

CCBE Response to the consultation on the European Commission's White Paper on Artificial Intelligence

05/06/2020

Introduction and summary

The Council of Bars and Law Societies of Europe (the 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.

In this document, it is the intention of the CCBE to explain in more detail a number of its responses to the general questionnaire regarding the consultation on the [White Paper on Artificial Intelligence – A European approach to excellence and trust](#) (as copied below in the ANNEX on page 12-22), and to provide more detailed suggestions on the issues of the greatest relevance from the point of view of lawyers. This document takes much of its inspiration from the recently published [CCBE Considerations on the Legal Aspects of Artificial Intelligence](#) (AI).

First, the CCBE expresses its concerns as to the way in which the consultation questionnaire was formatted. In particular, the questionnaire has not been tailored to specific sectors and use cases, and does not offer respondents the opportunity to indicate per question from which perspective the reply is given. As a result, it will be very difficult to interpret the various replies without additional background information as to how the respective respondents have approached the various questions. Moreover, many of the questions are leading questions offering only a closed set of options as a result of which it is impossible to express a meaningful opinion.¹

For these reasons, the CCBE wishes to clarify that the scope of its response to this consultation is mainly limited to aspects related to the rule of law, administration of justice and fundamental rights. Moreover, the CCBE also addresses certain liability issues as well as training needs for lawyers and law firms regarding the use of AI in legal practice.

The parts below are structured along the topics addressed in the consultation questionnaire and address the following main issues:

- **An ecosystem of excellence:**
 - **EU-level funding** should be made available for sectoral regulators – including bars and law societies – in order to **train lawyers** on topics such as the use of novel technologies and AI in the justice area while respecting ethical principles and data protection requirements.
 - **Interaction amongst all sectors**, private and public, is essential for ensuring that the ethical values that guide the various actors are designed into the AI systems themselves.

¹ Reference is made to the CCBE remarks regarding the Commission consultation on the 'Stocktaking of the Commission's 'Better Regulation' approach' where the CCBE called upon the Commission to revise its methodology of designing questionnaires. See Paragraphs 3-6 under this link:
https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/Position_papers/2018/EN_NA_20181019_CCBE-remarks-on-the-Commission-consultation-on-the-Commissions-Better-Regulation-approach.pdf

- Lawyers need to be provided with **access to testing and reference facilities** to be able fully to exercise their role and responsibilities in ensuring the proper deployment and review of AI tools.
- **An ecosystem of trust:**
 - **Artificial intelligence and human rights:** virtually all human rights can be affected by the use of AI systems. Various actions are therefore needed, amongst which: thorough assessments of the effect of AI systems; independent and expert scrutiny; transparency on the use of AI; ensuring the availability of remedies; new legal frameworks to codify the principles and requirements governing the use of AI, in conjunction with voluntary ethics codes committing AI developers to act responsibly.
 - **As an alternative to the proposed risk-based approach, the CCBE calls for a more targeted approach** which sets legal requirements tailored to the needs of the specific sectors and circumstances after a more detailed evaluation of risks and assessment of legal or other appropriate measures.
 - **The use of AI by courts and in criminal justice systems is a high risk** as it undermines many of the foundations on which justice is based. Any deployment of such tools should therefore be preceded by in-depth evaluation and impact assessments with the involvement of all relevant actors and stakeholders and be strictly regulated taking into account the procedural architecture underpinning judicial proceedings. In any case, a **right to a human judge** should be guaranteed at any stage of the proceedings.
 - A combination of **ex-ante compliance and ex-post enforcement mechanisms** is needed on the basis of a set of **mandatory requirements**.
- **Safety and liability implications of AI, IoT and robotics**
 - **Certain important changes will need to be made to the current legislative framework** considering the fundamental differences that exist between traditional products and AI, in particular, when it comes to the notions of product, fault, and defect.
 - **The CCBE would opt for a separate instrument 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.
 - Issues to be considered when amending the current legislative framework include: the **notion of product; lack of foreseeability** in the functioning of AI systems; **addressee of liability; defences; type of damage and victims; rule of evidence** and the reversal of **burden of proof** in certain situations; and the question of **mandatory insurance**.

Section 1 - An ecosystem of excellence

With the rise of AI and the arrival of legal tech, legal practice has become increasingly complex due to novel legal issues being raised by AI and the development of highly sophisticated digital tools which lawyers need to master and understand. There is also a need for lawyers to make conscious and responsible use of these new technologies in order to carry out their activities in the best possible way, protecting the relationship of trust between the lawyer and the client and ensuring compliance with professional obligations. In this regard, the most obvious principles to respect in the use of AI tools concern: the duty of competence, the duty to inform the client, maintaining lawyers' independence in terms of defence and advice, the duty to preserve professional secrecy/legal professional privilege and the obligation to protect the confidentiality of clients' data. Therefore, training is needed to extend lawyers' general competence in understanding the technological environment that they are likely to be working in in the future.

The CCBE therefore strongly supports the idea that **EU-level funding should be made available for sectoral regulators** – including bars and law societies – as they are best positioned to understand and address the training needs for their respective sectors – such as lawyers – particularly as regards how AI can be used in a way which is compatible with their ethical codes and professional duties. In this respect, reference is made to the [contribution of the CCBE for the next EU policy on judicial training](#)² which also highlights the need for training of lawyers on topics such as the use of novel technologies and artificial intelligence in the justice area while respecting ethical principles and data protection requirements.

