

EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ)

2ND REPORT ON THE USE OF ARTIFICIAL INTELLIGENCE (AI) IN THE JUDICIARY
based on the information contained in the CEPEJ resource Centre
on cyberjustice and AI



ADOPTED BY THE CEPEJ AT ITS 46TH PLENARY MEETING
(18-19 JUNE 2026)
CEPEJ(2026)7

French Edition :

Commission européenne pour l'efficacité de la justice (CEPEJ) - 2eme Rapport sur l'utilisation de l'intelligence artificielle (IA) dans le système judiciaire, basé sur les informations contenues dans le centre de ressources sur la cyberjustice et l'IA de la CEPEJ.

The opinions expressed in this document are the responsibility of the author(s) and do not necessarily reflect the official policy of the Council of Europe.

The reproduction of extracts (up to 500 words) is authorised, except for commercial purposes as long as the integrity of the text is preserved, the excerpt is not used out of context, does not provide incomplete information or does not otherwise mislead the reader as to the nature, scope or content of the text. The source text must always be acknowledged as follows "© Council of Europe, year of the publication". All other requests concerning the reproduction/translation of all or part of the document should be addressed to the Documents and Publications Production Department (SPDP) or publishing@coe.int.

All other correspondence concerning this document should be addressed to the European Commission for the efficiency of justice (CEPEJ) or cepej@coe.int

Cover design and layout:

European Commission for the efficiency of justice (CEPEJ), Directorate-General for Human Rights and the Rule of Law, DG1, Council of Europe

Photo: Shutterstock

© Council of Europe, June 2026

Table of Contents

Executive Summary	2
I. Introduction	2
II. Objectives for this report	3
III. The Resource Centre on Cyberjustice and Artificial Intelligence	3
1. Purpose	3
2. Structure	3
3. Methodology	4
4. User engagement	4
IV. Key elements of the Resource Centre	4
1. Number of cyberjustice & AI tools	4
2. Main categories of application	4
3. Indication if the system is implemented by a public, private body, or by academia	6
4. Main target group/audience of the tools	6
5. Country (region) of application	7
6. Selected examples of cyberjustice tools added in 2025 to the Resource Centre by area of application	7
V. Contextual developments and important regulations in 2025	9
1. The impact of EU AI Act on court practice	10
2. Cybersecurity in courts	11

Executive Summary

To date, 176 cyberjustice tools, aiming at improving judicial efficiency and accessibility, primarily from Europe, have been identified and listed in the CEPEJ Resource Centre on Cyberjustice and Artificial Intelligence (AI), of which 51 cyberjustice tools were added in 2025.

In 2025, Large Language Models (LLMs) to assist judicial professionals in legal research and drafting have been increasingly deployed, while earlier entries focused on the general digitalisation of judiciary.

The integration of AI into the administration of justice is now no longer a secondary concern but a fundamental component of broader public sector reform.

Despite growing interest in AI applications across justice systems, as proven by the Resource Centre, countries have not yet established systematic mechanisms to collect and analyse data on the AI applications' impact.

There are shortcomings in the development of judicial AI tools, where technology is often pursued for its own sake rather than to address clearly defined problems. Thus, existing solutions do not always respond to real user or institutional needs.

Cybersecurity is an increasingly important concern for judicial authorities, encompassing a wide array of technical safeguards for IT security, safe cloud computing, the integrity and privacy of judicial data.

The phased application of the EU AI Act began in 2025 prohibiting certain AI practices, such as crime prediction systems and requiring AI literacy efforts. As of December 2027 (initially foreseen for mid-2026, and only recently postponed), high-risk systems, to which those used in the justice system could potentially belong, will require, among other things, a Fundamental Rights Impact Assessment. This regulation potentially affects directly more than half of the Council of Europe member States.

The Resource Centre supports the implementation of the Council of Europe Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law, by identifying and allowing discussion of AI systems used in the judiciary.

