FLI Position on adapting Non-Contractual Civil Liability Rules to Artificial Intelligence

AI Liability Directive* – Full Version

View the executive summary:

futureoflife.org/ai-liability-summary

28 November 2023

Angelica Fernandez
policy@futureoflife.org

* Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, COM(2022) 496 final, 28.9.2022 (AILD)

Contents

The Future of Life Institute (FLI) works to promote the benefits of technology and reduce their associated risks. FLI has become one of the world's leading voices on the governance of artificial intelligence (AI) and created one of the earliest and most influential sets of governance principles, the Asilomar AI Principles. FLI maintains a large network among the world's top AI researchers in academia, civil society, and private industry.

In March of this year, we released an open letter that sparked a global debate on AI safety.

Introduction

Safety and liability are intertwined concepts. Safe AI requires a coherent and strong liability framework that guarantees the accountability of AI systems. Liability affects the incentives of producers, users, and other parties susceptible to AI harms. An effective incentive structure can enhance the development of safe AI systems while protecting the rights of relevant stakeholders. Individuals should be compensated for harm caused by AI systems. At the same time, as we have advocated in the context of the EU AI Act,[1] if we are to avoid the catastrophic risks of ungoverned AI development, ex-ante requirements on safety are crucial.

There is a wide range of AI systems, all of which should be subject to liability. It is possible to develop an AI system that is too fast, complex or opaque to be effectively controlled or supervised. Providers and operators of an AI system often have control over when and how the system is designed and used, and oversee its performance in real-world scenarios. These parties also control the safety features built into the AI system prior to its market deployment and set the thresholds for tolerable risk in systems made available to the public. Furthermore, providers have a distinct informational advantage compared to operators, as they know more about, for instance, how a system was tested or on what data it was trained - knowledge that may not be passed along to the operator but which could make adverse consequences more or less likely. In such cases, providers should bear more liability than operators. The allocation of liability across the value chain of AI is influenced by various factors. Delineating liability across the value chain of an AI system is a challenge that should be addressed by the legislator. This paper addresses that challenge.

The forthcoming EU AI Act intends to mitigate some of these risks. Moreover, other legislation mitigates risks from AI systems in specific sectors (e.g. autonomous vehicles).[2] However, AI systems' decision-making autonomy can hinder developer supervision and duty of care and cause errors less predictable to humans despite *ex-ante* risk mitigation measures. These characteristics make it difficult to determine where and how a human should intervene to override or correct a decision. Neither oversight roles nor *ex-ante* risk mitigation measures can guarantee error-free AI systems. The law can help users to trust potentially risky systems by putting an effective and reliable system of redress in place to address harms if and when they materialise. This position is in line with the EU Charter of Fundamental Rights European Union values, and the High-Level Expert (HLEG AI) liability report.

1 See FLI position paper on the EU AI Act, 4 August 2021. https://futureoflife.org/document/fli-position-paper-on-the-eu-ai-act/; Brakel M and Uuk R, FLI position paper: AI Act Trilogue. https://futureoflife.org/document/fli-ai-act-trilogues/.

2 For example, in the domain of transportation, with regards to autonomous cars, the following specific regulation applies: the General Vehicles Safety Regulation, the Approval and Market Surveillance of Vehicles Regulation and the Motor Vehicles Insurance Directive.

AILD and PLD: the two prongs of the EU AI liability framework

The EU AI regulation package is broader than the AI Act alone[3]. The European Commission proposes two additional legislative instruments to shape the liability framework for AI systems: a set of non-contractual civil liability rules for AI (AILD), and a revision of the Product Liability Directive (PLD)[4], which is currently under negotiation.

The European Commission proposal on non-contractual civil liability rules for AI (AILD)[5] establishes a fault-based liability framework for all AI systems, regardless of their risk under the proposed AI Act. The AILD commends non-contractual fault-based civil liability claims for damages caused by an output, or the absence of an output, from an AI system. A fault-based claim usually requires: proof of damage, the fault of a liable person or entity, and a causal link between the two. However, AI systems can make it difficult or impossible for victims to gather the evidence required to establish this causal link. The AILD aims to make it easier for claimants in two ways. Firstly, help them to establish their claims by requiring the disclosure of relevant evidence and by mandating access, under specific circumstances, to defendants' information regarding high-risk AI systems. Secondly, lighten the burden of proof by imposing a rebuttable presumption of causality, establishing a default causal link between non-compliance with a duty of care and the AI system output or failure to produce an output that gave rise to the damage. The latter is distinct from a full reversal of the burden of proof, in which the victim bears no burden and the person presumed liable must prove that the conditions of liability are not fulfilled.

The AILD addresses the burden of proof in AI-related damage claims specifically, where other aspects of civil liability are left to national laws. By focusing on procedural aspects of liability, the AILD is consistent with a minimum harmonisation approach, which allows claimants to invoke more favourable rules under national law (e.g., reversal of the burden of proof). National laws can impose specific obligations to mitigate risks, including additional requirements for users of high-risk AI systems.

While the AILD deals with the fault of AI providers, the Product Liability Directive (PLD)[6] focuses on AI system defects. When this technology causes physical harm, property damage, or loss or corruption of data, it is possible to seek compensation from any manufacturer that integrates an AI system into another product – without the injured person having to prove the manufacturer's fault, as with any other product. Under the PLD, "manufacturers" equate to developers or producers of software, including AI systems providers within the AI Act.[7] Manufacturers can be liable for post-market changes, including software updates and machine learning. The PLD alleviates the burden of proof in complex cases, such as when there is a failure to comply with safety requirements. In cases where the claimant would face excessive

3 'A European Approach to Artificial Intelligence' (Shaping Europe's digital future) https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

4 For the proposed revision see Proposal for a Regulation of the European Parliament and of the Council on General Product Safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, COM/2021/346 final (PLD proposal); For the original text see 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 (OJ L 210, 7.8.1985, p. 29).

5 Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, COM(2022) 496 final, 28.9.2022.