Another essential aspect is **interaction amongst all sectors**, private and public, for ensuring that the ethical values that guide the various actors are designed into the AI systems themselves. It is not sufficient merely to rely on trust in the expertise of technical specialists operating in the field of computer systems. New bridges of trust must be built taking into account the specific expertise and roles of actors and specialists across different sectors and professions. In this regard, the CCBE wishes to highlight that lawyers play an important role to ensure access to justice, defence of the rule of law and protection of democratic values, and as such have a particular role to play when it comes to the further development and deployment of AI tools, especially in those areas where access to justice and due process are at stake.

Lawyers therefore also need to be provided with **access to testing and reference facilities** to be able fully to exercise their role and responsibilities in ensuring the proper deployment and review of AI tools. This is particularly important when AI tools may come to be contested in court proceedings and need to be reviewed by the parties.

Section 2 - An ecosystem of trust

I. Artificial intelligence and human rights

In general, the use of AI in automated decision-making processes may reshape the interaction between citizens and public/private decision-makers. This may undermine citizens' ability to seek advice, or to contest or seek to reverse decisions. Therefore, robust redress mechanisms need to be ensured as well as a close involvement of those actors who have a function in protecting citizens' rights (e.g. lawyers and judges).

Further, virtually all human rights may be affected by the use of AI systems. The CCBE stresses the following in particular:

From the CCBE's point of view, the **right to a fair trial** is a key point of concern. While issues pertaining to the use of AI in court and in criminal proceedings will be identified below, also a **right to a human judge** is part of the right to a fair trial.

Besides, potential **bias** of the data sets which AI uses to learn is also a clear example of an issue affecting the fairness of a trial. AI systems do not understand the entire context of our complex societies. Their input data is the only context in which they operate and if the data provided to train AI is incomplete or include (even non-intentional) bias, then the output of AI can be expected to be incomplete and biased as well. Also, at the current development stage, AI systems often lack transparency in their conclusions. They lack explainability, i.e. the ability to explain both the technical processes of an AI system and the related human decisions (e.g. application areas of a system). Therefore, humans do not understand or have doubts regarding how AI systems reach conclusions.

² https://www.ccbe.eu/fileadmin/specialty_distribution/public/documents/TRAINING/TR_Position_papers/EN_TR_20200427_CCBE-contribution-for-the-next-EU-policy-on-judicial-training.pdf

These conclusions can be harmless in ordinary use, but when used before a court, the conclusions may interfere with the fairness of the proceedings.

For the sake of **transparency** and in order to enable individuals to defend their rights, it seems appropriate that the persons impacted by the use of an AI system should be duly informed that AI is being used and that data concerning the matter put in issue by him or her may be considered by an automated system. This corresponds with the current data protection principles, which in general must be followed when using AI, as must also any other applicable legal standards. As is common elsewhere, ensuring the availability of remedies will be likely to be the appropriate measure to address cases of misuse of AI systems.

The right to freedom of expression and information may be affected as well – AI will allow for more scrutiny and control of the way in which people can express themselves both online and offline. While positive uses can be seen when fighting against hate speech and fake news, the line between the beneficial use of AI and its misuse appears to be tenuous.

Similarly, the **right to freedom of assembly and association** comes into consideration when using AI to identify participants of assemblies, protests or of any other large gathering. While useful in some situations to protect public order, such tools can easily be misused against political opponents. Systems capable of automated recognition of individuals (face or movement recognition) and analysis of their behaviour are already available. It may well be that these tools will influence the participation of people in assemblies, thus tempering the right to freedom of assembly and association.

The right to a protected life, in the context of smart weapons and algorithmically operated drones will also be affected by AI.

The right to protection against discrimination may be inflicted when employers use AI to automate parts of employee recruiting processes. Even today, systems capable of pre-selection of workplace candidates are available.

In our digital age, the amount of data humans provide about themselves is enormous. Whether it is metadata or content data, they provide many details of their personal lives or details that are just generally private. AI lives on data and its ability to work with the data and combine them is immense. **The right to privacy and data protection** is therefore clearly at stake.

Democratic principles and the rule of law are closely linked to human rights as they complement each other. When noting the right to privacy, gathering of information from people's social network profiles on their political views and then (mis)using them to affect voting preferences and elections, not only tampers with the right to privacy, but also may be considered as an interference with one of the principles of democratic society that has a direct impact on public order.

In view of these considerations, the CCBE recommends that the following actions be taken:

- In general and based on currently available recommendations³ in this field, **thorough assessments of the effect of AI systems on various human rights, democratic principles and the rule of law** is one of the key measures which should be used to prevent unwanted conflicts with these rights, principles and rules. Such assessments should be implemented as soon as practical, even at the early development stage by evaluating the potential impact AI systems may have on human rights throughout their entire life cycle.

³ Council of Europe, Commissioner for Human Rights: Unboxing Artificial Intelligence: 10 steps to protect Human Rights (<https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64>).

- It is also required that AI systems are put under **independent and expert scrutiny**, especially when public use is intended. Making the output of such scrutiny publicly available will not only decrease the chance of intentional and non-intentional biases but will also likely increase the trustworthiness of AI systems. Opening AI systems for scrutiny by any stakeholder may increase their trustworthiness even more; however, this will not be possible without proportionate interferences with trade secrets and other IP rights of AI developers.
- For the sake of **transparency** and in order to enable individuals to defend their rights, persons impacted by the use of an AI system should be **duly informed that AI is being used** and that data concerning him or her matter may be considered by an automated system. This corresponds with the current data protection principles, which in general must be followed when using AI, as must also any other applicable legal standards.
- As is common elsewhere, **ensuring the availability of remedies** will likely be the appropriate measure to address cases of misuse of AI systems or damage caused by them.
- It needs to be assessed whether the currently available **legal frameworks** are adequate or need to be adapted in order to ensure that AI systems are used in compliance with human rights. Possibly, some new legal frameworks may need to be established to codify certain principles and requirements in conjunction with voluntary ethics codes committing AI developers to act responsibly. Since technology (including AI) is extra-national, where the need for a legal framework which is not limited to one jurisdiction can be supported, the development of such a framework would arguably be desirable and would seem to be in line with current developments.⁴

Alongside these general actions, certain rules and principles need to be established in specific areas, most notably as regards the use of AI by courts and in criminal justice systems, as set out below.

