EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of European Lawyers

Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

CCBE position paper on the proposal for a regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)

8/10/2021

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 45 countries, and through them more than 1 million European lawyers. The CCBE responds regularly on behalf of its members on policy issues which affect European citizens and lawyers.

Introduction and executive summary

On 21 April 2021, the European Commission presented a proposal for a regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. The proposal is supplemented by 9 annexes.

The CCBE previously issued comments on the communication on the digitalisation of Justice in the EU, a response to the consultation on the European Commission's White Paper on Artificial Intelligence as well as its own considerations on the legal aspects of Artificial Intelligence.

With this paper, the CCBE wishes to further develop its position in relation to several aspects of the proposal for an Artificial Intelligence Act (hereafter "the AIA" or "the proposal").

In particular, the CCBE considers that:

- **Despite the choice of a risk-based approach, the proposal should contain specific provisions on the use of AI in the field of Justice.**
- **The proposal must contain clearer prohibitions in Article 5. Any type of social scoring should be prohibited, as well as automated recognition of human features in publicly accessible spaces or the use by AI systems of biometrics to categorise individuals into clusters.**
- **A judge should not be allowed to delegate all or part of his/her decision-making power to an AI tool: there should be prohibited in the field of Justice not only automated decision making by AI systems but also the use of those AI systems which produce "decisions" of a nature which might tempt a human judge simply to adopt such decisions uncritically – effectively rubber-stamping what in effect would be automated decision-making.**
- **The entire decision-making process must remain a human-driven activity and human judges must be required to take full responsibility for all decisions. A right to a human judge should be guaranteed at all stages of the proceedings. Annex III.8 and Recital 40 should clarify that, where an AI system may be used to "assist" judicial authorities, the possibility of it doing so to, in effect, reach decisions or formulate the expression of such decisions is excluded.**

- **The proposal should definitively exclude the use of AI tools which may infringe a person's fundamental rights; for example: for the purposes of so-called "predictive policing" and for the purposes of determining risks of future offending as an aid to the making of decisions as to the granting of bail, the imposing of a sentence, following conviction, the making of decisions concerning probation and, generally, during prosecution and trial.** Furthermore, the output of an AI system should not, of itself, be treated in judicial proceedings as having the status of **evidence**.
- **The principles of transparency and explainability must be strictly observed. In those cases where the manner in which an AI system produces an output is not transparent or where that output cannot be sufficiently explained, the output must not be taken into account by a law enforcement authority and removed from the file.**
- **The AIA should define the notion of "judicial authority", as mentioned in Recital 40 and Annex III.8.**
- **The use of an AI system to apply the law to a "concrete set of facts" should be excluded and the relevant deletions should be made in Recital 40 and Annex III.8.**
- **The transparency obligations laid down in Article 13 must be strengthened.**
- **The exception to the principle of transparency, laid down in Article 52, paragraph 1, for certain AI systems intended to interact with natural persons should be discarded.**
- **There should be a ban or moratorium on the use of automated technologies in border and migration control until they are independently assessed for compliance with international human rights standards.**
- **The proposal should limit uses and applications of AI systems that violate access to social rights and benefits**.
- **Specific provisions should be adopted on AI liability issues. The following issues must be considered:**
    - **the notion of product**;
    - **the lack of foreseeability in the functioning of AI systems;**
    - **the addressee of liability**;
    - **the defences**;
    - **the type of damage and the victims**;
    - **the rule of evidence and the reversal of burden of proof in certain situations; and**
    - **the question of whether there should be mandatory insurance.**

A. General comments: the use of AI in the Justice area

The use of Artificial Intelligence raises many questions, especially with regard to fundamental rights and the rule of law, and thus constitutes a real challenge for both judicial institutions and lawyers. When considering the different possible uses of AI in the judicial process, its introduction within court systems could undermine many of the foundations on which justice is based, as the CCBE stressed in its response to the European Commission's White Paper on Artificial Intelligence.