6 PLD Compromise Text leaked by Contexte, 28 April 2023.

7 Recital 12 Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final, 28.9.2022.

difficulties in proving defectiveness due to technical or scientific complexity, both defectiveness and its causal link to damage can be presumed if the claimant has demonstrated that: (i) the product contributed to the damage; and (ii) it is likely that the product was defective or that the defectiveness is a likely cause of the damage.[8] It is important to note that there is no overlap with the AILD in claims brought under the PLD, which is a no-fault strict liability regime.[9]

These two legislations, the AILD and the PLD, were proposed to complement one another. However, because the AILD exclusively targets AI systems, particularly high-risk AI systems, this paper will focus on that proposal. FLI acknowledges that liability cannot be considered in isolation and that non-contractual civil liability for AI is only a part of a broader regulatory framework that includes ethical guidelines, safety regulations, and rules on contractual liability. Furthermore, the AILD proposal has a narrowly defined scope and does not affect other means of seeking redress at the national level, whether through court proceedings, non-court solutions, alternative dispute resolution, or representative actions under Directive (EU) 2020/1828 of the European Parliament and of the Council or under national collective redress schemes. Nonetheless, the AILD proposal represents a critical component in shaping the regulatory landscape surrounding the development and use of increasingly advanced AI systems and thus merits our particular attention.

AILD's shortcomings are hard to overlook. It falls short of what is expected for an effective AI liability framework in three crucial aspects. First, it underestimates the black box phenomena of AI systems and, therefore, the difficulties for claimants and sometimes defendants to understand and obtain relevant and explainable evidence of the logic involved in self-learning AI systems. This situation is particularly evident for advanced general purposes AI systems (GPAIS). Second, it fails to make a distinction between the requirements for evidential disclosure needed in the case of GPAIS versus other AI systems. In a case involving GPAIS, claimants' ability to take their cases to court and provide relevant evidence will be severely undermined under a fault-based liability regime. Third, it does not acknowledge the distinct characteristics and potential for systemic risks and immaterial harms stemming from certain AI systems. It's time to acknowledge these shortcomings and work towards enhanced effectiveness (an effective possibility for parties to access facts and adduce evidence in support of their claims) and fairness (implying a proportionate allocation of the burden of proof).

To remedy these points, FLI recommends the following:

8 "A product shall be considered defective when it does not provide the safety an average person is entitled to expect or that is required under Union or national law" Art. 6 PLD Compromise text.

9 Recital 9 PLD proposal, ibid.

Strict liability for GPAIS to encourage safe innovation by AI providers.

FLI recommends a strict liability regime[10] for general-purpose AI systems (GPAIS). Strict or no fault-based liability will account for the knowledge gap between providers, operator of a system, claimants, and the courts. It will also address the non-reciprocal risks created by AI systems. This model will incentivise the development of safer systems and placement of appropriate guardrails for entities that develop GPAIS (including foundation models), and increases legal certainty. Furthermore, it can protect the internal market from unpredictable and large-scale risks.

Given their emergent capabilities, unpredictable outputs, potential for instrumental autonomous goal development, and low level of interpretability, GPAIS should be explicitly included in the scope of the AILD. Because GPAIS creates non-reciprocal risks even if the desired level of care is attained, only strict liability is sufficient to incentivise a reduction of harmful levels of activity.[11]

To clarify the scope of our proposal it is important to understand that we define GPAIS as "An AI system that can accomplish or be adapted to accomplish a range of distinct tasks, including some for which it was not intentionally and specifically trained."[12] This definition underscores the ability of a GPAIS to accomplish tasks beyond its specific training. It includes unimodal (e.g., GPT-3 and BLOOM) and multimodal (e.g., stable diffusion, GPT-4, and Dall-E) systems, and systems at different points of the autonomy spectra, with and without humans in the loop.[13] It is worth noting that the AI Act, in its current stage of negotiation, seems to differentiate between foundation models and GPAIS. For the sake of clarity, we refer to "General purpose AI systems" as a future-proof term that encompasses the terms "foundation model", and "generative AI". It provides legal certainty for standalone (deployed directly to affected persons) and foundational GPAIS (provided downstream to deployers or other developers). Moreover, we classify GPAIS as above a 10^23 FLOPS threshold, which brings into scope currently deployed AI systems such as Megatron Turing MLG, Llama 2, OPT-175B, Gopher, PanGu Sigma, AlexaTM. Falcon, and Jurassic-1 Jumbo, among others. Furthermore, GPAIS can be used in high-risk use cases, such as the dispatching of first response services, or the recruitment of natural persons for a job. These cases are under the scope of high-risk AI systems.[14] However GPAIS serves a wide range of functions not regulated by Annex III of the AI Act but presenting serious risks. For example, GPAIS can be used to develop code or

10 "A strict liability rule not only induces the optimal level of care but the optimal activity level as well. If an activity is inherently risky, even despite efficient precautions, we may want to refrain injurers from engaging in this activity altogether (or, at least, to reduce the level of this activity).179 A fault-based regime does not achieve this, since an injured can avoid paying for the costs of her activity by taking the required level of care. This explains why most jurisdictions impose strict liability for driving a car, for instance. In certain contexts, AI applications could also cause serious harm, even if proper precautions are taken, e.g. because the AI cannot be trained on sufficiently rich data." Buiten, Miriam and de Streel, Alexandre and Peitz, Martin, EU Liability Rules for the Age of Artificial Intelligence, CERRE Report, March 2021, p.40

11 Lior A, AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy, 46 Mitchel Hamline Law Review, 2020.

12 Gutierrez, C.I., Aguirre, A., Uuk, R. et al. A Proposal for a Definition of General Purpose Artificial Intelligence Systems. DISO 2, 36 (2023). https://doi.org/10.1007/s44206-023-00068-w

13 The term GPAIS also encompasses systems with "emergent" abilities, meaning new and surprising abilities that manifest at threshold levels of model parameter count and/or training computation. See J. Wei et al., "Emergent abilities of large language models," arXiv preprint arXiv:2206.07682, 2022; D. Ganguli et al., "Predictability and surprise in large generative models," 2022, pp. 1747–1764.

14 As per Art. 6(2) of the AI Act EC proposal.

create weapons, as acknowledged by the Hiroshima process.[15]

There are three compelling reasons for adding strict liability to both high-risk AI systems and GPAIS:

1. Strict liability prevents informational asymmetries in disclosure rules for GPAIS cases, guaranteeing redress and a high level of consumer protection.

This recommendation aligns with the opinion of the Expert Group on Liability and New Technologies[16] and the Parliament's own initiative resolution from October 2020.[17] It is also the option preferred in the Commission's public consultation.[18] The Commission expressed these preferences in the Explanatory Memorandum accompanying the AI Liability Directive proposal.[19] Yet it then chose an approach that assigns a fault-based liability framework for high-risk systems. This decision significantly degrades the level of consumer protection and simultaneously increases the burden on claimants to often unrealistic and untenable levels.

From a consumer perspective, what matters most is access to an effective accountability scheme, regardless of the type of AI systems that caused the harm. A fault-based framework, as the European Commission has presented it, presumes that the claimant (i.e., consumer) needs to prove the causal link for fault, which, given the informational asymmetries mentioned above, is often extraordinarily difficult and sometimes impossible.[20] Requiring proof without the technical or legal means to provide that proof undermines the effectiveness of the right to compensation, given the superior knowledge AI corporations and developers are bound to have.

In a claim concerning an AI system, the claimant should be required to explain neither the AI system's specific, proprietary, and inordinately complex characteristics, nor how such characteristics link to the damage. As GPAIS have the most advanced capabilities, they present a diverse range of potential and sometimes unpredictable harms. Consumers should be able to immediately presume that if they are harmed by the use of those systems, they are protected and will be compensated. This assurance is only possible in a strict liability scenario for GPAIS.

2. The necessary level of care to safely deploy a GPAIS is too complex for the judiciary to determine, leading to a lack of legal certainty for all economic actors in the market.

For cases related to GPAIS, the necessary level of care and the acceptable level of risk may be difficult to determine in view of the rapidly evolving nature of AI capabilities. Presently, the judiciary, which may lack technological and risk knowledge compared to developers and

15 OECD,'G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI 2023.

16 European Commission, Directorate-General for Justice and Consumers, Liability for artificial intelligence and other emerging digital technologies, Publications Office, 2019. https://data.europa.eu/doi/10.2838/573689.

17 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html.

18 Commission Staff Working Document, Impact Assessment Report accompanying the document Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, SWD(2022) 319 final, 28.9.2022. https://ec.europa.eu/info/sites/default/files/1_4_197608_impact_asse_dir_ai_en.pdf.

19 Explanatory Memorandum of the AILD.

20 For a procedural law perspective on the admissibility of evidence in courts regarding AI systems cases, see Grozdanovski, Ljupcho. (2022). L'agentivité algorithmique, fiction futuriste ou impératif de justice procédurale ?: Réflexions sur l'avenir du régime de responsabilité du fait de produits défectueux dans l'Union européenne. Réseaux. N° 232-233. 99-127. 10.3917/res.232.0099; Grozdanovski, Ljupcho. (2021). In search of effectiveness and fairness in proving algorithmic discrimination in EU law. Common Market Law Review. 58. 99-136. 10.54648/COLA2021005.

manufacturers, would ultimately determine both of these levels, leading to a lack of legal certainty. GPAIS opacity challenges the basic goal of legal evidence, which is to provide accurate knowledge that is both fact-dependent and rationally construed. This barrier triggers myriad procedural issues in the context of GPAIS that are not resolved by the mechanisms established in Art. 3 and 4 AILD. Moreover, assessment by the judiciary is complicated by the lack of commonly accepted standards for appropriate care and risk levels for deploying GPAIS, further contributing to the uncertainty of future judicial findings.[21]

This difficulty is related to the lack of clear thresholds that one could use to distinguish between "safe" and "unsafe" GPAIS, the lack of standards on risk mitigation measures for high-risk AI systems and GPAIS, and the fact that current scientific and technical knowledge cannot anticipate the autonomous self-learning capabilities of future AI systems.

Strict liability for GPAIS is a useful lever to control uncertain technological risk because there is no need for in-depth knowledge of the optimal level of care.[22] This will benefit judges and regulators who need to assess whether a system caused damages, as well as providers and claimants who can more reliably predict the conduct and findings of the court. It is often argued that this is not new, as judges have to face cases involving complex technology, for example, in the case of patent disputes. In such cases, they generally rely on external technical experts to explain the workings of the relevant technology. However, in the case of GPAIS, even experts in machine learning would struggle to explain how certain complex systems function or why a particular output was or was not produced, as interpretability of large-grown neural models is lacking in both theory and practice.

3. Disclaimers on liability issues and a lack of adequate information-sharing regimes between upstream and downstream developers place a disproportionate compliance burden on downstream developers using GPAIS.

In the absence of a liability regime to create the right incentives for the deployment of safe systems and models, the frequent use of GPAIS (which includes foundation models) often leads to significant downstream risks. 'Downstream' refers to numerous actors in the value chain: (i) providers, who modify base models, substantially or not, and (ii) operators, which include importers, authorized representatives, and importers of an AI system. We take 'upstream' to mean the original developers of GPAIS. For the sake of consistency Recital 15 AILD retains the AI Act definitions, for AI systems, providers, and users. The comparison table below clarifies some of these terms:

21 Generally speaking, when any artificial intelligence-based information system is implemented, there should be computer literacy programmes for users and debates involving professionals from the justice system, in line with 5 agreed principles for the use of AI in Judicial systems. See European Commission for the Efficiency of Justice (CEPEJ), 'European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment' (Council of Europe, February 2019) https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

22 Hacker, Philipp, The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future (November 25, 2022). Available at http://dx.doi.org/10.2139/ssrn.4279796

Table 1: Comparing entity defintions in the AI Act proposal with the AILD proposal.

Legal definition	AI Act proposal	AILD proposal
Provider	A natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge. (Art.3(2) AI Act (EC Proposal)).	A provider is a "person subject to the obligations of a provider" (Art 3 AILD). In the context of the AILD, providers are legal persons or natural persons subject to the obligations under the AI Act, particularly Chapter 2 and 3 of Title III for high-risk AI systems, as the AILD refers to them in that context.
User	Any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal nonprofessional activity; Also called a deployer in the Parliament's proposed version of the Act.	Same meaning as in the AI Act as per Art. 2(3) AILD.
Operator	The provider, the user, the authorized representative, the importer and the distributor.	Not explicitly defined but to be interpreted in the same meaning as in the AI Act, as per Recital 15 AILD.

Depending on the final AI Act text, all upstream foundation models, regardless of their capabilities, may have to comply with certain *ex-ante* transparency obligations, including documenting training processes, providing information downstream, undergoing model evaluation and internal red teaming, and enabling downstream testing of their models.[23] However, depending on the use case, downstream providers do not necessarily have the same *ex-ante* requirements as upstream providers, even though their applications built on top of an upstream foundation model can inflict harm at scale. The inclusion of GPAIS in the scope of the AILD will help to level the playing field for small and medium-sized enterprises (SMEs) by more evenly spreading the incentives and risks of delivering better and safer products. This approach eliminates the need for SMEs to shoulder an extra burden of compliance when operating in the market and reduces the legal uncertainties they face when adopting AI in the EU because they are able to republish or produce in court disclosures from upstream providers regarding the risks and properties originating upstream.