II. Possible adjustments to existing EU legislative framework relating to AI

A. Risk-based approach

The CCBE is concerned that an exercise of categorising risk as “high” or “low” on the basis of abstract criteria is too simplistic and will lead to structurally defective regulation. A more targeted approach is called for.

In particular, the factors to be considered in determining risk are many and complex, depending upon the specific use cases, the circumstances of its use, the complexity of the task, the risk posed by any malfunctioning of the AI and its technical nature. For example, AI for a case management system used by courts poses less risk than AI for the assessment of a defendant’s probability of recidivism.

In these circumstances, first, it is not appropriate to give the same legal treatment to things which are technically different, for example, artificial intelligence, the internet of things and other digital technologies, even although they sometimes share common features. In reality, a more nuanced approach, taking into consideration the complex new challenges brought by AI, is called for.

Second, in the White Paper, it is acknowledged that the level of risk can be very different even within the same "sector", such as healthcare. Regulation seeking to neutralise risks can therefore be effective

⁴ See the Council of Europe activities in this field and its Ad Hoc Committee on Artificial Intelligence that has been established on 11 September 2019 to assess the need for such legal framework: <https://www.coe.int/en/web/artificial-intelligence/-/the-council-of-europe-established-an-ad-hoc-committee-on-artificial-intelligence-cahai>.

only if it targets very specific risks in specific circumstances, such as a risk of discrimination in law enforcement surveillance systems, or a risk of an unfair trial if parties in a case are not given the opportunity to assess, discuss and raise objections against an AI tool which was used in the judicial decision-making process.

The CCBE therefore calls for a more targeted approach based on the following actions:

- **Evaluation of the specific risks and damage** that the use of AI tools can cause in specific sectors and circumstances.
- **Assessment of the kind of legal or other appropriate measures** that could be undertaken to address the identified risks and damage in specific sectors and circumstances, bearing in mind that, in a given sector, there can be very widely different risk levels depending upon the precise use to which the AI is put. Within this context, there also needs to be an evaluation of the extent to which existing EU rules need to be adapted or adjusted.
- **Setting of legal requirements tailored to the needs of the specific sectors and circumstances.** In this context, it is important to consider how general principles, such as non-discrimination and fair trial rights, apply and need to be adhered to.

B. High-risk AI application: the use of AI by courts

When we look at the different possible uses of AI in the judicial process, we immediately see that its introduction within court systems could undermine many of the foundations on which justice is based (See the table below).

In the field of justice, there might be strong incentives for using AI. Public authorities have already identified alleged budgetary benefits that could be obtained by replacing some judicial staff with automated systems. The potential use of AI tools could also be seen as a means to enable judges to make more consistent and higher-quality judgments more quickly, rationally and efficiently. There is, therefore, no doubt that there will be attempts to deploy AI will in the field of justice, which raises the question of the conditions for such a use.

The need for an ethical framework regarding the use of AI by courts is therefore clearly apparent and, hence, the CCBE supports the initiative of the Council of Europe European Commission for the Efficiency of Justice (CEPEJ) which has adopted an “ethical charter on the use of artificial intelligence in judicial systems and their environment”⁵.

But ethical reflection alone will not be sufficient, and it is also necessary to identify effective and binding operational rules and principles that can govern, in practice, the use of AI tools by courts. In particular, the use of AI tools must be reconciled with the fundamental principles that govern the judicial process and guarantee a fair trial, e.g.: equality of arms, impartiality, adversarial procedures, etc. Even if the temptation to sacrifice all for efficiency may be present, these fundamental rights have to remain guaranteed to all parties seeking justice.

Table: Identification of possible uses of AI in court systems and imminent dangers for fundamental rights and the rule of law

⁵ See the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment as adopted by the CEPEJ during its plenary assembly on 3-4 December 2018, and is available online at: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

Use of AI by Courts					
Stages	Management of cases	Pre-trial	Trial	Judges' deliberation/ decision-making	Post sentencing
(Potential) AI applications	<ul style="list-style-type: none"> - Case management system - Electronic communications - Digital platforms accessible for lawyers/clients - Automatic monitoring of procedures - Automatic system for monitoring procedural delays - Automatic system for completing procedural formalities - Automatic decisions on the progress of the case - Queue management - Automatic sorting of appeals 	<ul style="list-style-type: none"> - Plea-bargaining: Prosecutor's databases 	<ul style="list-style-type: none"> - Use of videoconference - Automated transcription / automated translation - Automated presentation of file's document on screens during hearings - Case management (in a situation of complex cases) - Use of emotional AI (detection of emotions, etc....) 	<ul style="list-style-type: none"> - Case law tools - Prediction technology - Legal researches and analysis / autonomous researches - Scoring of risks / assessment of the suspect (probability of recidivism) - Automated judgments (decision trees) - Writing assistance tools and drafting judgments - Decision making systems - Intelligence assistant systems (identification of patterns, analysis of data...) 	<ul style="list-style-type: none"> - Scoring of risks / probability of recidivism / parole opportunities
Main principles and issues to be taken into account					
Principles	<ul style="list-style-type: none"> - Adversarial proceedings - Rule of law, due process, security - No restriction of access to justice - Equality of arms - Transparency of decision-making - Access to data by lawyers 	<ul style="list-style-type: none"> - Adversarial proceedings - Equality of arms - Access to data by lawyers - Data protection and compatibility with fundamental rights 	<ul style="list-style-type: none"> - Adversarial proceedings - Fair trial - Transparency - Neutrality (in profiling) - No use of emotional AI when videos are used during a trial 	<ul style="list-style-type: none"> - Adversarial proceedings - Fair trial - Transparency about use of AI by judge - Transparency of decision-making process - Algorithms and accountability - Liability if errors occur - Access to evidence - Right to request for a human intervention (judge) 	<ul style="list-style-type: none"> - Adversarial proceedings - Fair trial - Transparency of decision-making process - Algorithms and accountability - Right to appeal