I. Introduction

1. This annual report¹ offers a summary of the collection of artificial intelligence (AI) and cyberjustice tools/systems applied within European judicial systems (collectively referred to as 'cyberjustice tools') through the CEPEJ Resource Centre on Cyberjustice and Artificial Intelligence (hereinafter referred to as 'the Resource Centre' or 'the Centre').²

2. The concept of AI tools (systems) discussed in the report is based on the Council of Europe Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law (CETS No. 225, hereinafter as 'the Framework Convention').³

¹ This report was drafted by the members of the CEPEJ Artificial Intelligence Advisory Board (AIAB)

² Available at <https://www.coe.int/en/web/cepej/resource-centre-on-cyberjustice-and-ai>.

³ Article 2 of the AI Framework Convention provides the following definition: "artificial intelligence system" means a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment".

3. This report was drafted by the members of the CEPEJ Artificial Intelligence Advisory Board (AIAB).⁴ The AIAB provides expert advice on AI related issues in the judicial environment. It was established in 2022 to support the CEPEJ in monitoring the actual emergence of AI applications in the justice sector and to implement related strategies as well as to contribute to the reflection on the use of AI in justice systems with respect to human rights. The AIAB is a key element of the roadmap to ensure an appropriate follow-up of the “European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment” (referred to as ‘CEPEJ AI Charter’), adopted in 2018.⁵ The AIAB is steered by and reports regularly to the Working Group on Cyberjustice and Artificial Intelligence (CEPEJ-GT-CYBERJUST).

4. This second report covers the developments and activities of the year 2025, providing an overview of this year’s progress and emerging issues concerning cyberjustice tools in the general field of justice.

5. In the final section of the report, the AIAB highlights contextual and regulatory developments from the reporting period that are not directly deducible from the collected data, but which are relevant to the general application of AI in the field of justice.

II. Objectives of this report

6. This report aims at giving factual insights, useful for dialogue and research on the responsible integration of cyberjustice tools in the justice sector.

7. Data collected in the Resource Centre allow analysis of how these tools are reshaping legal systems while identifying risks and governance issues.

8. This annual overview aims to help decision-makers to stay informed of technological advancements and opportunities in the justice sector.

III. The Resource Centre on Cyberjustice and Artificial Intelligence

1. Purpose

9. The Resource Centre, established in 2023, monitors the integration of modern digital technologies, particularly AI systems, into justice systems, enabling their evaluation. As a publicly accessible resource, its aim is to identify key technologies that could improve the efficiency, transparency and accessibility of the justice system,⁶ while encouraging consideration of human rights in the development, responsible use and ethics of these tools.

10. Page impressions count 15,423 views of English version and 3,483 views of the French version at the time of preparation of this report.⁷

2. Structure

11. The tools featured in the Resource Centre are sorted by main areas of application that capture key legal tasks: 1) Document search, review and Large-scale Discovery, 2) Online Dispute Resolution, 3) Prediction of Litigation Outcomes 4) Decision support, 5)

⁴ The AIAB is composed of five board members (mandate 2024-2025): Katie Marie Atkinson (United Kingdom), Jehanne Dussert (France), Alfonso Peralta Gutierrez (Spain), Matthieu Quiniou (France), Marek Świerczyński (Poland), Morgan Briggs (United Kingdom).

⁵ Available at <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>.

⁶ Full explanation available at: <https://www.coe.int/en/web/cepej/resource-centre-on-cyberjustice-and-ai> (in particular frequently asked questions (FAQ) section).

⁷ See current numbers at <https://public.tableau.com/app/profile/cepej/vizzes>.

Anonymisation and pseudonymisation, 6) Triaging, allocation and workflow automation, 7) Recording, transcription and translation, 8) Information and assistance services. The Resource Centre provides the following details for each tool: name, a short description, the year of deployment, status of development, country of application and the addressed target group.