As many of the world's developers of GPAIS are non-European,[24] European SMEs are mostly considered downstream providers of GPAIS. They could be disproportionately affected by a fault-based liability framework and face claimants when an accident occurs. Currently, there are no clear legal avenues for these economic actors to share the burden of liability with GPAIS providers or, at a minimum, obtain clear information from the GPAIS provider on why, for example, systems might have produced harmful outputs.

23 Luca Bertuzzi, 'Spanish Presidency Pitches Obligations for Foundation Models in EU's AI Law' (www.euractiv.com, 7 November 2023) https://www.euractiv.com/section/artificial-intelligence/news/spanish-presidency-pitches-obligations-for-foundation-models-in-eus-ai-law/ accessed 24 November 2023.

24 The main GPAIS providers are Meta, Google, Anthropic, Inflection AI and Open AI. Mistral AI and Aleph Alpha are the only two European companies developing GPAIS. For a detailed overview of the landscape of major AI corporations developing GPAIS, including foundation models, see UK Competition & Market Authority, AI Foundation Models: Initial Report, 18 September 2023.

Disclosure of evidence rules such as those established in the AILD are intended to help claimants identify a liable actor. However, this is a complex task if there is no clarity on the allocation of responsibilities along the value chain. Information-sharing regimes between upstream and downstream providers illustrate this complexity. While protecting confidential information and business trade secrets, information-sharing obligations should be sufficiently transparent to ensure court-ordered evidence disclosures can assign liability to the correct actor. To ensure a fair apportionment of liability and risk, there should be a clear delineation regarding outputs, or the failure to produce outputs, that led to harm in a claim for damages, and whether they can be traced back to GPAIS, particularly where these are controlled by different legal entities.

Currently, no such information-sharing requirements between GPAIS providers and downstream providers exist. Improving information-sharing regimes on foundation models is a negotiation point of the AI Act. There will potentially be an obligation to draw up and make available certain information to providers of AI systems who intend to integrate foundation models in their AI systems. However, diminishing the informational asymmetry depends on the quality of the information being disclosed, the frequency of these disclosures, the nature of the disclosure (voluntary or mandated) and the extent to which providers of GPAIS have enough meaningful information from the pre-training of models that can be shared, given the black box effect of model training.

Information-sharing is key because injured parties are often at a significant disadvantage compared to AI developers in terms of access to, and understanding of, information on how an output was produced and how a system operates. This information asymmetry can undermine the fair apportionment of risk. Our research into the terms and conditions of the main AI providers shows that other than mechanisms for voluntarily reporting incidents or bugs between these two links of the value chain, the main providers of GPAIS do not envisage any particular information-sharing regime that could simplify the disclosure of evidence requirements in a liability case.[25] For example, in the context of ChatGPT, OpenAI would be the foundation model developer *and* the GPAIS developer, whereas it would only be the former, in the context of Microsoft's Bing, a GPAIS built on top of OpenAI's GPT-4 foundation model. There should be appropriate liability redress mechanisms to enable downstream providers to seek compensation from upstream providers when held liable for damages. This is particularly critical in light of the informational and resource imbalances between large upstream and smaller downstream providers.

When it comes to information sharing, AI corporations appear to be attempting to absolve themselves of liability once a technology is released to other actors in the supply chain. Annex I of this paper shows the extent to which main GPAIS providers insert limitation of liability clauses in their terms and conditions, even while knowing such voluntary exemptions are not always enforceable. For example, Open AI model cards warn against some of these risks:

25 FLI (2023), Can we rely on information sharing? (Blogpost) available at https://futureoflife.org/ai-policy/can-we-rely-on-information-sharing/.

> "Known risks associated with smaller language models are also present with GPT-4. GPT-4 can generate potentially harmful content, such as advice on planning attacks or hate speech. It can represent various societal biases and worldviews that may not be representative of the user's intent, or of widely shared values. It can also generate code that is compromised or vulnerable. The additional capabilities of GPT-4 also lead to new risk surfaces."[26]

Additionally, OpenAI acknowledges that more research is needed to understand the risks related to the newer capabilities of their systems. Sophisticated AI systems like GPT-4 are thus deployed into the market with a considerable risk profile that is known by the provider. It is currently unclear to what extent an average user is informed and cautious in their use of these systems, as there are many cases of AI systems harming users.[27] FLI asserts that knowledge of material risk should be a standard to allocate liability to GPAIS providers.

Reflected in the table below are some of our findings on the terms and conditions of major GPAIS providers, which indicate additional information-sharing shortcomings between upstream and downstream developers and between the average user and these entities.

Table 2: Mapping Terms of Use conditions from major general-purpose AI developers which would apply to downstream companies.

	OpenAI [Terms of Use]	**Meta** [AIs Terms of Service]	**Google** [API Terms, Google Terms]	**Anthropic** [Terms of Service]	**Inflection AI** [Terms of Service]
Services provided "as is", meaning the user agrees to receive the product or service in its present condition, including any faults, even if not immediately apparent.	✓	✓	✓	✓	✓
Disclaiming any warranties, including as to quality, reliability, or accuracy.	✓	✓	✓	✓	✓
Developer not liable for most types of damages, sometimes even if they are foreseeable.	✓	✓	✓	✓	✓
Limiting liability to $200 (or less) or the price paid by the user.	✓		✓	✓	✓

26 GPT-4 System Card, 23 March 2023. https://cdn.openai.com/papers/gpt-4-system-card.pdf p. 3.

27 "According to the AIAAIC database, which tracks incidents related to the ethical misuse of AI, the number of AI incidents and controversies has increased 26 times since 2012. Some notable incidents in 2022 included a deepfake video of Ukrainian President Volodymyr Zelenskyy surrendering and U.S. prisons using call-monitoring technology on their inmates. This growth is evidence of both greater use of AI technologies and awareness of misuse possibilities." Nestor Maslej, Loredana Fattorini, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Helen Ngo, Juan Carlos Niebles, Vanessa Parli, Yoav Shoham, Russell Wald, Jack Clark, and Raymond Perrault, "The AI Index 2023 Annual Report," AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, April 2023.

Contractual derogations, as the ones found in every term of service and use for GPAIS, lower the standard for consumer protection and should not be allowed. The affected parties of this behaviour are not only the "average consumer,"[28] but also downstream providers, often SMEs, using GPAIS products. For these reasons, EU legislators should place *ex-ante* requirements on GPAIS providers in the AI Act and also allow liability regardless of fault through the AILD. This shift will strengthen overall AI regulation in the EU by increasing the incentive for providers (*ex-ante* and *ex-post*) to release only market-safe products.