Main concerns

The above table shows that one can imagine using AI tools in the management or follow-up of files; during hearings (either in the trial or pre-trial phase); to facilitate the judge's decision-making (the deliberation phase); and in the follow-up of the execution of decisions.

The above table also indicates the principles that might be impacted by the use of AI tools due to a multitude of negative realities that might occur, for example:

- The use of data and elements that have not been the subject of an adversarial debate.
- The exploitation of conclusions (even partial ones) that have not been obtained through the reasoning of the judge.
- The lack of transparency of the process, since it becomes impossible to know what should be attributed to the judge and what comes from a machine.
- The absence of a playing field (equality of arms).
- The undermining of the principle of impartiality due to the impossibility of neutralising and knowing the biases of the system designers.
- Breach of the principle of explicability due to the existence of results that are beyond human reasoning and cannot be traced.

The use of AI tools by courts could therefore severely undermine the current procedural architecture underpinning judicial proceedings, especially if it were accepted that the judge could access such tools alone during the deliberation process.

The current general architecture of a trial is explained by the need to ensure compliance with a number of principles and to produce decisions that come from the judge him/herself, in the light of the arguments and evidence provided by the parties. The judge is impartial and his/her decisions contain explanations that make it possible to understand which legal provisions and precedents can justify them.

Operational rules and principles

It is therefore important that **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, a set of rules and principles governing the use of AI should be defined and adopted. In particular, the following minimum safeguards should be upheld:

- **The possibility to identify the use of AI:** all parties involved in a judicial process should always be able to identify, within a judicial decision, the elements resulting from the implementation of an AI tool.
- **Non-delegation of the judge's decision-making power:** under no circumstances should the judge delegate all or part of his/her decision-making power to an AI tool. In any case, a **right to a human judge** should be guaranteed at any stage of the proceedings.
- **The possibility for the parties to verify the data input and reasoning of the AI tool.**
- **The possibility for the parties to discuss and contest AI outcomes** in an adversarial manner outside the deliberation phase and with a reasonable timeframe.
- **Compliance with GDPR principles.**
- **The neutrality and objectivity of AI tools** used by the judicial system should be guaranteed and verifiable

As demonstrated above, much debate is still needed critically to assess what role, if any, AI tools should play in our justice systems. Change should be embraced where it improves or at least does not worsen the quality of our justice systems. However, fundamental rights and adherence to 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.

Any deployment of such tools should therefore be **strictly regulated and be preceded by in-depth evaluation and impact assessments** with the involvement of all relevant actors and stakeholders.

C. High-risk AI applications: the use of AI in criminal justice systems

Some of the police forces' work in the **prevention of crimes** – including all forms of technical surveillance such as **intercepting, collecting and analysing data** (text, audio or video) and **analysis of physical evidence** (DNA samples, cybercrime, witness statements, ...) – can potentially be technically supported by the use of AI. This also gives rise to various issues; for example, inherent **bias** in tools used for predicting crime or assessing the risk of re-offending and tools like **facial recognition technology** being inaccurate at identifying people of different races. Such forms of discrimination pose a threat to civil rights. 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. 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.

As regards the use of **Biometric identification systems (e.g. face recognition) in publicly accessible spaces**, the CCBE considers that this should not take place until specific guidelines or legislation at EU level is in place which are in full compliance with the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights, including relevant case law.

Biometric identification tends to have serious flaws that endanger civil rights. It has been proven in multiple studies to be inaccurate at identifying people of different races. Also, there are grave concerns that the trigger words which are used by national security agencies are not sufficiently refined and thus the phone conversations of millions of people are monitored without a legal basis.

Further, the widespread use of Biometric identification systems may pose severe risks for an open and pluralistic society if not used proportionately with a proportionate 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 they become.

Therefore, when it comes to the use of AI tools in criminal justice systems, most of the rules and principles set out above under I and II.B will also apply. Any deployment of such tools should therefore be **strictly regulated and be preceded by in-depth evaluation and impact assessments** with the involvement of all relevant actors and stakeholders.

D. Mandatory requirements of a possible future regulatory framework

The CCBE agrees that the following mandatory requirements are important for the establishment of a future regulatory framework for AI:

- **The quality of training data sets**
- **The keeping of records and data**
- **Information on the purpose and the nature of AI systems**
- **Robustness and accuracy of AI systems**
- **Human oversight**
- **Clear liability and safety rules**

In addition, the CCBE also stresses that the requirement of **explainability** is of particular importance for the justice environment, i.e. the ability to explain both the technical processes of an AI system and the related human decisions.

As set out above under point II.A, it is important that the legal requirements are tailored to the needs of specific sectors and circumstances.