3. Methodology

12. Data is collected primarily through the CEPEJ's European Cyberjustice Network (ECN) members,⁸ including most Council of Europe member states and observers. The data is then classified and reviewed by the AIAB. Information is updated progressively, with new entries added and inaccuracies being corrected.

13. To obtain information, the CEPEJ provides a dedicated online form for readers and users to share their thoughts and experiences and allowing the identification and inclusion of new cyberjustice tools.⁹ The CEPEJ organises ECN webinars and AIAB meetings where participants can discuss their experiences and perspectives on the information presented in the Resource Centre.

4. User engagement

14. CEPEJ actively seeks feedback through various channels to enrich the Resource Centre and stay current with cyberjustice developments. Its work has been prominently featured in high-level policy and academic events. For instance, the Bingham Centre for the Rule of Law, an independent research body, explicitly referenced the "1st Report on the use of artificial intelligence (AI) in the judicial system based on the information contained in the CEPEJ's Resource Centre" as a key document for a panel discussion on Council of Europe standards for AI in the courts.¹⁰

15. The Resource Centre's data has been used in formal submissions to international human rights bodies. In its written submission to the United Nations Special Rapporteur on the independence of judges and lawyers, the European Criminal Bar Association (ECBA) cited the 2025 CEPEJ report and its data as evidence of the widespread consideration of AI implementation across European Union jurisdictions.¹¹

IV. Key elements of the Resource Centre

1. Number of cyberjustice & AI tools

16. Number of systems: 176

2. Main categories of application

17. According to the data collected, there is a significant diversity in the types and applications of AI tools being used or developed for the justice sector.

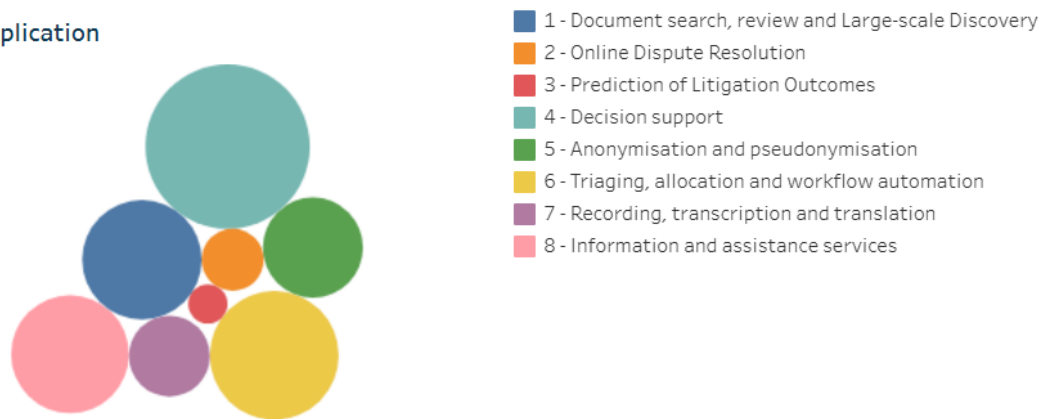
⁸ See <https://www.coe.int/en/web/cepej/european-cyberjustice-network-ecn->.

⁹ Available at <https://www.coe.int/en/web/cepej/resource-centre-on-cyberjustice-and-ai>.

¹⁰ Available at <https://binghamcentre.biicl.org/events/1447/ai-in-the-courts-ground-breaking-standards-from-the-council-of-europe-and-perspectives-from-the-member-states>.

¹¹ Available at <https://www.ohchr.org/sites/default/files/documents/issues/ijudiciary/cfis/ga80/subm-sr-independence-judges-cso-55-european-criminal-bar-association.pdf>.