The importance of a strict liability regime for GPAIS depends partly on the level of scrutiny to which these providers will be subject by the agreed version of the AI Act. Low level requirements could mean that downstream operators such as SMEs will face a heavier burden, as they will become the main target of liability claims for products for which they are not the main developer of, for which they lack information about, and for which there is no clear safety standard. The AI Act may include strict requirements for GPAIS. But if those requirements do not create the right incentives to deploy safe systems, meaningful liability regulation becomes even more crucial.

RECOMMENDATIONS:

- Specify in Art. 1(1)(a) of the AILD that the Directive will be applicable to GPAIS, whether or not they would otherwise qualify as high-risk AI systems.
- Include GPAIS in the definitions in Art. 2 of the AILD, and clearly define GPAIS that will be subject to strict liability.
- Add a provision to the AILD establishing strict liability for GPAIS.
- Establish a joint liability scheme between upstream and downstream developers and deployers. In order to ensure consumers are protected, all parties should be held liable jointly when a GPAIS causes damage, with compensation mechanisms allowing the injured person to recover for the total relevant damage. This is in line with Art. 11 and 12 of the PLD compromised text.
- Specify that knowledge of a potential harm should be a standard when allocating responsibility to the different links of the value chain, whether it has occurred or not. Model cards on AI systems should be used as an indication of the knowledge of harm a GPAIS provider has upon the deployment of their system, to allocate risk.
- Clearly link the forthcoming AI Act obligations on information sharing to GPAIS in the AILD as a way of reducing informational asymmetries between (potential) claimants and AI developers.
- Specify that neither contractual derogations nor financial ceilings on the liability of an AI corporation providing GPAIS or high-risk AI systems are permitted. The objective of consumer protection would be undermined if it were possible to limit or exclude an economic operator's liability through contractual provisions. This is in line with Recital 42 of the PLD proposal.

28 The "average consumer" is often presumed to be a "reasonably well informed and reasonably observant and circumspect" consumer. This derives from Case C-210/96 Gut Springenheide and Tusky v Oberkreisdirektor des Kreises Steinfurt [1998] ECR I-4657, para. 31.

Include commercial and non-commercial open-source[29] AI systems in the AILD to encourage a strong and effective liability framework.

FLI urges the EU legislators to include commercial and non-commercial open-source AI systems under the liability framework of the AILD.

The term "open source" is being applied to vastly different products without a clear definition.[30] The business model of some AI systems labelled as open source is also unclear. Finally, there is no consensus on which elements can be determined to characterise commercial or non-commercial open source in this new regulatory landscape.

Weights for foundation models that are widely available, such as those that are publicly posted on the Internet, present substantial security risks. For instance, anyone with access to the model weights can remove security safeguards within the model and then leverage the unprotected model to automate the infliction of harms. These harms can range widely in impact. This is as much the case with non-commercial open-source AI systems as it is for their commercial counterparts.

Open-source AI systems are not directly addressed in the scope of the AILD. There are three crucial reasons to change this, and include both commercial and non-commercial open-source AI systems under the AILD's liability framework, regardless of whether they are considered GPAIS or narrow AI systems.

1. Unlike with traditional software, there is no clarity of what 'open source' means in the context of AI. This introduces loopholes for unsafe AI systems to be deployed, using the banner of 'open source' to shield them from regulatory scrutiny.

Open source AI systems are a popular and an increasingly common feature of the GPAIS market. Often the idea of source AI systems is confused with that of open source software. The two are different. As a result, liability with regard to these systems should be discussed and explicitly introduced in the scope of the AILD.

As indicated before, the AILD is linked to the PLD. FLI is concerned that the exemption in the PLD could set a worrisome precedent that may exclude open source AI systems from liability in the AILD framework. As of November 2023, the current version of the PLD compromise text, which will be used to start the trialogue, highlights that the scope of the PLD "shall not apply to free and open-source software unless such software is offered in exchange for a price or for personal data not exclusively used for improving the security, compatibility or interoperability of the software." Similar wording is also to be found in the initial text presented by the European

29 For ease of understanding the term "open-source" is used as a colloquial term to refer to models with public model weights. As briefly discussed in this paper, so-called open-source AI systems don't actually provide many of the benefits traditionally associated with open-source software, such as the ability to audit the source code to understand and predict functionality.

30 Widder, David Gray and West, Sarah and Whittaker, Meredith, Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI (August 17, 2023). http://dx.doi.org/10.2139/ssrn.4543807.

Commission.[31] In both versions of the PLD text, non-commercial open-source software (e.g., AI systems developed in an academic setting or by non-profits) is excluded from the product liability framework, even though it entails considerable and even catastrophic risks of misuse by malicious actors.

The specific risk and safety characteristics of AI should translate into a higher standard being required for deploying these products in the market. Some systems, such as life-sustaining medical devices, entail an especially high risk of damage to people and, therefore, demand exceptionally high safety expectations. Likewise, any AI system that can be used in sensitive downstream applications demands a high bar of safety. Any exemption for open source must be carefully reviewed. It must take into account, inter alia, the objective characteristics, the properties of the product in question, and the specific requirements of the group of users for whom the system product is intended.

Finally, there is no clarity on the business model of some open-source AI systems and no consensus on which elements can be used to determine the commercial or non-commercial nature of open source AI systems in this new regulatory landscape.[32] For these reasons, including labeled open source AI systems[33] could introduce loopholes such that unsafe AI systems are deployed under the banner of non-commercial open source to avoid regulatory scrutiny.

2. Deploying AI systems under an open-source license poses irreversible security risks and enables misuse by malicious actors. This compromises the effectiveness and legal certainty of the whole AI liability framework.

The decentralized control of open-source systems means that any misuse or unintended consequences that arise will be extremely challenging, if not impossible, to cut off by the upstream provider. There is no clear mechanism to control the open distribution of high-risk capabilities in the case of advanced AI systems and models once they are distributed or deployed. This will not be the case in a closed-source and closed-weights AI system working on the basis of licensing, as the provider can enforce and update guardrails and revoke access upon evidence of misuse. In the context of scalable, unpredictable, opaque, and autonomous systems, the EU legislator cannot dismiss this potential for misuse and unintended consequences. FLI is not opposed to licensing schemes exempting certain uses within the liability framework, such as use for exclusively academic purposes. However, a blanket exemption on all "open-source" AI systems should be avoided. Moreover, artificial distinctions on the commercial and non commercial nature of these systems upon which different legal obligations might be placed is also inadvisable.

