation (EU) 2023/2844 (hereinafter Digitalisation Regulation)[7] aims to improve the efficiency and the resilience of cross-border judicial cooperation procedures, still mostly a paper-based endeavour as things stand. It will also enhance access to justice, as citizens and companies will have the option of using digital communication channels to make certain submissions to the competent authorities and to participate remotely in court hearings through videoconferencing and other distance communication technologies.

2. Key elements

The Digitalisation Regulation provides a comprehensive legal framework for the use of digital technologies in **civil, commercial, and criminal cases with cross-border implications** by establishing rules on digital communication between competent judicial authorities, and between natural and legal persons (parties to the proceedings) and the competent judicial authorities. It is also applicable to electronic exchanges with Union agencies and bodies. Additionally, the Regulation establishes a legal basis for conducting videoconferencing sessions across Member States and lays down harmonised rules on the acceptance of electronic documents and electronic signatures and seals, building up synergies with the eIDAS Regulation[8]. The Digitalisation Regulation includes the following main elements:

- **The use of an e-CODEX-based decentralised IT system** is mandatory for digital exchanges between competent judicial authorities and between these authorities and the Union agencies and bodies. This obligation is subject to certain limited and well-defined exceptions where the use of the decentralised IT system is either not possible (e.g., disruption of the system, physical nature of the material, etc.) or not appropriate (e.g., direct judge-to-judge communication, etc.);
- **The use of digital communication channels** by natural and legal persons is optional and applies only in civil and commercial matters. The Regulation establishes a European electronic access point (EEAP) on the e-Justice Portal, which would allow natural and legal persons to submit cases or otherwise communicate with the competent authorities;

https://doi.org/10.30709/eucrim-2024-018

- The Regulation allows for the use of **videoconferencing and other distance communication technology** in the following ways:
  - In **civil and commercial matters** – the provision applies where at least one of the parties to the proceedings or their presentative is present in the territory of another Member State. The possibility is subject to the discretion of the authority – the decision should be based on the existence of the technology, the opinion of the other party, and the appropriateness of the use of such technology for the purposes of the case at hand. The procedure for holding the hearing should be the one under the applicable national law;
  - In **criminal matters**, the scope of videoconferencing is limited to certain judicial cooperation procedures. Special attention is paid to the protection of the procedural rights of the persons. Again, national law governs the procedure for conducting videoconferencing;
- **Qualified electronic signatures/seals** must be used for communication between competent authorities and between these authorities and the Union agencies and bodies. Natural or legal persons may either use a qualified electronic signature or seal, or electronic identification with assurance level high, as specified in the eIDAS Regulation;
- Documents **should not be denied legal effect** only because they are in electronic form;
- **Training** of justice professionals should be ensured by Member States.

The Regulation is complemented by some technical provisions:

- The decentralised IT system will be established by implementing acts. 24 implementing acts in total will be adopted by 2028. The adoption of each implementing act will be followed by an implementation period of two years for the actual development of the reference implementation software (or national back-end system) and deployment of the system at national level;
- The Commission will provide a reference implementation software, which Member States may select over nationally developed back-end systems.
- The Commission will set up and maintain the EEAP and will provide for user support.

The Regulation **entered into force** on 16 January 2024. The **date of application** will be 15 months from the entry into force of the regulation for the videoconferencing provisions and two years from the date of entry into force of the corresponding implementing acts setting up the decentralised IT system and EEAP.

The work on the implementing acts is currently underway with discussions on the first batch of implementing acts. In criminal matters, the procedures relating to the European Investigation Order, the European Arrest Warrant, and the Freezing and Confiscation Orders will be the first ones to be digitalised.

III. Final remarks

The digitalisation of justice is clearly an ongoing process that will continue. It will require a combination of measures, from funding and organisational aspects, to rule setting and training. Digitalisation implies, on the one hand, specific measures at the level of each institution and, on the other hand, coordinated efforts at national and European level to respond to the needs of justice in the most efficient way. Digitalisation is a

necessary and inevitable process that should lead to more accessible, transparent, and efficient justice and which responds to the demands and expectations of our increasing digitalised economy and society.

1. White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, available at: <https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en> accessed 10. January 2025.↩
2. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final.↩
3. Proposal for a Directive of the European Parliament and the Council on liability of defective products, COM(2022), 495 final.↩
4. Full reference: 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) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.↩
5. As mentioned above under "prohibited AI practices", risk assessments concerning an individual in order to assess the likelihood of their committing a crime or predicting the occurrence of an actual or potential crime based solely on profiling an individual or on assessing their personality traits and characteristics is prohibited. In line with the presumption of innocence, individuals should always be judged on their actual behaviour, thus such tools should only support a risk assessment when there are objective, verifiable facts to support a reasonable suspicion and if there is a human assessment.↩
6. The 2024 EU Justice Scoreboard, COM(2024) 950, available at: <https://commission.europa.eu/document/download/84aa3726-82d7-4401-98c1-fee04a7d2dd6_en?filename=2024%20EU%20Justice%20Scoreboard.pdf> accessed 10 January 2025.↩
7. Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation, OJ L, 2023/2844, 27.12.2023.↩
8. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, 73.↩

Authors statement

The information and views set out in this article are those of the authors and do not necessarily reflect the official opinion of the European Commission.

COPYRIGHT/DISCLAIMER
© 2025 The Author(s). Published by the Max Planck Institute for the Study of Crime, Security and Law. This is an open access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see https://creativecommons.org/licenses/by-nd/4.0/.
Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union

https://doi.org/10.30709/eucrim-2024-018