Change should be embraced where it improves or at least does not worsen the quality of our justice systems. However, the respect for fundamental rights and adherence to high ethical standards that underpin institutions based on the rule of law, cannot be subordinated to mere efficiency gains or cost-saving benefits, whether for court users or judicial authorities. In particular, AI systems should be introduced only when there are sufficient safeguards against any form of bias or discrimination.

Therefore, it is important that, if deployed, AI tools are properly adapted to the justice environment, taking into account the principles and procedural architecture underpinning judicial proceedings. Before AI tools are implemented in judicial systems, the CCBE considers that a set of rules and principles governing the use of AI must be defined and adopted. Furthermore, the CCBE recalls that a fair trial begins with a fair investigation, and that the use of AI by law enforcement authorities must also be assessed having regard to the uses that may be made of the outputs of AI systems during any subsequent trial.

In this regard, the CCBE welcomes the recognition by the proposal of the risks caused by the use of AI systems in the law enforcement and justice areas, in particular the potentially significant impact of the use of such systems on democracy, the rule of law, and individual freedoms as well as the right to an effective remedy and to a fair trial[1].

However, as explained in its response on the White Paper on AI, the CCBE regrets that a **more targeted approach** has not been chosen by the European Commission, in order to set legal requirements tailored to the needs of specific sectors, use-cases and circumstances. The horizontal risk-based approach may give the impression that as long as the listed technical requirements are met, there is no longer a problem with the use of artificial intelligence.

The CCBE considers that the proposal should contain provisions targeting specific risks in specific circumstances, such as a risk of an unfair trial if parties in a case are not given the opportunity to assess, discuss and raise objections against the results produced by an AI tool which was used in the judicial decision-making process. In order to ensure respect for fundamental rights and the right to a fair trial, it should be clearly and explicitly expressed that the proposed regulation does not preclude the establishment of additional general rules further restricting or prohibiting the use of artificial intelligence in the fields of justice including criminal investigations by law enforcement authorities.

Therefore, use of AI tools must be reconciled with the fundamental principles that govern the judicial process and guarantee a fair trial, including, for example, the use of adversarial procedures, the equality of arms, and the impartiality of the court. Even if there might be a temptation to sacrifice all for efficiency, these fundamental rights must remain guaranteed to all parties seeking justice.

[1] Recital 40 of the proposal.

B. Prohibited AI systems

The CCBE welcomes the prohibition in Article 5 of the proposal of certain AI practices which contradict EU values of respect for human dignity, freedom, equality, democracy, the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of children.

However, the CCBE regrets that **such prohibitions are too limited in their scope and include broad exceptions**. This is particularly relevant with regard to the use of AI for **social scoring** (Art. 5.1.c.) and the use of remote **biometric identification systems** in publicly accessible spaces for the purposes of law enforcement (Art. 5.1.d.).

The CCBE agrees with the Joint Opinion of the European Data Protection Supervisor ("EDPS") and the European Data Protection Board ("EDPB") on the proposal, which considers that future AI regulation should prohibit any type of social scoring and any use of AI for automated recognition of human features in publicly accessible spaces or the use of biometrics by AI systems to categorise individuals into clusters[2].

Regarding social scoring, the prohibition provided for in the proposal is undermined by the two conditions set out in article 5 (c) (i) and (ii), e.g. "unrelated to the context" and "unjustified or disproportionate", whose wording may leave room for a broad interpretation allowing the prohibition to be overridden. Furthermore, the prohibition should be extended to the placing on the market, putting into service or use of AI systems by businesses, and not be limited to public authorities or private actors acting on their behalf. The impact of such technology on democracy and the rule of law cannot be underestimated. Not only are rights to privacy and family life infringed, but discriminations are intensified, and citizens can find themselves in opposition to a superior state (and an unfavourable score). In some cases, the presumption of innocence will *de facto* be reversed by social scoring and its outcomes. Anonymity, including not being scored for specific behaviours, is often the corner stone for being able to fully exercise one's fundamental rights. This is undermined by social scoring technologies or even made impossible.