---

31 Recital 13 of the European Commission Proposal of the PLD already indicates that: "[The product liability framework] should not apply to free and open-source software developed or supplied outside the course of a commercial activity. This is, in particular, the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable, and redistributable."

32 Different proposals on defining open source are on the table. For example, the Open Source Initiative (OSI) is leading a process to get an evidence-based consensual definition. They are discussing contentious issues like whether potentially sensitive training data should be made open and whether restricting the use of these open source models to specific areas such as 'ethical' domains is acceptable under the banner of 'open source,' or not. It is clear from this process and others, that the traditional definition of open source, applicable to software does not currently cover AI. See Widder, David Gray and West, Sarah and Whittaker, Meredith, Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI (August 17, 2023). http://dx.doi.org/10.2139/ssrn.4543807; Elizabeth Seger, Noemi Dreksler, Richard Moulange, Emily Dardaman, Jonas Schuett, K. Wei, et al., Open-Sourcing Highly Capable Foundation Models: An Evaluation of Risks, Benefits, and Alternative Methods for Pursuing Open-Source Objectives, Center for the Governance of AI, 29 September 2023.

33 By labeled open source, we refer to the practice of calling open source commercial AI systems for marketing and other purposes but without giving the community the same access that traditionally is expected from open source software.

3. If open-source AI systems are allowed to be deployed in the market without being subject to the same rules as other systems, this would not only create an unequal playing field between economic actors but also devoid the AI liability framework of its effectiveness.

If open-source AI systems are allowed to be deployed in the market without being subject to the same rules as other systems, this would not only create an unequal playing field between economic actors but also devoid the AI liability framework of its effectiveness. Branding a system as open-source to escape liability is already a market dominance strategy of some tech behemoths.

By going the route of explicitly including all open-source AI systems in the AILD framework, this *ex-post* framework would contribute indirectly to the enforcement of AI Act provisions on risk mitigation, as well as the application of sectoral product safety regulation that intersects with the products under the scope of the EU AI Act.

RECOMMENDATIONS:

- Explicitly include in the scope of the AILD both commercial and non-commercial open-source AI systems.
- Define the elements to be considered commercial open-source AI systems, in collaboration with the open-source AI community and civil society stakeholders, so as to enhance the legal certainty of economic operators. For example, even though Llama 2 is not generally sold and its source code was not released, it is a commercial open source system. Llama 2 model poses a serious risk for misuse due to its wide availability and advanced capabilities. Therefore, whether their systems are open source or not, GPAIS providers such as Meta should not be exempt from liability vis-à-vis the products they release into the market.
- Carefully review and justify based on evidence if exemptions for open source are needed. If yes, explicitly address non-commercial open-source AI systems exemptions, in line with other EU law instruments. For example, through licensing agreements, there could be a limited exemption in the liability framework for exclusively academic researchers, so long as they do not proliferate the liability-emitting artefacts to third parties and there are obligations to subject these systems to rigorous physical and cybersecurity access controls to prevent the deliberate or accidental leaking or proliferation of model weights. They should also be subject to external audits, red-teaming, and information-sharing obligations.
- Subject to rigorous physical and cybersecurity access controls all non-commercial open-source models over a certain threshold, or those which exhibit emergent capabilities. This will prevent the deliberate or accidental leaking or proliferation of model weights. These non-commercial open-source models should also be in the scope of external audits, red-teaming, and information-sharing obligations.

Establish a fault-based liability with reversed burden of proof for non-general purpose high-risk AI systems.

FLI agrees with the AILD proposal that some high-risk AI systems should fall under a fault-based liability regime. This will be the case of non-general purpose high risk AI systems.[34] However, the presumption of fault should lie on the provider of an AI system. This would ease the burden for claimants and facilitate their access to justice by minimising information asymmetry and transaction costs. Providers of AI systems can rebut this presumption of fault by proving their compliance with and observance of the required level of care, or by the lack of a casual link between the output and the damage. Non-compliance liability[35] relies on the AI Act as the "backbone" of AI safety legislation for the liability framework.

As acknowledged by the Commission, several specific characteristics of AI can make it difficult and costly for injured parties to identify and prove the fault of a potentially liable entity in order to receive compensation.[36] As mentioned earlier harmed individuals are subject to significant information asymmetry with respect to the AI systems they interact with because they may not know which code or input caused harm. The interplay between different systems and components, the multitude of actors involved, and the increasing autonomy of AI systems adds to the complexity of proving fault.[37] Liability, in this case, will be placed on the AI developer, which is the party that can reduce harm at the lowest cost.

FLI believes that a fault-based liability regime with a reversed burden of proof for non general purpose high-risk AI systems is a sufficient and balanced approach. Following the risk-based approach of the AI Act, it seems sensible to have less stringent requirements than strict liability for these AI systems, which do not necessarily exhibit the self-learning and autonomous capabilities of GPAIS. Moreover, these systems are defined narrowly in Annex III and will be subject to rigorous requirements under the AI Act.

This recommendation goes beyond a rebuttable presumption of fault of the operator as suggested by the European Parliament.[38] However, it encourages compliance with the obligations established under the AI Act, reinforcing *ex-ante* safety requirements while providing more flexibility to AI developers than a strict liability framework. Furthermore, opting for a reversed burden of proof reinforces the close relationship between product safety rules and liability rules. A breach of standardised safety requirements under the AI Act should prompt a presumption of fault under Art. 3(5) AILD for high- and low-risk AI. This presumption already exists in the PLD proposal, as non-compliance with product safety legislation triggers liability. Therefore, explicitly including it in the AILD would reinforce the coherence of the AI package regulation.

34 As indicated before GPAIS will be subject to strict liability.

35 Wendehorst, C. (2022). Liability for Artificial Intelligence: The Need to Address Both Safety Risks and Fundamental Rights Risks. In S. Voeneky, P. Kellmeyer, O. Mueller, & W. Burgard (Eds.), The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives (Cambridge Law Handbooks, pp. 187-209). Cambridge: Cambridge University Press. doi:10.1017/9781009207898.016

36 Characteristics such as autonomous behaviour, continuous adaptation, limited predictability, and opacity. European Commission (2021), Civil liability – adapting liability rules to the digital age and artificial intelligence, Inception Impact Assessment. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules- to-the-digitalage-and-artificial-intelligence_en.