Areas of application



18. Based on the data for 2025 the distribution of the 51 new tools added to the CEPEJ Resource Centre across the 8 categories is as follows: (many systems belong to two categories):

- 1) Document search, review and Large-scale Discovery¹²: 9 tools
- 2) Online Dispute Resolution¹³: 3 tools
- 3) Prediction of Litigation Outcomes¹⁴: 2 tools
- 4) Decision support¹⁵: 33 tools
- 5) Anonymisation and pseudonymisation¹⁶: 11 tools
- 6) Triaging, allocation and workflow automation¹⁷: 14 tools
- 7) Recording, transcription and translation¹⁸: 5 tools
- 8) Information and assistance services¹⁹: 25 tools

19. The main focus during this period was on providing decision support, which was often combined with information and assistance services. This reflects the trend of integrating Large Language Models (LLMs) to support legal professionals with their research and drafting tasks. This indicates a significant shift. While earlier entries focused on traditional 'cyberjustice' (i.e. general digitalisation), new entries are heavily weighted towards artificial intelligence, particularly generative AI and natural language processing (NLP).

¹² These solutions create a searchable collection of case-law descriptions, legal text and other insights to be shared with legal experts for further analysis and large-scale discovery on high volumes of electronic documents. Examples are search engines with interfaces applied to case law and judicial files.

¹³ These solutions cover technologies used for the resolution of disputes between parties with limited human intervention, which can be achieved through hardware and/or software. It concerns mainly Alternative Dispute Resolution, but also dispute resolution in the context of courts.

¹⁴ These solutions cover tools that use symbolic representations of legal knowledge and also, contrastively, tools that learn from large datasets to identify patterns in the data that are consequently used to visualise, simulate or predict new litigation outcomes.

¹⁵ These solutions facilitate or automate stages in the decision-making processes in the justice systems. So far, there have been no reports of fully automated decision-making processes without any human supervision. Examples include systems summarising texts, extracting specific information in applications, calculating scales for sentencing and compensation.

¹⁶ These solutions are used for removing and replacing identifying information such as personal data of court users in judgments.

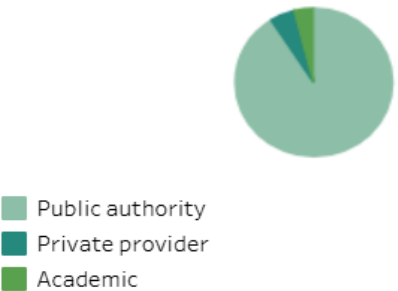
¹⁷ These solutions are used to facilitate or complete some tasks and activities during the lifecycle of the proceedings within the Case Management System, minimising the need for human input. Examples are: registration and allocation of court matters, assigning levels of priority to tasks or individuals to determine the most effective order in which to deal with them.

¹⁸ These solutions are capable of recognising and analysing speech as well as written text and communicating back. Their main use for courts is in voice/speech recognition and transcription of court proceedings as well as translation.

¹⁹ These solutions provide individuals with information on services available in the justice systems and link individuals to the services and opportunities that are available. Examples are chatbots or other interfaces accessible for the public.

3. Indication if the system is implemented by a public, private body, or by academia

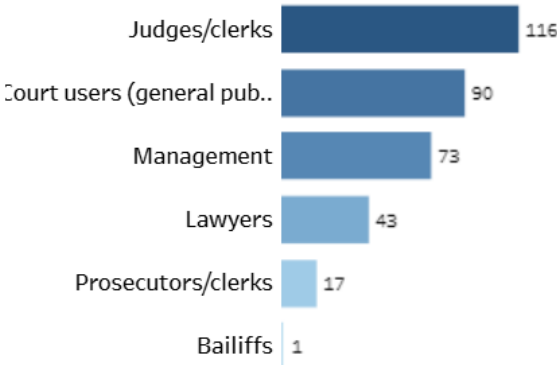
Implementation



20. This distribution shows a current focus on the public sector, with private sector or academia playing a supportive role to the public institutions.

