

Brussels, 24 March 2025
(OR. en)

7418/25

LIMITE

EJUSTICE 17
JURINFO 4
FREMP 68
COPEN 66

NOTE

From: General Secretariat of the Council
To: Delegations
Subject: Digitalisation of justice and fundamental rights challenges

Delegations will find in Annex a document on digitalisation of justice and fundamental rights challenges, which will serve as a basis for the discussions during the meeting of the e-Justice Working Party on 28 March 2025.

Digitalisation of justice and fundamental rights challenges

I. INTRODUCTION

The digitalisation of justice, particularly the integration of Artificial Intelligence (AI) and the growing use of videoconferencing for hearings, presents various challenges to the effective exercise of individuals' fundamental rights.. However, digitalisation also offers significant benefits, such as improving access to justice and ensuring that judicial hearings are conducted within a reasonable time. Access to justice can be strengthened through the judicious and efficient use of digital tools in the justice system, provided appropriate safeguards are in place.

In civil law, the Digitalisation Regulation ((EU) 2023/2844), once implemented, will significantly enhance the fundamental right of access to justice. By establishing the European Electronic Access Point, it will enable individuals or companies to file claims electronically in cross-border cases, removing current practical barriers that particularly hinder consumers from exercising their right to justice. The Regulation also provides a legal basis for the participation of parties in hearings via videoconferencing.

In criminal law, the Digitalisation Regulation allows for videoconferencing in a limited number of cross-border situations within the execution of mutual recognition instruments. While in-person attendance is preferable to ensure a fair process, allowing participation by videoconference offers several benefits, such as preventing trial delays, avoid trials in absentia, and reducing the needs for intrusive measures like issuing a European Arrest Warrant. The report of the 10th round of Mutual Evaluations on the European Investigation Order has recommended that the Commission address the issue of the accused's participation in trials via videoconference from another Member State. The Commission is currently working on this matter.

The right to a fair and public hearing within a reasonable time largely depends on the efficiency of national court systems. Digital tools, including AI-based tools, could significantly enhance this efficiency by supporting justice professionals in their work. Compliance with the AI Act ensures that AI tools respect fundamental rights, notably through mandatory Fundamental Rights Impact Assessments for high-risk systems. Therefore, the use of AI-based tools should be encouraged in the justice sector, provided they adhere to regulatory standards and only assist rather than replace, judicial decision-making. The final decision must remain human-driven. Additionally, EU data protection laws protect individuals from decisions with legal effects solely based on automated processing. However, it's important to recognize that not everyone has equal access to reliable internet or digital tools. Certain groups, including older individuals, persons with disabilities, and those from disadvantaged social or economic backgrounds, may face challenges due to limited digital literacy or lack of appropriate infrastructure.

The use of videoconferencing in criminal proceedings raises questions about whether the existing EU acquis on procedural safeguards for suspects and accused persons is adequate to ensure the necessary protection in this context. It also prompts the need to consider whether additional specific measures are required to fully safeguard the right to a fair trial and the rights of defence.

These issues have been addressed by the Council on various occasions and prepared, sometimes by the e-Justice Working Party, sometimes by the Working Party on Fundamental Rights (FREMP):

- The **Council Conclusions of 9 June 2020** highlighted the challenges posed by digitalisation, including AI's role in society and the economy¹.
- The **Council Conclusions of 13 October 2020** focused on how digitalisation can enhance the effectiveness of justice systems².

¹ Council conclusions on shaping Europe's digital future, 2020/C 202 I/01, OJ C 202I, 16.6.2020, p. 1-12

² Council Conclusions 'Access to justice – seizing the opportunities of digitalisation' 2020/C 342 I/01, OJ C 342I, 14.10.2020, p. 1-7

- The **Council Conclusions of 20 October 2023** emphasized digital empowerment in protecting fundamental rights, particularly within sectors like justice, while fostering a safe digital environment³.
- In its **Conclusions of 5 March 2024**, the Council urged the Commission to incorporate a fundamental rights perspective in all EU actions related to legal protection and access to justice, including leveraging digitalisation opportunities⁴.
- In its **Report on the 10th Round of Mutual Evaluations on the European Investigation Order of December 2024**, the Commission is invited to, upon due assessment of the findings of this report and after identifying the most appropriate legal instrument, address at legislative level the question of the participation of the accused person in the trial via videoconference from another Member State⁵.
- At its **December 2024 meeting**, the Council (Justice and Home Affairs) approved conclusions on AI's role in the justice sector⁶.
- In its **Conclusions of 7 March 2025**, the Council commended the wide range of areas in which Union funding has contributed to protecting and enforcing fundamental rights, including providing access to justice through digital means, as well as creating secure and safe online environments⁷.