Regarding biometric identification systems, the CCBE considers that this should not take place until it is possible to ensure a full compliance with the Charter of Fundamental Rights of the EU and the European Convention on Human Rights, including relevant case law. Biometric identification tends to have serious flaws that endanger civil rights. Further, the widespread use of biometric identification systems may pose severe risks for an open and pluralistic society if not used proportionately with an intended aim such as ensuring public safety. In many situations, anonymity is the most important safeguard of freedom, and biometric identification techniques that cover major areas in the public space endanger this freedom. The more accurate they are and the more widespread their use, the more dangerous to fundamental rights they become.

Moreover, the CCBE stresses that the proposal should be strengthened with **the prohibition of automated decision making by AI systems in the field of Justice.**

The CCBE considers the judge should not be allowed to delegate all or part of his/her decision-making power to an AI tool. Therefore, the proposal should prohibit automated decision making by AI systems in the field of Justice or even systems which promote the temptation to only rubber-stamp prepared decisions of AI systems. In any case, a right to a human judge should be guaranteed at all stages of the proceedings.

[2] EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, points 29-35.

C. High Risk AI systems

The CCBE welcomes the classification of certain AI systems as "High Risk", in particular systems related to law enforcement; migration, asylum and border control management; and the administration of justice (Annex III, points 6,7 and 8). However, the CCBE would wish to make the following comments:

1. AI systems used for law enforcement purposes

As explained in its response to the White paper on AI, the CCBE considers that the use of AI in criminal justice systems and law enforcement raises numerous issues, such as **inherent bias** in tools used for predicting crime or assessing the risk of re-offending. Such **forms of discrimination** pose a threat to civil rights. Beyond bias and discrimination, fundamental rights risk being undermined by the use of AI systems which replace necessary individual assessments by statistical calculations or assessing probabilities. Such tools are not properly applicable to the circumstances of an individual, but are built upon statistical or actuarial calculations derived form a consideration of either a general population, or a supposedly representative sample of the general population.

A number of predictive policing systems have been shown to reflect biases in the dataset upon which they have been educated or in the features of the system. Such systems tend disproportionately to include people from certain communities. This is because the crime statistics used to educate the systems reflect policing activity rather than crimes committed. Police activity in relation to some social or racial groups may be disproportionately higher than it is in relation to other groups, and the systems built on such datasets will reflect convictions achieved in relation to those groups as opposed to the number of crimes actually committed by persons in those groups compared to crimes committed by members of other less-intensively policed groups. The AI tool will therefore reflect policing bias. Predictive policing systems can undermine the presumption of innocence by treating people as individually suspect on the basis of inferences about a wider group.

The outputs of risk assessment tools in the criminal justice system and in the pre-trial context, such as algorithms for profiling individuals in trials, pose serious threats to fundamental rights. These tools base their assessments on extensive collection of personal data unrelated to the alleged misconduct of the accused. Furthermore, some predictive policing systems may also take into account the number of times an individual has been suspected of a crime, whether or not that individual was subsequently convicted. This collection of personal data for the purpose of predicting the risk of re-offending cannot be seen as necessary or proportionate to the objective pursued, especially in view of the implications for the right to privacy and the presumption of innocence. Furthermore, substantial evidence has shown that the introduction of such systems into criminal justice systems in Europe and elsewhere has led to unfair and discriminatory outcomes[3].

Additionally, the use of AI in the field of digital forensic work and re-offence risk assessment faces challenges, given that the specific ways the algorithms work is usually **not disclosed** to the persons affected by the result of their use. This leaves the defendant unable to challenge the predictions made by the algorithms, which jeopardises the right to a fair trial.

Another concern relates to the **inequality of arms** that may arise between the more advanced capabilities which prosecutors may have at their disposal and the more limited resources lawyers may have.