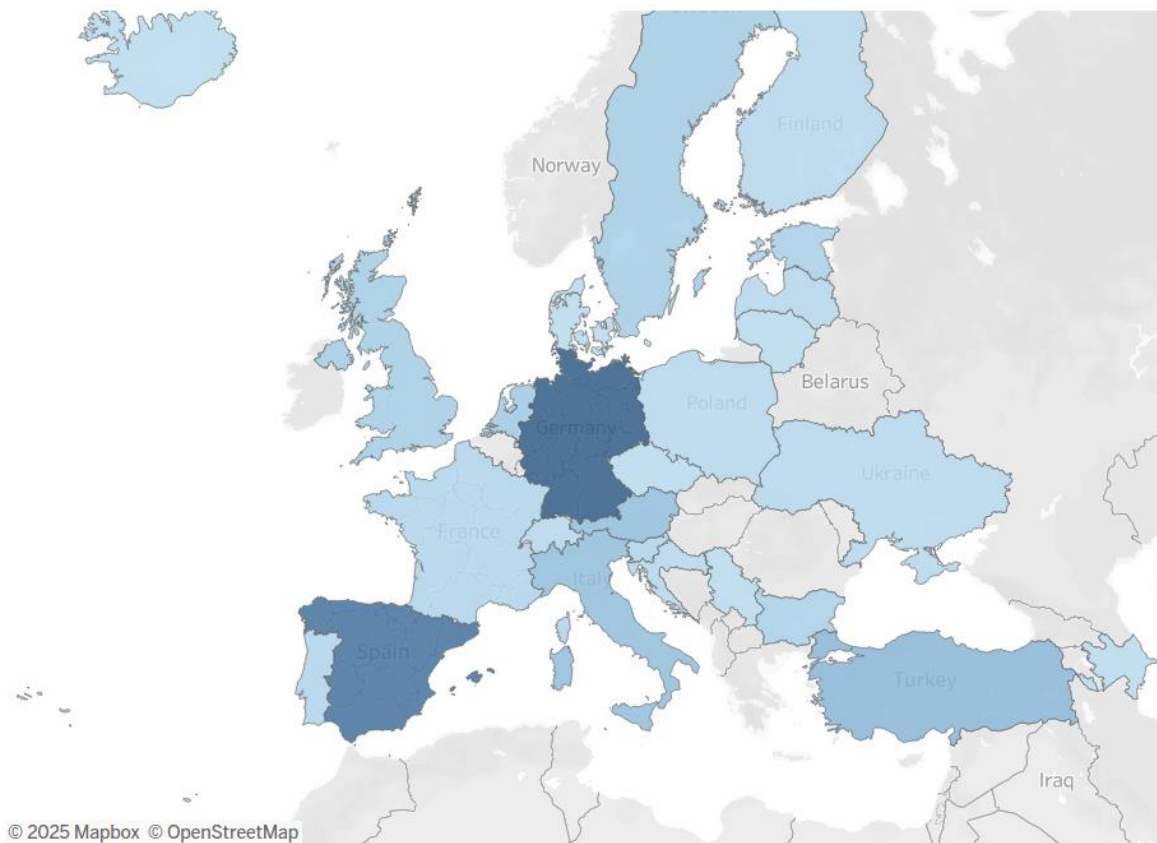
4. Main target group/audience of the tools

Target audience



21. The AI tools are designed for various target groups within the justice system, mainly judges, court users and court management.

5. Country (region) of application



22. The research is currently focused on the use of AI tools in the European judiciary. Most of the systems are already operational, but still with a significant number in the pilot/beta phases. It is difficult to determine the exact distribution of tools, as some countries communicate sub-modules of more comprehensive systems, while others apply similar tools under different names within federal structures.

6. Selected examples of cyberjustice tools added in 2025 to the Resource Centre by area of application

1) Document search, review and Large-scale Discovery

Document Analysis – Legislation, Spain

This tool is part of a suite of AI-powered services provided by the Ministry of the Presidency, Justice and Parliamentary Relations of Spain. It automates and facilitates various document processing tasks including document analysis by legislation. It identifies references to legislation within a document and navigates to the parts of the document where such references are made. It also displays the range of the norm, its full denomination and the link to the Official State Gazette site where it is published.

