Position Paper
on the European Commission Consultation On adapting liability rules to the digital age and AI

Brussels, 20 December 2021

This position paper accompanies the response of the Confederation of European Security Services (CoESS) to the European Commission's consultation on adapting liability rules to the digital age and Artificial Intelligence (AI).

CoESS believes that an adequate EU liability regime is the foundation of an effective uptake of AI technologies in the services industry and must be implemented in coherence with the future EU AI Act. We support a targeted revision of the EU product liability framework with strict and coherent rules, which are adapted to the specific character of a disruptive technology such as AI and create legal certainty for users of AI systems.

From the view of the security services, the integration of AI in security solutions could allow for a significant increase in performance of security processes, translating in a better protection of European citizens, critical infrastructures and the economy at large against public security threats. This integration will however only be successful if liability rules (1) provide clear responsibilities and provisions for user-liability, (2) mirror the complex liability chain in AI, and (3) do not introduce an unrealistic burden of proof on companies.

To this end, CoESS recommends future liability rules on AI to reflect the following considerations:

(I) Harmonised rules in alignment with EU AI Act

CoESS recommends to harmonise national liability rules for providing AI-enabled products and services, and the European Commission to ***assess whether the Product Liability Directive should be transformed in an EU Regulation*** to avoid fragmentation of liability rules across Europe. Member States should therefore not be allowed to maintain broader and/or more far-reaching national strict liability schemes for AI-enabled products and services. It is of utmost importance that definitions and provisions are in full alignment with the EU AI Act, but also other EU legal frameworks such as the Radio Equipment Directive 2014/53 and Cybersecurity Act (Regulation 2019/881).

(II) Risk-based approach

CoESS stresses that any liability regime would need to be carefully examined and evaluated in order to avoid negative effects, e.g. on innovation and AI uptake. Strict liability rules for AI should be

reserved for a limited number of AI-enabled products and services which impose a high material risk (e.g. life, health, property) for the public, following a risk-based and use-case focused approach.

All AI-systems with a high-risk, including their use-cases, should be exhaustively listed in an Annex of the liability regime. Systems that are not listed in the Annex should remain subject to fault-based liability. Due to the rapid technological developments in AI, such a list should be able to be amended by means of Delegated Acts.

(III) Technological neutrality and burden of proof

Persons suffering material harm from the malfunctioning of an AI system should have the same level of protection compared to cases without involvement of an AI system, following an approach of ***technological neutrality***.

CoESS agrees that in certain situations, the lack of transparency (opacity) and explainability (complexity) of AI systems could make it difficult for injured parties to prove that a product is defective or to prove fault. Therefore, it should be assessed how to ***ease the burden of proof for injured parties***.

CoESS thereby agress that the defendant (any actor along the liability chain) should be obliged to disclose necessary technical information (e.g. log data) to the injured party to enable the latter to prove the conditions of the claim. It is, however, of outmost importance to ***define "necessary technical information"*** in an appropriate way to ensure that the defendant's intellectual property rights are adequately protected. For example, the defendant should not be required to disclose the source code or the operating model of the AI system – but rather information on the input data and output data used by the AI system.

CoESS believes that, as a baseline, when any operator along the liability chain of an AI system failed to ***comply with their legal obligations as laid down in the EU AI Act***, courts should infer that the damage was caused due to that operator's fault. A prerequisite should, however, be that the injured party can prove a causal link between that fault and the damage.

In cases of complex and/or opaque and/or highly autonomous AI systems, we however stress that it would be inappropriate to shift the burden of proof from the injured party to the defendant – not even if it, in a given case, is necessary to establish how such an AI system operates in order to substantiate a claim.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

(IV) Mandatory Insurance

CoESS believes that a ***harmonised insurance obligation*** should be laid down at EU level for all operators along the liability chain for high-risk AI products and AI-based services that are covered by the liability regime.