The **Fundamental Rights Agency (FRA)** has published reports on AI and fundamental rights, including "Getting the Future Right: Artificial Intelligence and Fundamental Rights"⁸ and "Bias in Algorithms - AI and Discrimination"⁹.

³ 14309/23

⁴ 7127/24

⁵ 15834/1/24 REV 1

⁶ 16933/24

⁷ 6878/25

⁸ <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights>

⁹ <https://fra.europa.eu/en/publication/2022/bias-algorithm>

FRA is currently working towards a guidance on fundamental rights-compliant ‘digital justice’.

During the meeting of the e-Justice Working Party scheduled for 28 March 2025, where the delegates of the FREMP Working Party will be convened, FRA will present its work on artificial intelligence and fundamental rights based on the above mentioned reports

FRA will also present key considerations regarding high-risk artificial intelligence in the Artificial Intelligence Act from the perspective of fundamental rights and will share some preliminary reflections based on the ongoing projects concerning the assessment of high-risk artificial intelligence.

Other international institutions have provided relevant insights, such as:

- **The Council of Europe's** the European Ethical Charter on the use of AI in judicial systems and their environment¹⁰,
- **The Organisation for Economic Co-operation and Development (OECD)'s** recommendations on AI¹¹,
- **The UN Human Rights Council Resolution (10 July 2024)** on human rights and the independence of the judiciary¹²,
- **The Council of Europe's** Framework Convention on AI and Human Rights, Democracy and the Rule of Law AI¹³, and
- **The UN High-level Advisory Body's** Final Report on governing AI for humanity¹⁴.

¹⁰ <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>

¹¹ <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

¹² <https://documents.un.org/doc/undoc/gen/g24/120/36/pdf/g2412036.pdf>

¹³ Council of Europe Treaty Series - No. [225], [Vilnius, 5.IX.2024]

¹⁴ https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf

II. CHALLENGES POSED BY THE DIGITALISATION OF JUSTICE, THE USE OF AI IN THE JUDICIARY, AND VIDEOCONFERENCING FOR HEARINGS

The digitalisation of justice, the use of AI in justice and of videoconferencing in hearings may present some challenges to fundamental rights within the EU, particularly concerning access to justice, fairness, privacy, transparency, and equality. However, existing EU legal frameworks, notably the AI Act and the Digitalisation Regulation, provide safeguards to address these concerns, ensuring that digital tools enhance rather than compromise justice. These regulations aim to achieve two key objectives: improving the efficiency of justice while safeguarding fundamental rights.

1. Access to Justice

- **Digital divide:** not all individuals have equal access to digital tools, which risks excluding vulnerable groups, such as the elderly, people with disabilities, and those in rural areas, from the justice system.
- **Disparities in access to legal information:** people who are unfamiliar with digital platforms may struggle to access legal information, leading to unequal access to justice. However, AI can serve as a supplementary tool to existing legal information systems. By offering greater transparency in legal processes and providing user-friendly guidance, AI can enhance access to justice and ensure legal information is more accessible to those who need it.

2. Fair Trial

- **AI transparency:** when AI is used in supporting decision-making, the lack of transparency in how decisions are made can compromise fairness and individuals' rights of defence. Defendants may be unable to challenge AI-generated components of decisions, including parts of the reasoning. The AI Act (Article 86) ensures that affected persons have the right to receive clear explanations from deployers on AI-assisted decisions that significantly impact their rights, health, safety, or fundamental rights, including in judicial matters.