E. Compliance framework

As regards the question **how to ensure that AI is trustworthy, secure and in respect of European values and rules**, the CCBE considers that a combination of **ex-ante compliance and ex-post enforcement mechanisms** is needed.

However, instead of adhering to a very generic and abstract compliance framework, the appropriate compliance measures must be considered and tailored to the needs in specific sectors and circumstances. The addressees of the compliance framework will therefore also depend and differ according to the exact field that is targeted by the compliance measures.

It is also important to ensure that AI tools are not deployed, especially in the public sector, without having first defined the compliance framework.

Section 3 – Safety and liability implications of AI, IoT and robotics

I. Need to amend the current EU legislative framework for liability

In approaching the question of the liability model for AI systems, some may be tempted to say that the law is already well-developed, especially regarding product liability as well as other liability regimes in force in the Member States, and all that is required in order to protect potential victims is to apply it. On the other hand, because AI is a new development, some may want to seek to reinvent the law of liability to deal with the issues it raises.

If one looks to existing liability models, there are a few possible approaches to address the issue of civil liability in respect of AI: 1) a liability system based on the concept of fault or 2) a strict liability system. Within these broad categories, there may be scope for differing approaches. For example, as regards the latter, the system could be either a pure strict liability regime – where there is liability whether or not there is a defect and where no defences to exclude or reduce liability are allowed – or a strict liability system which allows several defences, following the model of the Directive 85/374/EEC⁶ (EU Product Liability Directive). Moreover, other liability regimes might be worth considering in the context of AI. For example, the recently published report of the Expert Group on Liability and New Technologies set up by the European Commission mentions vicarious liability (liability arising from the actions of others) regarding autonomous technology. Furthermore, contractual liability or other compensation regimes could be applied in some digital ecosystems alongside or instead of tortious liability.⁷

Approaches seem to differ significantly as to the best regime to tackle the issue of liability in respect of AI as well as the political decision that should be adopted in this regard. Despite the approach adopted, **it is clear that certain important changes will need to be made to the current legislative framework** considering the fundamental differences that exist between traditional products and AI, in particular, when it comes to the notions of product, fault, and defect. Questions of to whom liability might be extended, the burden of proof and defences must also be reconsidered.

The CCBE would opt for a separate instrument on AI liability issues rather than amending the Product Liability Directive, recognised as effective in respect of traditional products. Trying to introduce additional measures into the Product Liability Directive in order to cope with AI would necessarily adversely affect the process of research and development for other products, which is not desirable. Any AI products currently falling under the Product Liability Directive should then be taken out of the scope of the Directive and be incorporated into the scope of the new one.

However, the Commission only seems to be considering – at least for the time being – the changes that might need to be made to the *existing* EU instruments, notably to the Product Liability Directive, as well as to national liability regimes, and not the possibility to create a new instrument. In any case, **the CCBE believes that 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**. Another approach might lead to a situation where the adapted national rules would differ significantly between the Member States.

⁶ [Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products](#)

⁷ European Commission: [Report from the Expert Group on Liability and New Technologies](#) – New Technologies Formation: Liability for Artificial Intelligence and other emerging digital technologies, December 2019, pp.36–37.

More precisely, the following observations should be considered by the Commission:

II. Issues to be considered when amending the current legislative framework

A. Notion of product

As already mentioned above, there are fundamental differences between traditional products and AI. First, regarding the notion of product, it should be borne in mind that AI systems are increasingly coming into common use not only as stand-alone systems – which can run on general-purpose computers – but also as part of more complex products. An example of the former is medical diagnosis software used to analyse CT scans for early signs of cancer and of the latter is self-driving vehicles. The CCBE holds that AI should be thoroughly defined in the new legislative instrument.

B. Lack of foreseeability in the functioning of AI systems: impact on the notions of fault and defect

Second, the attribute of self-learning and autonomous decision-making in AI systems militates against the use of traditional legal reasoning based upon the concept of “foreseeability” as a basis of liability. In this context, an AI system may cause damage either as a result of a traditional “defect” for example in the software, but also as a consequence of its “own” actions determined by data and algorithms, without any “defect” in the traditional sense. Thus, liability for damages cannot easily be attributed to “fault” on the part of a person (whether natural or legal) nor by the existence of a defect in a product, in the sense of a specific malfunction in that product.

Under these conditions, one could say that liability for actions taken by an AI system should not necessarily be linked to the notion of fault (in its traditional sense) or a “defect” (in its traditional sense). In this regard, it can also be noted that the existing Product Liability Directive, although based on the existence of a “defect”, defines “defect” not in the traditional sense, but in relation to outcome – i.e. “a product is defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account...” (Article 6(1))”.

C. Addressee of liability

Third, there is the question of to whom liability might extend. That may be a challenging task given the opacity of AI systems and bearing in mind the multiplicity of persons potentially involved, possibly in multiple jurisdictions, and in the case of some persons, their work could be subsequently utilised without their knowledge in an AI system.

There are several possibilities of identifying different actors to whom liability could be attributed. For example, the Expert Group’s report suggests that not only the *producer*, but also the *operator* should be held liable, depending on the circumstances⁸.

The introduction of the notion of “operator” as the “person who is in control of the risk connected with the operation of AI and who benefits from its operation” is to be welcomed in this regard, with a distinction between frontend and backend operator. Such operators, as well as producers, would have to comply with specific duties of care, giving rise to liability in the event they failed to comply with such duties.

⁸ European Commission: Report from the Expert Group on Liability and New Technologies – New Technologies Formation: Liability for Artificial Intelligence and other emerging digital technologies, pp. 39-46.

D. Defences

If the EU legislator institutes a scheme of strict liability for AI products, meaning that whenever AI has caused damage, the addressee of liability for this AI should be liable to cover the damage, detailed consideration should be given to providing for appropriate defences.

However, the specific defences that are currently provided for in the Product Liability Directive should be reconsidered. In particular, the exceptions set out in Article 7 b) (the defect not being in existence at the time when the product was put into circulation) and e) (the state of the art defence) should be rejected in relation to AI. In this regard, the CCBE agrees with the consideration expressed in the expert group's report that a development risk defence should not apply in the context of emerging digital technologies: the producer should be strictly liable for defects even if said defects appear after the product was put into circulation, as long as the producer was still in control of updates to, or upgrades of the technology.⁹

E. Type of damage and victims

When it comes to damages, it is necessary to regard as losses for which damages should be available under specific conditions not only physical and material damage but also the destruction of the victim's data..

As the risks inherent in and damage which may be caused by AI are not as such foreseeable, the damage being covered should not be limited to foreseeable damage. Causal nexus should be considered. Moreover, as AI systems are in a state of constant development, there should be no limitation of liability to damage which is proven to have been foreseeable, so long as, in any given case, the use made of the AI falls into the category of being reasonable and the loss is proved to have been caused by that use of AI (in accordance with the rules of evidence which are explained below).

All of those suffering loss (whether natural or legal persons) should have a claim for damages with no restriction to, for example, only consumers or those using AI in the course of their business, trade or profession

F. Rule of evidence and the reversal of burden of proof in certain situations

Issues regarding the burden of proof also need to be reconsidered in the context of AI systems since self-learning and deep learning features of AI will necessarily lead to a decrease in predictability. Causal connections between input and system behaviour may be difficult to elucidate¹⁰. Under such conditions, the victim cannot always be expected to provide evidence on the internal malfunctions which led to the damages.

Victims should be entitled to facilitation of proof in situations where the difficulties of proving the existence of an element of liability are disproportionate, going beyond what should reasonably be expected. In some cases, the reversal of the burden of proof may be appropriate, such as in the absence of logged information about the operation technology (logging by design) or failure to give the victim reasonable access to this information.

⁹ European Commission: Report from the Expert Group on Liability and New Technologies – New Technologies Formation: Liability for Artificial Intelligence and other emerging digital technologies, p. 6.

¹⁰ Herbert Zech, Liability for autonomous systems: Tackling specific risks of modern IT; "Des voitures autonomes – Une offre de loi", essai, juillet 2018, n°02.226

Where several persons have cooperated in order to create an AI unit and the victim cannot prove which one of those persons has created the element leading to the damage, such facilitation rules should also be able to lead to a joint responsibility of those persons towards the victim. Redress claims between the tortfeasors should be possible.

G. Question of mandatory insurance

Finally, compulsory liability insurance could be seen as a solution to give victims better access to compensation in situations exposing third parties to an increased risk of harm and could also protect potential tortfeasors against the risk of liability.¹¹ When considering this possibility, there may also be broader issues of socio-economic policy to be taken into account. For instance, the perceived desirability of ensuring on the one hand that no-one who suffers loss through the operation of an AI system should go without compensation, set against concerns that there could be a chilling effect on innovation or unwanted interference in business to business relationships.

Moreover, there are other factors should be borne in mind in connection to a mandatory insurance scheme. For example, regarding the question of which actors should be obliged to take such an insurance, it may occur that the number of people who have contributed – in different moments and with different relevance – to an AI system is very large. The potential risks of AI systems can also be very different depending on the sectors where the AI system is used.

The CCBE therefore invites the Commission to carefully consider all these questions and weigh up the advantages and disadvantages of these possibilities.

ANNEX - Draft CCBE Response AI Consultation Questionnaire

¹¹ European Commission: Report from the Expert Group on Liability and New Technologies – New Technologies Formation: Liability for Artificial Intelligence and other emerging digital technologies, pp. 61-62.

Consultation on the White Paper on Artificial Intelligence - A European Approach

Fields marked with * are mandatory.

Introduction

Artificial intelligence (AI) is a strategic technology that offers many benefits for citizens and the economy. It will change our lives by improving healthcare (e.g. making diagnosis more precise, enabling better prevention of diseases), increasing the efficiency of farming, contributing to climate change mitigation and adaptation, improving the efficiency of production systems through predictive maintenance, increasing the security of Europeans and the protection of workers, and in many other ways that we can only begin to imagine.

At the same time, AI entails a number of potential risks, such as risks to safety, gender-based or other kinds of discrimination, opaque decision-making, or intrusion in our private lives.

The [European approach for AI](#) aims to promote Europe's innovation capacity in the area of AI while supporting the development and uptake of ethical and trustworthy AI across the EU. According to this approach, AI should work for people and be a force for good in society.

For Europe to seize fully the opportunities that AI offers, it must develop and reinforce the necessary industrial and technological capacities. As set out in the accompanying European strategy for data, this also requires measures that will enable the EU to become a global hub for data.

The current public consultation comes along with the [White Paper on Artificial Intelligence - A European Approach](#) aimed to foster a European ecosystem of excellence and trust in AI and a Report on the safety and liability aspects of AI. The White Paper proposes:

- Measures that will streamline research, foster collaboration between Member States and increase investment into AI development and deployment;
- Policy options for a future EU regulatory framework that would determine the types of legal requirements that would apply to relevant actors, with a particular focus on high-risk applications.