(V) Liability Chain along front-end and back-end operators

Liability should always be with the operator controlling the risk associated with the malfunctioning of the AI system. This key principle is however challenged mostly by the complexity of the liability chain and opacity of some AI-enabled products and services:

- In the case of AI, a multitude of actors intervenes in the technology's life-cycle, making it challenging to identify who was in control of managing the risk of using the AI system (***complexity***) and creating legal uncertainty for liability.
- The capacity of some AI-enabled product for self-learning and autonomy leads to ***opacity*** and a certain "black box" element, making it impossible to trace back a malfunctioning of the system to a specific human decision in the system's design and operation. Where autonomy of the systems leads to a modification of its intended use (and consequently of what is expected by users) or safety/security-by-design features, it should be considered to require a new re-assessment of the self-learning product by the manufacturer. In addition, an update liability regime could include reinforced requirements for manufacturers on instructions of use for AI-enabled products and services covered by the text.

Against this background, it is important that a liability regime for AI-enabled products and services exists that creates legal certainty on who can be held accountable in the case of a malfunctioning of the system. For such a regime, a multitude of other factors must also be taken into account:

- ***Interconnectednes*** with other AI and non-AI systems.
- ***Dependency*** on external data.
- ***Openness*** and software updates of the system.
- ***Vulnerability*** to cybersecurity breaches.
- ***Force majeure***.

As a key principle, liability should be with the operator along the liability chain who exercises control over the risk connected with the malfunctioning of the system. There will only be few cases, where this liability can be attributed to one single operator in the liability chain, which is why the term

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

"operator" should include the entire chain from provider (backend operator providing the product, data and updates) to user (frontend operator using the AI system), including concrete definitions of such terms.

As regards '***development risk defence***' of providers, we believe that the concept should be evaluated in the face of emerging technologies. Notably, we believe that the defence should not be available for products designed to be influenced by other interconnected products or services (e.g. complex IoT systems), and for AI products that continue to learn and adapt while in operation.

Similar to Data Protection Officers, operators along the liability chain should have the obligation to ***designate an AI-liability representative***.

(VI) Logging and reporting

In order to facilitate evidence gathering in case of an incident, and to clarify the concept of "control" / "authority" over managing risks of the malfunctioning of the AI system, CoESS recommends that ***mandatory provisions*** are laid out in a liability regime on ***product traceability, logging, transparency of design parameters and input/output data, and reporting on compliance with provisions of the future EU AI Act***.

(VII) Clear factors for user-liability

Users of AI systems, as per the definition of "user" in the EU AI Act, should only be liable of a malfunctioning of an AI system if they are ***best placed to have control of the system and/or do not comply with user-relevant provisions made in Chapter 2 and 3 of the future EU AI Act*** – including provisions on operations and maintenance. The following factors should be taken into account when including provisions on user-liability:

- The user can have limited knowledge of the AI system and data being used, depending on whether the system is deployed "***under its authority***" (see next point),
- The user should ensure that only ***adequately qualified personnel*** is operating high-risk AI systems who is capable of fulfilling human oversight provisions as set out in the EU AI Act.

Users should not be held liable in a case of "***force majeure***".

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

(VIII) Include a defition of the term “authority” or “control”

A potential legal proposal must include a clear definition of ***who has control, or authority***, over the operation of the AI system. Such definition is of particular relevance for business services putting into service an AI system.

(IX) Contractual Clauses

CoESS agrees that it might be suitable to prohibit contractual clauses that completely exclude liability for damage caused by AI vis-à-vis consumers. On the other hand, the overall contractual relationship between businesses should not be subject to EU harmonisation. If contractual liability waivers in relation to businesses would be subject to EU harmonisation, such contractual clauses should only be prohibited for certain types of harm (e.g. to life, body or health) and/or for harm arising from gross negligence or intent.

(X) Definition of liability in case of immaterial harm

The EU AI Act is also focusing on immaterial harm caused by the malfunctioning of an AI system. To define adequate compensation methods and processes in case of the cause of immaterial harm, CoESS recommends the European Commission to first make an assessment of relevant liability regimes existing on this matter at national level.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu