Position on the Digitalisation of Justice
European Criminal Bar Association

The ECBA

The European Criminal Bar Association ('ECBA') was founded in 1997 and is an association of independent specialist defence lawyers across Europe, representing the views of defence lawyers and promoting the administration of justice and human rights under the rule of law in Europe and among the peoples of the world.

The ECBA is one of the main interlocutors of the European institutions on issues of criminal justice and the protection of the right of defence and fundamental rights, representing thousands of legal practitioners all around Europe through their direct affiliation to the Association as individual members, or through the Collective members that participate to the life of the Association.

The ECBA acknowledges the growing role of technology in criminal law and criminal procedure, the current digitalisation of justice and the many other rapid developments in this domain, e.g. the rise of AI, digital evidence, the role of encryption in communication and financial flows and the use of video connections in court procedures or for remote communication. These developments must comply with the right to privacy and non-discrimination, procedural safeguards and must have sufficient effective legal remedies. Due to the rapid development in the technical field, the ECBA also considers it important that lawyers have knowledge in this area and that our members can exchange experiences from the various Member States and learn from them.

This has led to the ECBA setting up a working group that focuses on the entire digital aspect within criminal law and criminal procedure.

Digitalisation of justice as a tool for a fair trial

The ECBA recognizes the significant potential of digital tools, including artificial intelligence (AI), to enhance the efficiency and effectiveness of justice systems across Europe, understood as the capacity to put in place fair proceedings.

The ECBA emphasizes that transparency, accountability, equality of arms and access to justice are key elements necessary to achieve a balance between digitalisation and the protection of fundamental rights, including the rights of defence, to a fair trial, privacy and non-discrimination.

At this stage, the ECBA would like to reiterate its Statement of Principles on the use of videoconferencing in criminal cases in a Post Covid-19 World,[1] and to outline its position on certain further core aspects of the digitalisation of justice.

In respect of the use of videoconferencing we refer for the detail to our Statement, which we attach for ease of reading ('Enclosure 1'), as well as to the preliminary results of an ongoing consultation of practitioners on the use of videoconferencing in criminal proceedings, which we summarise in the attached document ('Enclosure 2').

1. Potential Gains and Associated Concerns

The ECBA acknowledges that the integration of digital tools and AI in the justice system has the potential to improve efficiency, the protection of individuals' rights and fairness of proceedings in several ways:

- Automating routine administrative tasks, allowing legal professionals to focus on complex legal issues;
- Enhancing case management and scheduling processes;
- Improving document analysis and e-discovery capabilities;
- Providing predictive analytics for case outcomes and resource allocation,[2]
- Allowing for AI-assisted legal research;
- Facilitating and advancing the exercise of defence rights, both in domestic and cross-border settings.

However, the ECBA strongly cautions against pursuing efficiency at the expense of the quality and fairness of criminal proceedings. The human component in criminal justice, including the nuanced assessment of the evidence and the individual circumstances of the accused and the case, must remain paramount.[3]

The ECBA is particularly concerned about the risk of dehumanizing criminal justice through over-reliance on technology.

On this matter, a perspective that is both acceptable and in tune with technological development could be allowing the use of AI models merely as a support to the judge, whose assessment must remain central, in order to mitigate the imperfection of judicial decision-making in a setting where equitable justice must continue to prevail exact justice.

The ECBA is also concerned about the potential use of AI models for crime prediction (due to algorithmic bias), sentencing or parole (black box issues), and digital forensics that rely on large datasets without access to the raw data or the ability to evaluate the AI model's methodology.

The use of AI models in criminal trials should be transparent, and adequate procedural safeguards must be established to mitigate the potential risks of misuse.