- **Risk of bias:** AI can perpetuate existing biases, leading to discriminatory outcomes, especially if trained on biased data sets. To prevent this, high-risk AI systems must meet specific requirements before being introduced to the market. In addition, the AI Act places particular emphasis on mitigating possible biases in data sets that could negatively impact fundamental rights or result in discrimination.
- **Decision-making assisted by AI:** overreliance on AI in legal decision-making could undermine impartiality if human judgment is sidelined. However concerns about AI replacing human judges are addressed in the AI Act which allows AI tools to support the judiciary but not replace judges' decision-making power. According to the AI Act, the final decision-making must remain a human-driven and this must be reflected in the conditions AI assisted judges. The decision to use AI in judicial processes is ultimately left to the judiciary itself, but it is crucial for legal professionals to be aware of the potential risks of over-reliance and partiality . To mitigate these risks, measures such as increasing AI literacy and providing judicial training are essential. The AI Act (Art. 4) mandates that providers and deployers of AI systems, including judicial administrations, take steps to ensure their staff has sufficient AI literacy. This includes considering the technical knowledge, experience, education, and training of individuals, as well as the context in which AI systems will be used and the groups of people affected by them.
- **Correlational errors:** AI may find correlations that are difficult to detect and challenge and/or that could result in unjust legal outcomes. To mitigate this risk, the AI Act imposes stringent requirements on dataset quality, human oversight, and explainability. These measures ensure that AI-generated correlations are subject to critical assessment and can be contested when necessary.

3. Lack of transparency and accountability

- **Opaque decision-making:** complex algorithms can reduce transparency, eroding trust in the justice system and undermining the perception of human-driven decisions. To address this, the AI Act requires deployers of high-risk AI systems used in judicial processes to provide clear, meaningful explanations of their decision-making (Article 86), ensuring transparency and enabling individuals to challenge AI-assisted outcomes. Additionally, high-risk systems must meet transparency standards.
- **Accountability gaps:** it is unclear who is responsible when AI systems make errors or discriminatory decisions, potentially harming individuals and eroding trust in the judiciary. EU legislation on AI, including the AI Act and the revised Product Liability Directive, emphasizes that a human is always accountable for AI actions. Furthermore, the AI Act ensures that AI-assisted decisions do not replace human judgment, keeping responsibility with the adjudicator. Finally, individuals retain the right to challenge decisions through established legal procedures.

4. Erosion of Human Agency

- **Overreliance on AI:** excessive dependence on AI for decision-making may lead to unquestioning acceptance of recommendations, potentially undermining fairness and integrity, and disqualifying the decision as human driven. This could also jeopardize the data subject's right not to be subject to a detrimental or legal decision based solely on automated processing. As noted earlier, the risk of over-relying on AI is addressed in the AI Act, particularly through the general AI literacy obligation (Art. 4) and human oversight requirements for high-risk AI providers and deployers. Judicial training on AI use in justice can help mitigate this risk. The Council conclusions on the use of AI in justice, adopted last December, emphasise the importance of judicial training in this area. Furthermore, the conditions for AI system use are determined by national legislators, who must consider the independence of the justice system.

- **Dehumanisation of justice:** relying on AI for decisions affecting individuals' lives may diminish the perception of human involvement in justice. However, the AI Act's principles ensure that AI does not replace judicial decision-making and that the final decision remains human-driven. Existing procedural guarantees further ensure that human judges retain decision-making authority, preserving the human aspect of judicial processes.

5. Right to privacy and data protection

- **Privacy risks in videoconferencing:** There are concerns about personal data protection when using videoconferencing tools from third-party providers, especially when it's unclear whether the tools comply with data protection requirements. Issues may include uncertainty about the data controller, storage locations and duration, who can access the data, and what data is collected and how. To address these concerns, the Digitalisation Regulation (Recital 32) clarifies that videoconferencing technology must meet applicable standards for personal data protection..
- **Virtual hearings potentially exposing sensitive personal data:** in virtual hearings, there is a risk that sensitive personal information, such as like private details shared during the session, could be exposed if proper security measures are implemented. Without security precautions like encryption, secure login and other safeguards, unauthorised individuals may gain access to personal data. The importance of robust security measures is emphasised in Recital 32 of the Digitalisation Regulation. Additionally, under the decentralised IT system it establishes, Article 3(3) and Article 14 ensure that information exchange complies with data protection standards, maintains the confidentiality of communications and upholds data security. These considerations are also crucial when using videoconferencing technology.