Database of Legal Positions of the Supreme Court (База правових позицій Верховного Суду), Ukraine

The database was created to promote the unity of judicial practice, enhance legal certainty, and facilitate access to legal positions contained in the Supreme Court's decisions. This tool is designed to support transparency in the application of law, stability of judicial decisions, and the overall improvement of the quality of justice

in Ukraine. The database was developed with the needs of legal practitioners in mind, incorporating modern IT solutions and elements of generative AI.

2) Online Dispute Resolution

Amica, Australia

Amica is an Australian government-supported online platform designed to help separating couples reach agreements on parenting and property matters without going to court. Using AI, it provides personalised suggestions based on factors such as the duration of the relationship, financial contributions, and future needs. The platform guides users through structured negotiations, enabling them to create legally enforceable agreements confidentially and cost-effectively. Amica is addressed at couples experiencing amicable separations who want a structured yet flexible approach to resolving family law issues.

3) Prediction of Litigation Outcomes

AI model for analysis and standardization of case law and prediction of outcomes in court cases, Bulgaria

The AI tool comprises a model trained on a wide range of anonymised court decisions, selected by judges across various legal fields, to detect and analyse recurring patterns. The AI tool processes data and provides automated case analysis, also supporting judicial work by generating draft judicial acts based on mandatory case law and case law selected by appellate and cassation judges. This tool will also include tools to detect inconsistencies and divergent practices, helping to improve predictability and consistency in the administration of justice. The app uses AI to interpret user requests and generate the required documents, instructions, or actions. Users input their issue, and the system produces the appropriate template or communication.

4) Decision Support

StruKI (Strukturierung mit Künstlicher Intelligenz), Germany

The aim of the 'StruKI' project is to provide an AI-based structuring tool to relieve the workload in the judiciary and to support work processes that would otherwise lead to a significant increase in work. This includes the AI-supported processing of applications for financial support in court proceedings (legal aid), the preparation of cost orders in mass proceedings or the the anonymisation of documents.

5) Anonymisation and Pseudonymisation

Document Anonymisation – Automatic, Spain.

This tool is part of a suite of AI-powered services provided by the Ministry of the Presidency, Justice and Parliamentary Relations of Spain. It automates and facilitates various document processing tasks including automatic document anonymisation. Automatic anonymisation consists of replacing all categories of nominal entities detected (e.g., personal names, places, identification codes of natural and legal persons) with hyphens. The tool also allows the user to navigate to the parts of the document where the anonymized entities appear. Once the anonymisation process is completed, the document can be downloaded for use and distribution.

6) Triaging, allocation and workflow automation

LexNET - NLP-automated upload of information, Spain

LexNET is the secure information exchange platform between judicial bodies and professionals involved with the Administration of Justice and provided by the

Ministry of Justice of Spain. LexNET allows for the digital submission of documents, as well as the transfer of copies when needed, by legal practitioners. It also allows for the delivery of notifications from judicial bodies. LexNET has incorporated Natural Language Processing (NLP) to streamline the update of new procedural documents. In particular, NLP is used to scan the documents (to be forwarded to judicial bodies) and extract the different nominal entities contained therein. These entities are then matched with the fields of the form that must be completed to properly route the forward of any given document – fields that the user would have needed to select manually, one by one. However, when matched, such fields are automatically set to the value of the extracted nominal entities, thus releasing the user from such manual burden.

7) Recording, transcription and translation

Chat-TF, Switzerland

Before submitting a query to an online artificial intelligence chatbot, such as ChatGPT, the Chat-TF system anonymises the query using AI techniques and then submits it to the chosen artificial intelligence engine (e.g. to generate a summary). Once the result has been obtained from the external artificial intelligence chatbot, the anonymised names are reintroduced into the text by the internal artificial intelligence system (Chat-TF) and is returned to the user.