2. Measures to Promote Digitalisation While Mitigating Risks

To promote responsible digitalisation of justice, we recommend the following measures:

- Develop clear, understandable ethical guidelines for the use of AI in legal decision-making, based on international standards;[4]
- Ensure transparency in AI algorithms used in the justice system, with regular independent third-party audits to prevent bias and errors;[5]
- Maintain human oversight and the right to appeal AI-assisted decisions;[6]
- Provide clarity on whether a (part of a) decision is AI generated;
- Limit the use of AI for judicial acts with a need for human validation such as the evaluation of the facts as well as the act of sentencing, preserving the essential human component of judgments;
- Implement strict data protection and privacy measures, with particular attention to safeguarding lawyer-client privileged information;[7]
- Establish a regulatory framework for the development and use of legal tech, with input from legal professionals, safeguarding the principle of technological neutrality of the legislation;[8]
- Ensure that the implementation of digital tools does not compromise the presumption of innocence or other fair trial rights and the principle of non-discrimination;[9]
- Create digital literacy programs for all stakeholders in the justice system;
- Develop contingency plans for system failures or cyber-attacks.[10]

There is already a substantial body of literature regarding the potential biases associated with AI models used in criminal proceedings[1112]. AI models are trained using specific datasets that often contain embedded discriminatory practices, racial profiling, or unbalanced representations of various social groups.[13] As a result, using such datasets to train AI models can perpetuate these biases, raising serious concerns about fairness and equality in criminal justice. Moreover, flaws in the design of the algorithms themselves can introduce bias, even when the dataset has been properly balanced to mitigate such risks.

Without knowing the exact dataset used to train an AI model (in accordance with the principle of transparency), it is impossible to assess the degree of bias risk. The problem is compounded when AI models operate as "black boxes," where the internal decision-making process remains opaque. While inputs and outputs may be clear, how the AI generates its results is often inscrutable, especially in the case of deep learning models.[1415] Unlike more transparent models, such as decision trees, where reasoning can be traced, black-box models obscure the rationale behind their conclusions. This lack of transparency undermines the ability to scrutinize AI-generated conclusions, which is a fundamental right under Article 6 of the European Convention on Human Rights (ECHR):

- Effective cross-examination becomes nearly impossible when the underlying decision-making process of the AI cannot be questioned;
- It makes appeals particularly challenging when decisions cannot be properly scrutinized.

This is precisely why we believe that the use of AI models in criminal proceedings must be subject to strict regulation and guided by robust ethical standards. In particular, AI should be heavily scrutinized in areas such as predictive policing, sentencing, and risk assessment related to preventive measures or parole. The use of AI in these contexts not only risks perpetuating bias but also threatens the erosion of the role of human oversight and evaluation, which is critical to individualized justice.

We argue that, in principle, AI should assist but never replace the deliberative process of judges. This conclusion aligns with Article 11 of Directive (EU) 2016/680, which prohibits solely automated decisions that produce adverse legal effects, unless authorised by law with appropriate safeguards, including human intervention. Nonetheless, robust auditing and transparency measures are essential to prevent circumvention of these legal protections. We also believe that the following regulatory framework should apply for the use of AI in criminal proceedings:

- Regular auditing of AI systems for bias and accuracy;

- Clear documentation requirements for training data sources and model architecture;
- Establishment of minimum explainability standards for AI used in criminal proceedings;
- Regular reassessment of AI systems' performance with new data;
- Regular retraining of AI models to account for changing social conditions.

Furthermore, we recognize that AI tools are already widely integrated into digital forensics,[16] evidence collection, and intelligence gathering, including OSINT (open-source intelligence) tools. AI's role in these areas should be carefully regulated. For example, tools such as Chainalysis Reactor, which trace cryptocurrency transactions, or image recognition software used in digital forensics, must be scrutinized to ensure their results meet the evidentiary standards required in criminal proceedings. The risks are particularly acute when the sources of information cannot be accurately identified, or when the data collection methods (e.g., scraping, accessing public or private APIs) are unclear. Without a clear chain of custody or transparency in data interpretation, the results of such AI-driven analyses could undermine the right to a defence.