In the **resolution on Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters**, adopted on 6 October 2021, the European Parliament expresses concern that the use of AI systems for law enforcement could potentially lead to mass surveillance, breaching key EU principles of proportionality and necessity. In this regard, the resolution highlights

[3] See the report of Fair Trials: "*Automating injustice: the use of Artificial intelligence & Automated decision-making systems in Criminal justice in Europe*", 9 September 2021.

the potential for bias and discrimination in the algorithms on which AI and machine-learning systems are based. It stresses that **AI-based identification systems are inaccurate and can wrongly identify minority ethnic groups and that AI-powered predictions can amplify existing discrimination, a concern in the context of law enforcement and the judiciary**[4].

The CCBE notes that the provision of Annex III.6.a. (which allows AI systems to assess the risk of offending) creates a risk of violating the principle of the presumption of innocence.

Furthermore, as noted above, such AI systems may make their predictions upon the basis of biased datasets or improper considerations, such as whether an individual has been "suspected" of an offence. Threats to fundamental rights also arise from the assessment of the risk of "reoffending" and "risk for potential victims of criminal offences", where AI systems can be used for a different purpose than the one originally intended. The CCBE considers that the right to a fair trial begins with a fair investigation. Therefore, the proposal should definitively exclude the use of AI tools for the purposes of so-called "predictive policing" and for the purposes of determining risks of future offending as an aid to the making of decisions as to the granting of bail, the imposing of a sentence following conviction, the making of decisions concerning probation and, generally, during prosecution and trial.

The CCBE points out that the recognition of AI systems used for law enforcement purposes in Annex III, point 6, could legitimise practices which might tend to undermine fundamental rights. Therefore, the principles of transparency and explainability must be strictly observed. In those cases where the manner in which an AI system produces an output is not transparent or where that output cannot be sufficiently explained, the output must not be taken into account by a law enforcement authority.

In any case, the outputs of AI systems for law enforcement purposes ought not to be admitted as evidence in any subsequent judicial proceedings. Such outputs must be removed from the Court file.

2. AI systems and the administration of justice

As above-mentioned, the CCBE considers that, if deployed, AI tools must be properly adapted to the justice environment, taking into account the principles and procedural architecture underpinning judicial proceedings. The CCBE welcomes the classification by the proposal, including Annex III.8 of the use of AI systems in the field of justice as high risk, "*considering their potentially significant impact on democracy, rule of law, individual freedoms, as well as the right to an effective remedy and to a fair trial*"[5].

The CCBE notes that, reflecting Recital 40, Annex III.8 provides an exception for "*AI systems intended to **assist** a **judicial authority** in researching and interpreting facts and the law and in applying the law to a **concrete set of facts**"*. However, the CCBE considers that such wording is unclear and should be clarified.

a) Exclusion of autonomous decision making

As stated above, the CCBE considers that the proposal should provide for the principle of non-delegation of the judges' decision-making power and the right to a human judge. Therefore, the role of AI tools, as presented in Annex III.8, should be defined in such a way that the use of the tools does

[4] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

[5] Recital 40 of the proposal.

not interfere with the judge's autonomous decision-making power. Indeed, under no circumstances should the judge delegate all or part of his/her decision-making power to an AI tool. AI tools should neither limit nor regulate the judge's decision-making power, for example by being used to make an automated decision. The provisions should also prevent AI systems from preparing decisions that need only to be rubber-stamped by human judges. When the judge´s decision is partially based on elements resulting from the use of an AI tool, the use of that tool and the relevance and applicability of its output should be properly justified and explained in the judgement.

The CCBE recalls that in its communication on the digitalisation of Justice in the EU, the European Commission stressed the "*considerable risks*" associated with the use of AI-based applications for automated decision-making and predictive justice and underlined that "*the use of Artificial Intelligence tools can support, but must not interfere with the decision-making power of judges or judicial independence*". The Commission concluded that "*the final decision-making must remain a human-driven activity and decision*"[6].

In this regard, Annex III.8 and Recital 40 should clarify that the use of an AI system to "assist" judicial authorities should not be permitted to make a judicial decision that might have a significant legal effect on individuals or legal persons. As indicated in the communication on the digitalisation of justice in the EU, the proposal should require that not only the final decision itself but also the entire decision-making process should remain a human-driven activity.