37 Buiten, Miriam and de Streel, Alexandre and Peitz, Martin, EU Liability Rules for the Age of Artificial Intelligence (April 1, 2021). Available at SSRN: https://ssrn.com/abstract=3817520 or http://dx.doi.org/10.2139/ssrn.3817520; Zech, H. Liability for AI: public policy considerations. ERA Forum 22, 147–158 (2021). https://doi.org/10.1007/s12027-020-00648-0.

38 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html.

RECOMMENDATIONS:

- Include a reversed burden of proof when there is non-compliance with the AI Act safety requirements. In accordance, modify Art 3 (1) AILD.
- Establish a clear distinction between non-general purpose high-risk AI systems (also sometimes referenced to as high-risk narrow AI systems) and GPAIS in the AILD.
- Create a mechanism that aligns the AI Act regulatory authorities, such as the AI Office, with the liability framework. For example, regulatory authorities under the AI Act could also become a "one-stop shop" for AI providers, potential claimants, and lawyers seeking to obtain evidence on high-risk systems and their compliance with their duty of care under the AI Act. They will be placed advantageously to assess prima facie the level of compliance of a given high-risk AI system and support potential claimants' evidence requests. This "one-stop-shop" mechanism could mirror some of the features of the mechanisms under GDPR that allow for cross-border enforcement cooperation between data protection authorities.

Protect the fundamental rights of parties injured by AI systems by including systemic harms and immaterial damages in the scope of the AILD.

FLI calls for the harmonisation of compensable damages across the EU and the inclusion of immaterial and systemic harms. This recommendation is without prejudice to the liability frameworks from EU Member States and the minimum harmonisation approach that the AILD aims to achieve. FLI argues that: (a) Immaterial and systemic harms stemming from AI systems should be in the scope of recoverable damages; and (b) In order to ensure consistent protection of fundamental rights across Member States, immaterial, societal, and systemic harms produced by an AI system should be defined by EU law and not by national laws.

Civil liability rules play a vital function in ensuring that victims can claim the compensation they deserve. By guaranteeing effective compensation, these rules protect the right to an effective remedy and a fair trial.[39] In the context of AI, they should also provide an effective remedy to AI-specific risks that have materialised. In this sense, civil liability rules serve to protect fundamental rights such as the right to life (Article 2 ChFR), the right to physical and mental integrity (Article 3 ChFR), the right to property (Article 17 ChFR), the right to a private and family life (Article 7 ChFR), and the rights to equality (Article 20 ChFR) and non-discrimination (Article 21 ChFR). These rights have a collective dimension that should be reflected in the EU's liability rules.

Addressing "systemic risk" and, by extension, societal-level harms, is not a new concept for the EU legislator,[40] as it has been addressed in the context of the Digital Services Act (DSA).[41] Some of the risks that AI poses are relatively small or unlikely on a per-incident basis, but together can aggregate to generate severe, impactful, correlated, and adverse outcomes for specific communities or for society as a whole. Adding a systemic risk dimension to the proposed liability framework in the AILD thereby reflects fundamental rights considerations.

First, Art. 34 DSA broadly classifies systemic risks into three categories, pertaining to: the dissemination of illegal content; the exercise of fundamental rights (such as dignity, respect for private and family life, the protection of personal data, freedom of expression); and public health and national security. Furthermore, the DSA specifies that risks can arise from the design and operation of a service, as well as from the malicious behaviour of users, whether they are individuals or institutional actors. The DSA's approach is evidence that the rationale behind the inclusion of systemic risk is heavily anchored to scale - understood as the number of individual users that could be harmed and the role that a service can play in the economy.[42] These two criteria fit seamlessly in the context of AI systems, particularly GPAIS, which are increasingly shaping critical domains, and that are used by an increasing number of users. FLI argues that, as in the context of the DSA, it should be similarly assumed from the known

39 Article 47 of the EU Charter of Fundamental Rights (ChFR).

40 Interestingly, Recital 12 of the AILD acknowledges systemic risks under the DSA framework.

41 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, p. 1–102.

42 Broughton Micova S and Calef A, Elements for effective systemic risk assessment under the DSA, 20 July 2023. https://cerre.eu/publications/elements-for-effective-systemic-risk-assessment-under-the-dsa/.

characteristics and capabilities of high-risk AI systems and GPAIS that there are systemic risks to their deployment and use.

This assumption is also grounded in the statements of leading AI corporations themselves, which caution against foreseeable risks in their model cards. For example, OpenAI identified that GPT-4 poses risks of "disinformation and influence operation," "[loss of] privacy," and "proliferation of conventional and unconventional weapons", among others. Moreover, "Risk to democratic processes" and "electoral processes" are often noted in EC policy documents and within the framework of the DSA.[43]

Example of immaterial harms:
Just two days before the Slovakian elections, an audio recording surfaced in which the leader of the Progressive Slovakia party is heard plotting to rig the election. The audio recording was later confirmed to be a 'deepfake', having been fabricated or manipulated using AI. [44]Here, the harm caused by the AI is systemic. No individual person suffered material damage, but the democratic process was manipulated and public trust was eroded.

Along with systemic harms, we also propose that immaterial harms (also referred to as "non-material harms" or "non-material damages") be covered within the scope of the AILD. Immaterial harms refer to harms that are challenging to quantify in monetary terms, as the damage itself is of a "qualitative" nature and not directly related to a person's physical health, assets, wealth, or income. Covering immaterial harms is necessary to account for the particular nature of damages caused by AI systems, including "loss of privacy, limitations to the right of freedom of expression, human dignity, [and] discrimination for instance in access to employment."[45] It is reasonable to consider that risks associated with AI systems can quickly scale up and affect an entire society. However, the proposed Directive leaves it up to Member States to define the damages covered. This could mean that a person discriminated against by a credit-scoring AI system could claim damages for such discrimination in one Member State, but not in another.

Including immaterial damages under the scope of the AILD also harmonises what constitutes damage by an AI system and avoids fragmentation of the level of protection to users across the EU. The Commission's PLD proposal includes a harmonised definition of what constitutes damage, even though it does not include immaterial damage.[46] This means that people harmed by defective products will enjoy uniform protection across the EU, while the protection of people harmed by AI systems will depend entirely on Member States' legislation. Currently, there is no uniform approach across the EU when it comes to the recoverability of non-material damages.[47] One category of EU countries does not differentiate between material and immaterial damage and considers both damages equally recoverable. This group includes

43 See for example Recital 81 DSA.

44 Meaker M, 'Slovakia's Election Deepfakes Show AI Is a Danger to Democracy' (Wired, 3 October 2023) https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/.