Importantly, the results of digital forensics tools using AI should not be viewed as definitive conclusions but rather as "recommendations" that must be subject to human oversight [37]. Courts must be vigilant in assessing whether AI-generated evidence meets the necessary standards of admissibility and reliability before such evidence is admitted in proceedings. There should be a strong consensus that automated data collection and AI-driven interpretations pose significant risks unless properly regulated.

Lastly, the principle of proportionality must be central to any discussion on the use of AI in criminal investigations. Under Article 8 of the ECHR, any interference with the right to privacy must be necessary and proportionate to the legitimate aim pursued. The deployment of AI in investigative tools that verge on mass surveillance, for example, must be carefully evaluated. In cases where AI's use constitutes a significant intrusion into privacy, it should be reconsidered and limited to circumstances where a court order has been obtained. This ensures compliance with the proportionality requirements and safeguards individuals' fundamental rights.

In conclusion, while AI has the potential to enhance the efficiency and accuracy of certain aspects of criminal justice, it must be used with caution. A balanced and regulated approach, grounded in transparency, ethical guidelines, and respect for human rights, is essential to prevent AI from becoming a tool that exacerbates existing injustices rather than alleviating them.

3 Infrastructure and Skills Needs

To effectively implement digital justice while ensuring fair proceedings, we identify the following key needs:

- Robust and secure IT infrastructure for Courts, including high-speed internet connections and protected cloud-based systems that ensure the confidentiality and integrity of sensitive legal data;[17][18]
- Hybrid systems for filing documents, ensuring that physical files remain an option to avoid hindering access to justice;
- Free access to e-filing platforms and case management software and free download of the files for parties and their lawyers as a consequence of the dematerialisation of the files, to ensure the effectiveness of the defendant's rights to have adequate facilities for the preparation of the defence and access to justice. This should also apply for a defendant that is detained;
- User-friendly and disability-friendly case management software and e-filing systems that are interoperable across different jurisdictions;[19]
- AI-powered legal research tools and document analysis software to assist, not replace, legal professionals;[20]
- The defence should have access to the raw data and should have access to the same investigative mechanisms/programs as the investigative team to search in (mass) data to guarantee the equality of arms;
- Secure video-conferencing platforms for remote (court) hearings and client meetings, also including (cross-border) meetings from detention facilities and prisons, with technical and legal safeguards to protect attorney-client privilege.[21] End-to-end encryption should be regarded as a fundamental safeguard for protecting attorney-client privilege;
- Remote court hearings should comply with an appropriate and compatible technical infrastructure and solutions which allow for true-to-life remote participation as mentioned in the Statement of Principles on the use of videoconferencing in criminal cases in a Post Covid-19 World, September 6, 2020, section D;
- Comprehensive digital skills training programs for all legal professionals, including judges, prosecutors, and defence lawyers;[22]
- Advanced cybersecurity measures to protect against data breaches and unauthorized access;[23]

- High-end audio and visual documentation systems for interrogations and court proceedings;

- Schemes to allow sole practitioners, small and medium law firms and lawyers working under legal aid schemes to have access to the available technological tools in order to ensure fair competition, the provision of quality legal services to all persons and companies, and the fairness of proceedings.

We emphasize the need for these tools to be reliable, up-to-date, and accompanied by proper training for all users to ensure effective implementation.

4. Measures to promote Digitalisation as a means of facilitating and advancing defence rights

New technologies can also be used as a means to facilitate the exercise of the rights of the defence and to improve the reliability of evidence and the ability of the defence to challenge evidence in the collection of which he has not participated:[24]

- The use of videoconferencing technologies could be encouraged as a means for suspected or accused persons to participate in procedural acts[25] at their request, in particular in cross-border cases. A two-fold distinction must be made between: a) the use of remote hearings in domestic and in cross-border cases; and b) the use of remote technology for conducting interviews of the suspect or accused person in the pre-trial stages of proceedings and its use for the trial hearings. This is because the seriousness of the interference with the fair trial rights and the rights of defence of the suspect or accused person in each situation differs, as do the circumstances that must be weighed in order to assess whether such restrictions are proportionate, adequate and necessary;