This consultation enables all European citizens, Member States and relevant stakeholders (including civil society, industry and academics) to provide their opinion on the White Paper and contribute to a European approach for AI. To this end, the following questionnaire is divided in three sections:

- **Section 1** refers to the specific actions, proposed in the White Paper's Chapter 4 for the building of an ecosystem of excellence that can support the development and uptake of AI across the EU economy and public administration;

- **Section 2** refers to a series of options for a regulatory framework for AI, set up in the White Paper's Chapter 5;
- **Section 3** refers to the [Report on the safety and liability aspects of AI](#).

Respondents can provide their opinion by choosing the most appropriate answer among the ones suggested for each question or suggesting their own ideas in dedicated text boxes. Feedback can also be provided in a document format (e.g. position paper) that can be uploaded through the button made available at the end of the questionnaire.

Section 1 - An ecosystem of excellence

To build an ecosystem of excellence that can support the development and uptake of AI across the EU economy, the White Paper proposes a series of actions.

In your opinion, how important are the six actions proposed in section 4 of the White Paper on AI (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Working with Member states	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Focussing the efforts of the research and innovation community	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Skills	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Focus on SMEs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Partnership with the private sector	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Promoting the adoption of AI by the public sector	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Are there other actions that should be considered?

500 character(s) maximum

The CCBE fully supports the idea that EU-level funding should be made available for sectoral regulators – including bars – as they are best positioned to address the training needs for their respective sectors – such as lawyers – particularly as regards how AI can be used in a way which is compatible with their ethical codes.

Interaction amongst all sectors, private and public, is crucial to ensuring that the ethical values are designed into the AI systems themselves. See separate CCBE response.

Revising the Coordinated Plan on AI (Action 1)

The Commission, taking into account the results of the public consultation on the White Paper, will propose to Member Plan to be adopted by end 2020.

In your opinion, how important is it in each of these areas to align policies and strengthen coordination as described in section 4.A of the White Paper (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Strengthen excellence in research	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Establish world-reference testing facilities for AI	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Promote the uptake of AI by business and the public sector	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Increase the financing for start-ups innovating in AI	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Develop skills for AI and adapt existing training programmes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Build up the European data space	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Are there other areas that that should be considered?

500 character(s) maximum

A united and strengthened research and innovation community striving for excellence

Joining forces at all levels, from basic research to deployment, will be key to overcome fragmentation and create synergies between the existing networks of excellence.

In your opinion how important are the three actions proposed in sections 4.B, 4.C and 4.E of the White Paper on AI (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Support the establishment of a lighthouse research centre that is world class and able to attract the best minds	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Network of existing AI research excellence centres	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Set up a public-private partnership for industrial research	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Are there any other actions to strengthen the research and innovation community that should be given a priority?

500 character(s) maximum

Focusing on Small and Medium Enterprises (SMEs)

The Commission will work with Member States to ensure that at least one digital innovation hub per Member State has a high degree of specialisation on AI.

In your opinion, how important are each of these tasks of the specialised Digital Innovation Hubs mentioned in section 4.D of the White Paper in relation to SMEs (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Help to raise SME's awareness about potential benefits of AI	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Provide access to testing and reference facilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Promote knowledge transfer and support the development of AI expertise for SMEs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support partnerships between SMEs, larger enterprises and academia around AI projects	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Provide information about equity financing for AI startups	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

[These points are further explained in the separate CCBE paper attached to the response of this consultation]

Are there any other tasks that you consider important for specialised Digital Innovations Hubs?

500 character(s) maximum

Section 2 - An ecosystem of trust

Chapter 5 of the White Paper sets out options for a regulatory framework for AI.

In your opinion, how important are the following concerns about AI (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
AI may endanger safety	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
AI may breach fundamental rights (such as human dignity, privacy, data protection, freedom of expression, workers' rights etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
The use of AI may lead to discriminatory outcomes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
AI may take actions for which the rationale cannot be explained	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
AI may make it more difficult for persons having suffered harm to obtain compensation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
AI is not always accurate	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Do you have any other concerns about AI that are not mentioned above?

Please specify:

500 character(s) maximum

- *AI may lead to unfair legally binding outcomes*
- *AI may hamper access to justice*
- *AI may undermine fair trial rights*

In general, the use of AI in automated decision-making processes may reshape the interaction between citizens and public/private decision-makers. This may undermine citizens' ability to seek advice, contest or reverse decisions. Therefore, robust redress mechanisms need to be ensured as well as a close involvement of actors protecting citizens' rights (e.g. lawyers and judges).

Do you think that the concerns expressed above can be addressed by applicable EU legislation? If not, do you think that there should be specific new rules for AI systems?

- Current legislation is fully sufficient
- Current legislation may have some gaps
- There is a need for a new legislation
- Other
- No opinion

Other, please specify

500 character(s) maximum

For some areas there might be a need for new legislation, whereas for others not, or only further clarifications are needed as to how existing rules apply to new circumstances resulting from the use of AI. See the CCBE's separate response for further details.

If you think that new rules are necessary for AI system, do you agree that the introduction of new compulsory requirements should be limited to high-risk applications (where the possible harm caused by the AI system is particularly high)?

- Yes
- No
- Other
- No opinion

Other, please specify:

500 character(s) maximum

Do you agree with the approach to determine “high-risk” AI applications proposed in Section 5.B of the White Paper?

- Yes
- No
- Other
- No opinion

Other, please specify:

500 character(s) maximum

No. The CCBE is concerned that an exercise of categorising risk as “high” or “low” on the basis of abstract criteria is too simplistic and will lead to structurally defective regulation. It is not appropriate to give the same legal treatment to things which are technically different, for example, artificial intelligence, the internet of things and other digital technologies, even although they sometimes share common features. A more targeted approach is called for (see attached CCBE paper).