45 European Commission, White Paper On Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

46 Art. 5 (a) of the compromised text of the PLD defines damages only as "material losses".

47 For an analysis on how damage caused by artificial intelligence (AI) systems is allocated by the rules of tortious liability currently in place in the EU, and whether – and if so to what extent – the national tort law regimes differ in that respect, see European Commission, Directorate-General for Justice and Consumers, Karner, E., Koch, B., Geistfeld, M., Comparative law study on civil liability for artificial intelligence, Publications Office of the European Union, 2021. https://data.europa.eu/doi/10.2838/77360; For an extensive comparison with reports from 26 European jurisdictions on recoverable damages see B Winiger/H Koziol/BA Koch/R Zimmermann (eds), Digest of European Tort Law II: Essential Cases on Damage (2011).

Belgium, France, Luxembourg, Spain, Hungary and Slovenia. The second category departs from the premise that immaterial damage is generally non-recoverable and only allows recovery of immaterial damage if expressly provided for by law. Countries like Italy, Germany, Poland, Austria, the Netherlands, Estonia, Lithuania, and the Nordic Countries follow this approach.[48]

Explicitly including immaterial damages and systemic harms in the recitals and definitions of the AILD would enhance the protective capacity of the framework and solidify the links between the AI Act and the AILD. Recital 4 of the AI Act[49] explicitly recognises "immaterial" harms posed by AI, both in the European Commission and Council text. The European Parliament's mandate for the AI Act further highlights immaterial harms, mentioning "societal" harm specifically.[50]

Scholars have also proposed attaching compensation for immaterial harms to a model of non-compliance liability when deployers and operators engage in prohibited or illegal practices under the AI Act.[51] This model could fit easily into existing non-discrimination, data protection, and consumer protection legislation. For example, Article 82 of the GDPR[52] provides for the liability of a controller or processor where their entity violates their obligations under the GDPR. In this sense, the scope of application for recoverable immaterial damages will not be too broad, countering the idea that including immaterial damages disproportionately broadens liability provision.

Finally, societal and systemic risks affect several individuals. The inclusion of immaterial harms strengthens the standing of these types of claims in court and broadens the possibilities of Member States in their national framework. In particular, given that the AILD is included in the scope of Directive (EU) 2020/1828[53], which applies to representative actions brought against infringements, by counterparties, of the provisions of Union law that harm or may harm the collective interests of consumers.

RECOMMENDATIONS:

- Modify Recital 10 AILD to include systemic harms and immaterial damages as recoverable damages.
- Include a definition of immaterial harm in the AILD based on the AI Act.
- Include the notion of systemic risk in the AILD in line with the DSA.

48 Commission Staff Working Document, Impact Assessment Report accompanying the document Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, SWD(2022) 319 final, 28.9.2022. https://ec.europa.eu/info/sites/default/files/1_4_197608_impact_asse_dir_ai_en.pdf.

49 The European Commission's initial proposal of the AI Act as well as the Council mandate both include in Recital 4 the wording: "Such harm might be material or immaterial."

50 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 2021/0106(COD), version for Trilogue on 24 October, 2023.

51 See Wendehorst, C. (2022). Liability for Artificial Intelligence: The Need to Address Both Safety Risks and Fundamental Rights Risks. In S. Voeneky, P. Kellmeyer, O. Mueller, & W. Burgard (Eds.), The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives (Cambridge Law Handbooks, pp. 187-209). Cambridge: Cambridge University Press. doi:10.1017/9781009207898.016; Hacker, Philipp, The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future (November 25, 2022). Available at http://dx.doi.org/10.2139/ssrn.4279796

52 Art. 82(1) GDPR establishes that "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered." Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

53 Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).

Annex 1: Limitation of liability clauses from main GPAIS providers.

OpenAI [Terms of Use]	"Neither we nor any of our affiliates or licensors will be liable for any indirect, incidental, special, consequential or exemplary damages, including damages for loss of profits, goodwill, use, or data or other losses, even if we have been advised of the possibility of such damages. Our aggregate liability under these terms shall not exceed the greater of the amount you paid for the service that gave rise to the claim during the 12 months before the liability arose or one hundred dollars ($100). The limitations in this section apply only to the maximum extent permitted by applicable law."
Meta [AIs Terms of Service]	"Our liability shall be limited to the fullest extent permitted by applicable law, and under no circumstance will we be liable to you for any lost profits, revenues, information, or data, or consequential, special, indirect, exemplary, punitive, or incidental damages arising out of or related to these Terms or AIs (however caused and on any theory of liability, including negligence), even if we have been advised of the possibility of such damages."
Google [API Terms, Google Terms]	"When permitted by law, google, and google's suppliers and distributors, will not be responsible for lost profits, revenues, or data; financial losses; or indirect, special, consequential, exemplary, or punitive damages. To the extent permitted by law, the total liability of google, and its suppliers and distributors, for any claim under the terms, including for any implied warranties, is limited to the amount you paid us to use the applicable APIs (or, if we choose, to supplying you the apis again) during the six months prior to the event giving rise to the liability. In all cases, google, and its suppliers and distributors, will not be liable for any expense, loss, or damage that is not reasonably foreseeable."
Anthropic [Terms of Service]	"To the fullest extent permissible under applicable law, in no event will we … Be liable for any direct, indirect, punitive, incidental, special, consequential, exemplary, or other damages arising out of or in any way related to the services, the materials, or these terms, whether based in contract, tort (including negligence), strict liability, or other theory, even if any anthropic parties have been advised of the possibility of damages, and even if the damages are foreseeable. To the fullest extent permissible under applicable law, the anthropic parties' total aggregate liability to you for all damages, losses and causes of action arising out of or in any way related to the services, the materials, or these terms, whether in contract, tort (including negligence) or otherwise, will not exceed the greater of the amount you paid to us for access to or use of the services (if any) in the six months preceding the date such damages, losses, and causes of action first arose, and $100. The foregoing limitations are essential to these terms, and we would not offer the services to you under these terms without these limitations.
Inflection AI [Terms of Service]	"Under no circumstances and under no legal theory (whether in contract, tort, or otherwise) shall inflection ai be liable to you or any third party for (a) any indirect, incidental, special, exemplary, consequential or punitive damages, including lost profits, lost sales or business, lost data, or (b) for any direct damages, costs, losses or liabilities in excess one hundred ($100) u.s. dollars. The provisions of this section allocate the risks under these terms between the parties, and the parties have relied on these limitations in determining whether to enter into these terms."