- **Technical vulnerabilities potentially compromising the integrity of hearings:** videoconferencing platforms may have vulnerabilities, such as software bugs or flaws, that could be exploited by hackers or malicious actors. These weaknesses could undermine the fairness, security, or accuracy of the hearing itself, and compromise procedural safeguards like lawyer-client confidentiality, potentially allowing outside influence or manipulation. Recitals 32 and 46, along with Article 6(5) of the Digitalisation Regulation, mandate that videoconferencing and other distance communication technologies meet applicable standards for communications confidentiality and data security, regardless of the type of hearing, ensuring the confidentiality of communications between a suspect, an accused or convicted person or an affected person and their lawyer.
- **Data security:** AI tools used in the judiciary process large volumes of personal data, raising concerns about compliance with the EU data protection laws. The AI Act requires that privacy and data protection rights are guaranteed throughout the entire lifecycle of the AI system, ensuring compliance with relevant EU legislation.

6. Equality before the law

- **Inequality of access:** the digital divide may exclude individuals without access to adequate connectivity, technology or digital skills, undermining the principle of equality before the law. For affected individuals, videoconferencing could make it more difficult for defendants, witnesses or victims to fully participate in proceedings, weakening the right to a fair trial. However, digitalisation has the potential to strengthen the fundamental rights, including access to justice and, the right to an effective remedy, and the right to a fair and public hearing within a reasonable time, through the smart and efficient use of digital tools. At the same time, allowing parties to attend hearings via videoconferencing offers benefits for individuals living in other Member States, rural areas, or for those with disabilities who may find it challenging to attend court hearings in person. Authorities should ensure access to the necessary infrastructure for using videoconferencing (as highlighted in Recitals 38 and 47 Digitalisation Regulation).

7. Right to an oral hearing

- **Remote hearings vs. physical presence:** videoconferencing can pose challenges to the right to a fair trial and the effective exercise of the rights of defence, such as limiting communication effectiveness and the ability to read body language. However, participation via videoconferencing can facilitate access to justice, and support the right to be present at trial, provided that necessary procedural safeguards are in place to adapt to the digital environment. Therefore, videoconferencing hearings must include appropriate safeguards and clear procedural rules to ensure they closely replicate the fairness and experience of in-person hearings.
- **Impersonal proceedings:** virtual hearings may lack the personal interaction of in-person hearings, potentially affecting the perception of justice. However, videoconferencing can reduce the number of in absentia trials and facilitate the participation of victims of crime, or vulnerable witnesses, by providing a safe-space, avoiding direct interaction with the suspect or accused person. Article 23 of the Victims' Rights Directive acknowledges this need and makes videoconferencing an option to address it.

8. Public trust in the judiciary

- **Perception of AI in courtrooms:** if AI is perceived as replacing or overly influencing human judgment, it could undermine public trust in the judicial system, particularly if AI decisions are opaque or biased. To address this, it is important to ensure the proper and consistent implementation of the AI Act. To support this, the European Commission is offering guidance and a comprehensive set of measures to promote the transparent and responsible use of AI, thereby reinforcing judicial integrity and preserving public confidence in the justice system.

The digitalisation of justice, the use of AI in justice, and videoconferencing for hearings present both complex challenges and significant benefits for fundamental rights in the EU. It is crucial to continue ensuring that the EU framework effectively balances these challenges and benefits.

III. DISCUSSION OF E-JUSTICE AND FREMP DELEGATES WITH THE FUNDAMENTAL RIGHTS AGENCY

Delegations are invited to reflect and express their opinion on:

- How can the EU framework ensure the efficiency of justice through digitalisation, the use of AI, and videoconferencing, while also enhancing fundamental rights?
 - What support would be necessary at the EU level to ensure these objectives are effectively achieved within national judicial systems?
 - Which tasks should remain the responsibility of humans when integrating AI-based tools in the field of justice?
-