- Issuing a European Arrest Warrant to bring a person to an arraignment or trial hearing, where their physical presence is not necessary but the law still requires it, should be avoided, and the use of video-conferencing technologies should be promoted to allow remote hearings in these cases (as well as during EAW proceedings, where the issuing of a EAW was considered necessary at the outset, but the hearing of the person during the EAW proceedings may lead to withdrawing the EAW and imposing less restrictive measures), in particular where it can avoid or replace detention or where a trial would otherwise be held in the person's absence.[26] This is particularly important in cases of low and medium level offences;

- No accused person should be prevented from attending his or her own trial in person, if they wish to do so, no matter how serious the offence of which they are accused. The more serious

the offence, the more important is the need to ensure that the person is physically present, given the fact that, for example, because justice imposed by means of a remote trial is not the equivalent of an in-person trial;

- The use of modern communication technologies to facilitate dual defence and defence in cross-border cases should be explored;

- Audiovisual recording of police interrogations should be mandatory, as it would contribute to the prevention of ill-treatment, to document the information on rights and duties provided to the person, the accuracy of the recording of the statements and a better assessment of their relevance and reliability;

- Audiovisual recording at the trial and appeal stages should also be considered, as it could strengthen the rights of the defence by providing an accurate record of the proceedings and the evidence and it also promotes open and transparent justice, and increases trust of and respect for the criminal justice system amongst the wider population;

- There should be a provision for ensuring electronic access to the case files for the suspect or the accused person and their lawyers, including where an accused person is in detention.

5. EU-Level Action to Promote Digitalisation

We believe the EU can play a crucial role in promoting the responsible digitalisation of justice through the following actions:

- Provide funding for national efforts to modernize court infrastructure and develop legal tech solutions;
- Develop EU-wide guidelines for the ethical use of AI in justice, with clear limits on its application;[27]
- Create technical standards for video-conferencing and e-filing systems to ensure interoperability and security across member states;[28]
- Establish procedural requirements for digital evidence handling and the protection of privileged information;[29]
-

- Foster the use of the e-CODEX system for seamless cross-border legal cooperation in order to create a common interoperating digital justice infrastructure;[30]
- Develop a standardized EU-wide e-signature system for legal documents;

- Leaving as a subsidiary tool for exchanging legal documents a common system of Registered Electronic Email;
- Facilitate knowledge sharing and best practices among Member States;
- Create an EU-wide platform for legal tech innovation and collaboration;
- Establish a central repository for EU and national case law and legal resources. As regards national case law, an automated translation should at least be available;
- Ensure that cross-border digital justice initiatives respect the procedural rights of suspects and accused persons;[31]
- Develop appropriate and compatible technical infrastructure and solutions which allow for true-to-life remote participation and the exercise of procedural rights by means of remote technologies in criminal cases[32];
- Explore ways to use digitalisation to promote and facilitate the exercise of defence rights, in particular in cross-border cases;
- Establish a right of the accused to be heard by video-conferencing in cross-border cases, in particular where this can avoid the issuing of a European Arrest Warrant (or lead to an EAW being withdrawn) or the conduction of trials in absentia.

In conclusion, the ECBA supports the responsible digitalisation of justice, with a focus on enhancing efficiency while safeguarding fundamental rights and the integrity and fairness of criminal proceedings. We call for a balanced approach that leverages technology to improve the administration of justice while preserving the essential human elements of legal decision-making. As the digitalisation of justice progresses, we urge ongoing consultation with legal professionals to ensure that technological advancements serve the interests of justice and protect the rights of all individuals involved in the criminal justice system.