8) Information and assistance service

Several popular generative AI tools, such as Gemini and Copilot, were added to the Resource Centre in 2025, reflecting both the growing use of these systems by legal professionals and their official provision to judicial staff.

V. Contextual developments and important regulations in 2025

23. The above mentioned growing use of generative AI tools by legal professionals and their official provision to judicial staff also highlights the risk of 'Shadow AI' as defined in the new CEPEJ Guidelines on the use of generative artificial intelligence for the courts.²⁰ Shadow AI refers to the unauthorized use of commercial public AI tools within the judiciary, which presents significant security vulnerabilities and ethical challenges for the court system.

24. Although AI is reportedly making legal work faster, so far, there is no evidence that it makes justice fairer or decisions more accurate. AI-generated evidence can also have a negative impact on the fairness of trials with deepfakes and digital enhancement technology. The resulting destabilisation of evidence reliability, risks increasing scepticism and harming public trust.²¹ To safeguard judicial autonomy, AI systems should be supported by existing checks and balances. These governance mechanisms are provided by both the Framework Convention and the EU AI Act.

25. Governments of the member states are now establishing strong policy and regulatory frameworks to mitigate risks associated to the potential for over-reliance on AI. For example, AI is increasingly being used for translating texts promptly with accuracy. However, unlike humans, such tools predict words based on probability rather than meaning or truth, which may result in incorrect or misleading translation results. In sensitive contexts, human expertise is necessary to ensure accuracy and trust. This makes qualified translators essential for projects requiring nuance and data protection.²²

²⁰Available at <https://rm.coe.int/cepej-2025-18final-en-draft-guidelines-on-the-use-of-generative-ai-for/48802a4ad1>.

²¹ *Artificial intelligence in judicial systems: promises and pitfalls*, UN Report of 16 July 2025, A/80/169, p. 13.

²² AI for Translation and Interpreting. A Roadmap for Users and Policy Makers, Conseil Européen pour les Langues/European Language Council, October 2025, doi: 10.5281/zenodo.17531283.

26. The year 2025 has been a period of significant development for AI regulation in the justice sector, with the EU AI Act's phased entry into application beginning to shape the landscape of technological deployment within courts, aligning with the broader principles of the Framework Convention.

1. The impact of EU AI Act on court practice

27. The phased application of the EU AI Act began in 2025 with the provisions concerning prohibited AI practices and AI literacy obligations entering into force on 2 February 2025. Specifically, the prohibition on use of crime prediction systems became effective, setting a clear, mandatory standard for Europe.

28. The rules governing General-Purpose AI (GPAI) / LLMs became applicable on 2 August 2025. These obligations require providers of generative AI tools used by the courts to produce technical documentation, ensure transparency about the data used for training, and comply with copyright law. The European Commission issued guidelines to clarify the scope of these obligations, which complement the voluntary General-Purpose AI Code of Practice.²³ These provisions are in line with the CEPEJ Guidelines on the use of generative artificial intelligence for the courts,²⁴ which calls for the transparent, verified, and cautious use of LLMs in the judicial context.

29. The AI Act's new governance and enforcement architecture became applicable in August 2025. This included the formal establishment of the European AI Office,²⁵ the designation of national competent authorities responsible for supervision and enforcement,²⁶ and the framework for penalties for non-compliance. This framework for enforcement is aligned with the Framework Convention's reliance on national measures to achieve its goals.

30. For courts and other judicial authorities, a critical date will be December 2027, when the main obligations for high-risk AI systems are set to apply, following the amendments introduced by the Digital Omnibus on AI (pending publication in the Official Journal).²⁷ Annex III of the AI Act explicitly classifies as high-risk those *"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"*. Institutions should prepare themselves for these obligations, as implementing an AI system that will be non-compliant poses a financial and operational risk.