Furthermore, to avoid any tendency that AI-made judgements might simply be signed off by a judge, the AIA must clearly provide for the right to a human judge, as above mentioned and underlined in the CEPEJ European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment[7].

b) Definition of judicial authorities

Although the proposal classifies as high-risk AI systems intended to assist judicial authorities, **the CCBE regrets the lack of a specific definition of the term "judicial authorities". A clear definition of this term is essential in order more clearly to set out the scope of the provision**.

Such a clarification is of paramount importance to avoid any risk of diverging interpretations of the meaning of "judicial authority", while at the same time specifying the framework in which the obligations relating to high-risk AI systems apply. Furthermore, it should be noted that the previous lack of definition of the term "judicial authority" has led to the raising of a number of cases before the European Court of Justice in the field of judicial cooperation in criminal matters.

In this respect, in cases concerning the interpretation of the Framework Decision on the European Arrest Warrant, the Court held that the concept of "judicial authority", within the meaning of that Framework Decision, is an ***autonomous concept of EU law[8]***, considering that such concept "*cannot be*

---

6 Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Digitalisation of justice in the European union "A toolbox of opportunities, COM(2020) 710 final, 2.12.2020, p.10-11.

7 European Commission for the Efficiency of Justice (CEPEJ), European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, December 2018, p.8: "When artificial intelligence tools are used to resolve a dispute or as a tool to assist in judicial decision-making or to give guidance to the public, it is essential to ensure that they do not undermine the guarantees of the right of access to the judge and the right to a fair trial (equality of arms and respect for the adversarial process)".

8 CJEU, 10 November 2016, Krzysztof Marek Poltorak, C-452/16 PPU, §52; CJEU, 10 November 2016, Ruslanas Kovalkovas, C-477/16 PPU, §48.

left to the assessment of each Member State" and "*requires, throughout the Union, an autonomous and uniform interpretation*"[9].

According to the Court, the words "*judicial authority* […] *are not limited to designating only the judges or courts of a Member State, but may extend, more broadly, to the authorities required to participate in administering justice in the legal system concerned*"[10].

Therefore, the CCBE considers that the provisions of the AIA should clearly define what is meant by "judicial authority" for the purposes of the AIA, and that this definition should be based on the case law of the Court of Justice of the European Union.

c) the notion of a "concrete set of facts"

The CCBE notes that the wording "*concrete set of facts*" in Annex III.8 raises concerns, as in many judicial procedures the set of facts constantly evolves during the judicial process. This requires defining the stage of the procedure where one can admit that there is a "*concrete set of facts*" and that AI can be used. Moreover, the use of the term "*concrete*" is unclear as to whether it is a precondition for the use of an AI system. This creates such uncertainty that the CCBE would recommend that this exception is deleted.

Therefore, the CCBE considers that the possibility for an AI system to apply the law to a "concrete set of facts" should be deleted by modifying the wording of Recital 40 and Annex III.8.

3. AI systems and Migration, Asylum and Border Control Management

Increasing examples of the use of AI in the field of migration control represent a growing threat to the fundamental rights of migrants, to EU law and to human dignity.

EU migration policies are increasingly supported by AI systems, such as facial recognition, profiling and predictive tools used in migration management processes, including forced return. These use cases may violate data protection rights, the right to privacy, the right to non-discrimination and various principles of international migration law, including the right to seek asylum.

Given these concerns and the significant power imbalance that these deployments exacerbate and exploit, the CCBE considers that there should be a ban or moratorium on the use of automated technologies in border and migration control until they are independently assessed for compliance with international human rights standards.

4. Considerations on Other High-risk AI systems

Artificial intelligence systems are used in the allocation of social and economic rights and benefits, to verify identity and to calculate welfare access scores. All this has a strong impact on people's access to vital public services and thus on the fundamental right of citizens to social security and social assistance. The risk of discriminatory profiling or false results goes hand in hand with the risks arising from the processing of sensitive biometric data. In several countries, the use of automated decision-

9 Krzysztof Marek Poltorak, C-452/16 PPU, §§31-32.

10 *Ibid*., §33

making systems to profile the unemployed has shown serious implications in terms of discrimination and data protection. In addition, similar risks arise from the intensive monitoring of workers' and students' performance targets and other measures concerning them. This is evidenced by cases of discriminatory use of AI technologies against people with disabilities by state and private entities in the allocation of social benefits and access to education.