November 1, 2024

ECBA Cyber & AI Working Group:

Gwen Jansen - de Wolf (Chair)
Adrian Sandru
Alexis Anagnostakis
Amedeo Barletta

Federico Cappelletti
George Zlati
Marie Poirot
Vânia Costa Ramos

We want to thank our following ECBA colleagues for their input:

Andreu Van den Eynde Adroer
Ángela Díaz-Bastien
Giovanni Flora
Jakoline Winkels
Judy Krieg
Julian Hayes
Luxembourg Association of Criminal Lawyers (ALAP) - collective member
Nikolai Venn

[1] See ECBA Statement of Principles on the use of video-conferencing in criminal cases in a Post Covid-19 World, September 6, 2020, https://www.ecba.org/extdocserv/20200906_ECBAStatement_videolink.pdf.
See ECBA Statement of Principles on the use of video-conferencing in criminal cases in a Post Covid-19 World, September 6, 2020, https://www.ecba.org/extdocserv/20200906_ECBAStatement_videolink.pdf.
-criminal-proceedings-was-published/?), which highlights the increasing prevalence of electronic evidence in criminal proceedings.

[3] This is reflected in the INNOCENT toolkit, p. 74, which stresses the importance of human oversight in electronic evidence handling.

[4] The INNOCENT toolkit, p. 74, also calls for clear guidelines on the use of AI in criminal justice.

[5] . The INNOCENT toolkit, p. 94, emphasizes the need for transparency and auditing of AI systems used in criminal justice.

[6] The INNOCENT toolkit, p. 75, stresses the importance of human oversight in AI-assisted decision-making.

[7] The INNOCENT toolkit, p. 81, also discusses the importance of protecting privileged information in electronic evidence.

[8] Supported by the INNOCENT toolkit, p. 63, which calls for a common legal framework for handling electronic evidence.

[9] INNOCENT toolkit, p. 47, emphasizing the importance of the presumption of innocence in the context of electronic evidence.

[10] Supported by the INNOCENT toolkit, p. 70, which discusses the need for contingency plans in electronic evidence handling.

[11] Arowosegbe, J. (2023). Data bias, intelligent systems and criminal justice outcomes. *Int. J. Law Inf. Technol.*, 31, 22-45. https://doi.org/10.1093/ijlit/eaad017.

[12] Gravett, W. (2021). Sentenced by an algorithm — Bias and lack of accuracy in risk-assessment software in the United States criminal justice system. *South African journal of criminal justice*, 34, 31-54. https://doi.org/10.47348/SACJ/V34/I1A2.

[13]] Barrett, L. (2017). Reasonably suspicious algorithms: Predictive policing at the United States border. *NYU Rev. L. & Soc. Change*, *41*, 327.

[14] Asatiani, A., Malo, P., Nagbøl, P., Penttinen, E., Rinta-Kahila, T., & Salovaara, A. (2020). Challenges of Explaining the Behavior of Black-Box AI Systems. *MIS Q. Executive*, 19, 7. https://doi.org/10.17705/2MSQE.00037.

[15] Pedreschi, D., Giannotti, F., Guidotti, R., Monreale, A., Ruggieri, S., & Turini, F. (2019, July). Meaningful explanations of black box AI decision systems. In *Proceedings of the AAAI conference on artificial intelligence*, 33(01), pp. 9780-9784.

[16] Solanke, A. A., & Biasiotti, M. A. (2022). Digital forensics AI: evaluating, standardizing and optimizing digital evidence mining techniques. *KI-Künstliche Intelligenz*, *36*(2), 143-161.

[17] The INNOCENT toolkit, p. 71, also highlights the importance of secure IT infrastructure for handling electronic evidence. Having regard to the need for the Courts to have an appropriate ITC infrastructure, see also CJEU, judgment of 17 October 2024, Marek Jarocki v. C.J., Case C-302/23, ECLI:EU:C:2024:905, para. 39, ' ... *the answer to the question referred is that Article 2(1) and (3) and Article 25(1) of Regulation No 910/2014 must be interpreted as not precluding national legislation under which a procedural document cannot be lodged with a court by electronic means and signed electronically unless that court has an appropriate ICT system and the lodging is carried out by means of that system*'.