31. The AI Act mandates that deployers of high-risk AI systems must perform a Fundamental Rights Impact Assessment (FRIA) prior to deployment (Art. 27). This compulsory assessment serves as a key human rights safeguard. This requirement runs parallel to, and should be coordinated with, the Council of Europe's efforts, such as the HUDERIA (Human Rights, Democracy, and the Rule of Law Impact Assessment) Methodology,²⁸ which provides a comprehensive framework tailored to assess and mitigate risks to human rights, democracy, and the rule of law across the AI lifecycle.

²³ Available at <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>.

²⁴ See note 19 above.

²⁵ Available at <https://digital-strategy.ec.europa.eu/en/policies/ai-office>.

²⁶ Available at <https://digital-strategy.ec.europa.eu/en/policies/fundamental-rights-protection-authorities-ai-act>.

²⁷ Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)

²⁸ Available at <https://www.coe.int/en/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems>.

2. Cybersecurity in courts

32. Cybersecurity is an increasingly critical concern for judicial authorities, encompassing a wide array of technical safeguards for IT security, safe cloud computing, the integrity and privacy of judicial data (see the International Cybersecurity Challenge (ICC) initiatives).²⁹ For instance, in 2025, a massive cyberattack struck the U.S. federal court system, leveraging a critical vulnerability to gain access.³⁰ The worldwide adoption of AI tools in the courts amplifies these concerns.³¹ The principles governing this field are consistently recalled in Council of Europe documents, such as the Guidelines of the Committee of Ministers of the Council of Europe on online dispute resolution mechanisms in civil and administrative court proceedings,³² which define and stress the importance of maintaining the security of network and information systems.

33. The EU AI Act integrates cybersecurity as an essential requirement for the trustworthiness and safety of high-risk AI systems, such as the ones used for administration of justice. Article 15 of the AI Act mandates that high-risk AI systems, including those used by judicial authorities, must be designed and developed to achieve an appropriate level of accuracy, robustness, and cybersecurity throughout their lifecycle. This fully aligns with the Framework Convention that promotes principles of reliability, safety, and trust.

34. To implement AI safely within the justice system, the relevant judicial authorities could adopt a Zero Trust Architecture,³³ a cybersecurity approach based on the idea that trust should never be granted implicitly but rather must be continually evaluated. Rather than assuming anyone inside the network is safe, this approach requires every user and device to be explicitly verified before they are granted access to case files or judicial data. It is also important to recognise that security is a shared responsibility between the courts (the deployers) and the AI providers, and that both parties must maintain specific safeguards.

35. Recent trends show growing attention to sovereignty in language and data processing. LLMs like Apertus (Switzerland) and Bielik Instruct (Poland), the latter trained on Polish-language and locally governed data, exemplify a European shift towards AI sovereignty. These models aim to ensure linguistic accuracy, legal contextualization, and compliance with domestic governance standards. Similar efforts across Europe reflect a growing intention to avoid dependence on global commercial models. Sovereign models trained on legally validated corpora (court rulings, statutes, doctrinal texts) support compliance with new legal frameworks and can serve as exemplars for responsible AI deployment in the judiciary.

²⁹ Available at <https://www.enisa.europa.eu>.

³⁰ *Russia Is Suspected to Be Behind Breach of Federal Court Filing System*, The New York Times, Aug. 12, 2025, <https://www.nytimes.com/2025/08/12/us/politics/russia-hack-federal-court-system.html>.

³¹ See further *Legal accountability for malicious cyber operations. Policy Brief*, Oxford Institute of Technology and Justice 2025, <https://www.techandjustice.bsg.ox.ac.uk/insights/legal-accountability-malicious-cyber-operations>, pp. 20 - 21.

³² Available at <https://www.coe.int/en/web/cdcj/online-dispute-resolution-mechanisms> and <https://rm.coe.int/dispute-resolution-en/1680b2ca19>.

³³ Available at <https://csrc.nist.gov/Pubs/sp/800/207/Final>.