In these areas, the CCBE considers that there is a need to limit the use and application of AI systems that violate access to social rights and benefits. Furthermore, the CCBE calls upon the EU institutions to include communities or people at risk of exclusion, minorities and other potentially affected communities in the development of their AI legislation and policies.

D. Transparency obligations

The CCBE welcomes the obligations that are to be applied to high-risk AI systems, including the use of AI in the field of justice. However, the CCBE recalls that principles of transparency and explainability are extremely important in criminal law cases. In cases where the decision is likely to be based on the data or outcomes provided by an AI tool, the parties and/or their lawyers should be given the opportunity to access that tool and assess its characteristics, the data used and the relevance of the outcomes it provides. As a result, "Learning software" should only be used to the extent that it would still be possible to verify how the machine achieved the proposed result and to distinguish the elements resulting from the use of AI from the judge's personal reflection.

Beyond the more targeted approach requested for justice, therefore, the CCBE considers that a special reference is needed in Article 13 regarding the fact that AI systems, if used in the justice system, do not obstruct the right to a fair trial and do not violate the rights of the defence. Moreover, given that the manner in which some AI systems produce their output may not be reasonably capable of explanation (the "black box" problem), and the fact that the transparency requirement might not always be satisfied whether for that or some other reason, the proposal must provide for other safeguards, for instance the outcome provided by an AI tool must not be taken into account in case of doubt or when the requirements of transparency or explainability are not satisfied.

The CCBE notes the exception stated in article 52 to transparency obligations applying to certain AI systems intended to interact with natural persons, namely, that such "*obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence*".

The CCBE considers that this exception is excessive and might jeopardise the right to a fair trial. In this regard, the CCBE welcomes the conclusions of the EDPS and the EDPB which consider that "*the fact that the transparency obligation does not apply to AI systems used to detect, prevent, investigate, or prosecute criminal offences is too broad of an exception. A distinction must be made between AI systems that are used to detect or prevent and AI systems that aim to investigate or help the prosecution of criminal offences. Safeguards for prevention and detection have to be stronger because of the presumption of innocence. Moreover, the EDPB and the EDPS regret the absence of cautionary warnings in the proposal, which can be interpreted as a greenlight for the use of even unproven, high-risk AI systems or applications"*[11].

Therefore, the CCBE considers that this proposed exception to the principle of transparency for certain AI systems should be deleted

[11] EDPB-EDPS, Joint Opinion 5/2021 on the AIA, 18 June 2021, point 70.

E. The need for liability rules

The CCBE regrets the absence of provisions regarding liability implications arising from the use of AI. Indeed, certain important changes need to be made to the current legislative framework considering the fundamental differences that exist between traditional products and AI products, in particular when it comes to the notions of product, fault and defect.

This seems to be particularly necessary because the application of the product liability laws on AI systems and the compensation of the typical damages caused by them may be disputed. For instance, even the qualification of software applications as products is subject to dispute at least in some Member States. Also, the compensation of intangible and pecuniary damages is not generally provided by the product liability laws.

The regulation of AI applications without a fair distribution of the associated risks may lead to unintentional impositions of these risks onto consumers.

The CCBE considers that specific provisions should be adopted on AI liability issues rather than amending the Product Liability Directive. Aspects such as compensation for damage and allocation of liability, as well as rules on the burden of proof, should be regulated at EU level.

The following issues must be considered when amending the current legislative framework:

- **the notion of product**;
- **the lack of foreseeability in the functioning of AI systems;**
- **the addressee of liability**;
- **the defences**;
- **the type of damage and the victims**;

  the rule of evidence and the reversal of burden of proof in certain situations; and
- **the question of whether there should be mandatory insurance.**