[18] One of the most common issues raised by criminal defense lawyers across various EU member states in a ECBA questionnaire on the use of video-conferencing in criminal proceedings is the lack of appropriate technology for video-conferencing on the court's side,

where disruptions often arise from outdated or insufficient equipment and poor connection quality.

[19] Supported by the INNOCENT toolkit, p. 63, which calls for standardized procedures for handling electronic evidence.

[20] The INNOCENT toolkit, p. 72, also emphasizes the role of AI in assisting, not replacing, human decision-making in evidence analysis.

[21] Supported by the FRA ECBA expert meeting summary, (https://www.ecba.org/content/index.php/working-groups/e-evidence/894-ecba-participation-at-the-fra-expert-meeting-on-digitalisation-and-justice-november-2023) which highlights the need for secure communication platforms in digital justice.

[22] The INNOCENT toolkit, p. 87, also stresses the importance of training for defence lawyers in handling electronic evidence.

[23] The INNOCENT toolkit, p. 70, also emphasizes the importance of cybersecurity in preserving the integrity of electronic evidence.

[24] See Ramos, V.C/Luchtmann, M./Munteanu, G, Improving Defence Rights Including Available Remedies in and (or as a Consequence of) Cross-Border Criminal Proceedings, Eucrim 3/2020, https://eucrim.eu/articles/improving-defence-rights/#docx-to-html-fn64.

[25] On the topic of the use of videoconferencing in criminal cases, see European Criminal Bar Association, "Statement of Principles on the use of Video-Conferencing in Criminal Cases in a Post-Covid-19 World", <http://www.ecba.org/extdocserv/20200906_ECBAStatement_videolink.pdf>, accessed 2 November 2020.

[26] Issuing a EIO for a suspect to be heard via a video link in another Member State is presented as alternative measure available under Union legal instruments on judicial cooperation to be considered before the use of an arrest warrant (see Official Journal of the EU, Commission Notice Handbook on how to issue and execute a European arrest warrant 2017/C 335/01 §2.5). On the topic of the use of videoconferencing in European Arrest Warrant cases, see European Criminal Bar Association, "Statement of Principles on the use of Video-Conferencing in Criminal Cases in a Post-Covid-19 World", <http://www.ecba.org/extdocserv/20200906_ECBAStatement_videolink.pdf>, accessed 2 November 2020.

[27] The INNOCENT toolkit, p. 74, also calls for EU-wide guidelines on AI use in criminal justice.

[28] Supported by the FRA ECBA expert meeting summary (https://www.ecba.org/content/index.php/working-groups/e-evidence/894-ecba-participation-at-the-fra-expert-meeting-on-digitalisation-and-justice-november-2023), which highlights the need for standardized technical solutions in cross-border digital justice., which highlights the need for standardized technical solutions in cross-border digital justice.

[29] The INNOCENT toolkit, p. 81, also discusses the need for procedural safeguards in handling electronic evidence.

[30] Supported by the INNOCENT toolkit, p. 101, which discusses the European Investigation Order for cross-border evidence gathering.

[31] See the FRA ECBA expert meeting summary (https://www.ecba.org/content/index.php/working-groups/e-evidence/894-ecba-participation-at-the-fra-expert-meeting-on-digitalisation-and-justice-november-2023), highlighting the need for cross-border digital justice to respect procedural rights. The INNOCENT toolkit, p. 47, also emphasizes the importance of protecting fair trial rights in cross-border proceedings involving electronic evidence., highlighting the need for cross-border digital justice to respect procedural rights. The INNOCENT toolkit, p. 47, also emphasizes the importance of protecting fair trial rights in cross-border proceedings involving electronic evidence.

[32] See ECBA Statement of Principles on the use of video-conferencing in criminal cases in a Posto Covid-19 World, September 6, 2020, https://www.ecba.org/extdocserv/20200906_ECBAStatement_videolink.pdf