If you wish, please indicate the AI application or use that is most concerning (“high-risk”) from your perspective:

500 character(s) maximum

- *The use of AI tools by courts in different phases, i.e. pre-trial, trial, deliberation/decision-making, and post sentencing.*
- *The use of AI tools for law enforcement purposes.*

For more explanation, reference is made to the separate CCBE paper attached to the response of this consultation.

In your opinion, how important are the following mandatory requirements of a possible future regulatory framework for AI (as section 5.D of the White Paper) (1-6: 1 is not important at all, 6 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
The quality of training data sets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
The keeping of records and data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Information on the purpose and the nature of AI systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Robustness and accuracy of AI systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Human oversight	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Clear liability and safety rules	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

In addition to the existing EU legislation, in particular the data protection framework, including the General Data Protection Regulation and the Law Enforcement Directive, or, where relevant, the new possibly mandatory requirements foreseen above (see question above), do you think that the use of remote biometric identification systems (e.g. face recognition) and other technologies which may be used in public spaces need to be subject to further EU-level guidelines or regulation:

- No further guidelines or regulations are needed

- Biometric identification systems should be allowed in publicly accessible spaces only in certain cases or if certain conditions are fulfilled (please specify)
- Other special requirements in addition to those mentioned in the question above should be imposed (please specify)
- Use of Biometric identification systems in publicly accessible spaces, by way of exception to the current general prohibition, should not take place until a specific guideline or legislation at EU level is in place.
- Biometric identification systems should never be allowed in publicly accessible spaces
- No opinion

Please specify your answer:

Biometric identification systems technologies tend have serious flaws that endanger civil rights. For example, facial recognition technology has been proven in multiple studies to be inaccurate at identifying people of different races. Also, there are grave concerns that the trigger words which are used by national security agencies are not sufficiently refined and thus the phone conversations and email correspondence of millions of people are monitored without a legal basis.

Further, the widespread use of facial recognition may pose severe risks for an open and pluralistic society if not used proportionately with a proportionate intended aim such as ensuring public safety. In many situations, anonymity is the most important safeguard of freedom, and facial recognition 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 they become.

Do you believe that a voluntary labelling system (Section 5.G of the White Paper) would be useful for AI systems that are not considered high-risk in addition to existing legislation?

- Very much
- Much
- Rather not
- Not at all
- No opinion

Do you have any further suggestion on a voluntary labelling system?

500 character(s) maximum

What is the best way to ensure that AI is trustworthy, secure and in respect of European values and rules?

- Compliance of high-risk applications with the identified requirements should be self-assessed ex-ante (prior to putting the system on the market)
- Compliance of high-risk applications should be assessed ex-ante by means of an external conformity assessment procedure
- Ex-post market surveillance after the AI-enabled high-risk product or service has been put on the market and, where needed, enforcement by relevant competent authorities
- A combination of ex-ante compliance and ex-post enforcement mechanisms
- Other enforcement system

- No opinion

Please specify any other enforcement system:

500 character(s) maximum

Do you have any further suggestion on the assessment of compliance?

500 character(s) maximum

Instead of adhering to a very generic and abstract compliance framework, the appropriate compliance measures must be considered and tailored to the needs in specific sectors and circumstances.

Section 3 – Safety and liability implications of AI, IoT and robotics

The overall objective of the safety and liability legal frameworks is to ensure that all products and services, including those integrating emerging digital technologies, operate safely, reliably and consistently and that damage having occurred is remedied efficiently.

The current product safety legislation already supports an extended concept of safety protecting against all kind of risks arising from the product according to its use. However, which particular risks stemming from the use of artificial intelligence do you think should be further spelled out to provide more legal certainty?

- Cyber risks
- Personal security risks
- Risks related to the loss of connectivity
- Mental health risks

In your opinion, are there any further risks to be expanded on to provide more legal certainty?

500 character(s) maximum

Yes, there are further risks that need to be considered as regards the use of AI in justice. In particular, AI tools must be properly adapted to the justice environment, taking into account the principles and procedural architecture underpinning judicial proceedings. In this regards, reference is made to the CCBE separate response.

Do you think that the safety legislative framework should consider new risk assessment procedures for products subject to important changes during their lifetime?

- Yes
- No
- No opinion

Do you have any further considerations regarding risk assessment procedures?

500 character(s) maximum

Do you think that the current EU legislative framework for liability (Product Liability Directive) should be amended to better cover the risks engendered by certain AI applications?

- Yes
- No
- No opinion

Do you have any further considerations regarding the question above?

500 character(s) maximum

The current legislative framework should be amended considering the fundamental differences that exist between traditional products and AI when it comes to the notions of product, fault and defect. Questions of to whom liability might be extended, the burden of proof and defences must also be reconsidered. The CCBE would, however, opt for a separate instrument on AI liability issues rather than amending the Product Liability Directive, recognised as effective in respect of traditional products.

Do you think that the current national liability rules should be adapted for the operation of AI to better ensure proper compensation for damage and a fair allocation of liability?

- Yes, for all AI applications
- Yes, for specific AI applications
- No
- No opinion

Please specify the AI applications:

Do you have any further considerations regarding the question above?

500 character(s) maximum

The CCBE is not able to comment on how the current national liability rules regarding compensation for damage and allocation of liability should possibly be adapted. However, we do believe that these aspects, including rules on the burden of proof, should be regulated at EU level and included in the reviewed Product Liability Directive (or in a separate instrument). Another approach might lead to a situation where the adapted national rules would differ significantly between the Member States.