European Parliament

Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence

Complementary impact assessment

STUDY

EPRS | European Parliamentary Research Service

Ex-Ante Impact Assessment Unit

PE 762.861 – September 2024

EN

Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence

Complementary impact assessment

In September 2022, the European Commission presented a proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence (AILD), with an accompanying impact assessment. The European Parliament's Committee on Legal Affairs (JURI) requested the present complementary impact assessment of the proposal, which focuses on specific research questions. The study critique identifies key shortcomings in the European Commission's impact assessment, not least an incomplete exploration of regulatory policy options and an abridged cost-benefit analysis, in particular of the strict liability regime.

The complementary impact assessment study proposes that the AILD should extend its scope to include general-purpose and other 'high-impact AI systems', as well as software. It also discusses a mixed liability framework that balances fault-based and strict liability. Notably, the study recommends transitioning from an AI-focused directive to a software liability regulation, to prevent market fragmentation and enhance clarity across the EU.

EPRS | European Parliamentary Research Service

AUTHOR

This study has been written by Philipp Hacker of European University Viadrina at the request of the Ex-ante Impact Assessment Unit of the Directorate for Impact Assessment and Foresight, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

ADMINISTRATORS RESPONSIBLE

Dieter Frizberg and Andriana Efthymiadou, Ex-ante Impact Assessment Unit, EPRS

In addition to internal revision, the study was subject to a double-blind external peer review organised by the Ex-Ante Impact Assessment Unit.

To contact the publisher, please e-mail EPRS-ExAnteImpactAssessment@ep.europa.eu

LINGUISTIC VERSIONS

Original: EN

Manuscript completed in September 2024.

PE 762.861
ISBN: 978-92-848-2244-7
DOI: 10.2861/1723734
CAT: QA-01-24-010-EN-N

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

Artificial intelligence (AI) liability is at the crossroads, both globally and in the EU. While several existing laws, from data protection to non-discrimination, establish liability for certain types of AI-facilitated harms, the AI Act and the revised Product Liability Directive (PLD) are the first two legal instruments at the EU level specifically implementing comprehensive obligations for AI systems along the entire AI value chain, and corresponding liability rules for defective AI products and software. Against this backdrop, the artificial intelligence liability directive (AILD), proposed by the European Commission alongside the PLD revision, faces several challenges as to how it fits into this novel regulatory framework. Undoubtedly, AI holds tremendous potential for societal benefit – from cancer screening to fraud detection and accident prevention – but also carries risks. The PLD, however, does not adequately cover the broad range of AI-specific risks, particularly not those relating to generative AI, such as discrimination and infringement on personality rights.

To chart a path forward for the AILD, this complementary impact assessment proceeds in four steps, after an initial general overview on AI liability. First, it provides an appraisal of the European Commission's initial impact assessment (IA) accompanying the proposal for an AILD in 2022. Second, the study investigates in detail the relationship between the PLD, the AI Act, and the AILD. Third, it compares the AILD framework with the rules proposed by the European Parliament in its resolution of 2020 on a civil liability regime for AI. Finally, it evaluates the need for and process of converting the AILD into a regulation for software liability more generally.

I. Appraisal of the European Commission's IA

In the discussion of the European Commission's IA, two key shortcomings are identified: an incomplete set of policy options and an abridged cost-benefit analysis of the policy options. Concerning the former, in particular, the IA pays little attention to the European Parliament's resolution of 2020 on liability for AI. Specifically, it fails to thoroughly investigate the possibility of integrating strict liability with liability caps, and it lacks depth in exploring a wider spectrum of negligence presumptions or complete reversals of the burden of proof. Consequently, the IA's analysis of the costs and benefits associated with alternative regulatory options, such as strict liability, is detailed inconsistently. While some aspects of these policy options are well-examined, the assessment is rather short in discussing the potential and drawbacks associated with a strict liability regime.

II. Relationship between the AILD, the PLD, and the AI Act

To fill these gaps, the following recommendations are made.

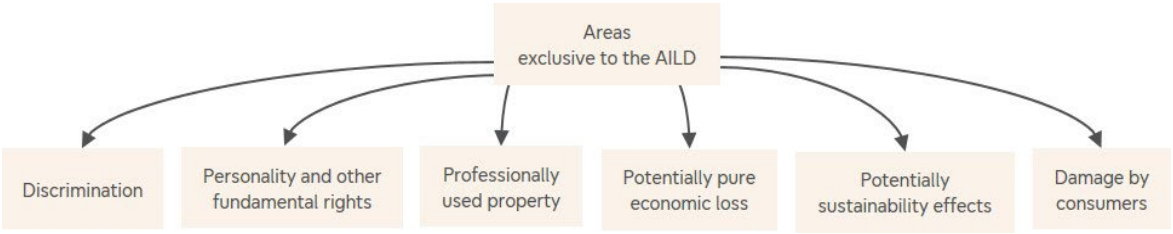
- **Identity of concepts and definitions**. The AILD includes several key concepts from the AI Act. For reasons of coherence and legal clarity, the AILD should adopt the concepts used in the AI Act (e.g. the definition of AI itself).
- **From high-risk to high-impact AI systems**. The AILD should, however, add certain categories that trigger the evidence disclosure obligations and the rebuttable presumptions concerning fault and causality.[1] This primarily concerns: general-purpose AI systems (e.g. ChatGPT); Old Legislative Framework systems (e.g. autonomous vehicles; transportation-related AI

[1] The AILD mandates that, under certain circumstances, injured parties have a right to obtain evidence from the person developing or using an AI system; in some cases, the AILD also establishes that the fault of these individuals – and that fault's causality for the AI output – is presumed unless these individuals can show evidence to the contrary.

applications more generally;[2] other AI systems falling under Annex I Section B AI Act[3]); and insurance applications beyond health and life insurance. The study suggests an umbrella term ('high-impact AI systems') to cover high-risk AI systems and those additional systems.

- **Rebuttal of presumption**. The AILD framework should allow for the causality presumption to be rebutted in cases where initial violations of the AI Act are rectified at later stages.
- **Article 14 and 26 AI Act violations**. Articles 14 and 26 AI Act require human oversight mechanisms in AI systems. The direct causation between a lack of ex-post oversight and harmful outputs is not always clear. It is suggested to establish a direct presumption of causality between AI outputs and damages for non-compliance with monitoring obligations.
- **Handling of prohibited AI systems**. For AI systems banned under Article 5 AI Act, the recommendation is to assume strict liability for any damages they cause.
- **Impact of general-purpose AI systems**. The current AILD framework does not adequately cover general-purpose AI systems, which can lead to significant harm particularly in the realms of non-discrimination (e.g. unbalanced content) and personality rights (e.g. hate speech and fake news). It is recommended that generative AI systems, such as ChatGPT, be classified under the new 'high-impact' category. This would bring them under the ambit of the AILD, ensure evidence disclosure, and establish presumptions of causality for safety violations. This, in turn, aids injured parties in legal claims.
- **Extension of the AILD beyond the PLD**. Given the PLD's limitations (e.g. concerning non-professional users and types of damage not covered by the PLD), there is a strong case for extending the AILD, to ensure a comprehensive liability framework (see Figure 1, below).
- **Applicability of the AILD to discrimination cases**. It should be made clear that the AILD applies to cases of liability for discrimination. The need for evidence disclosure mechanisms and a rebuttable presumption in discrimination cases is underscored by existing enforcement challenges and the legal precedent set by the Court of Justice of the EU (*Meister* case), which currently restricts access to data and algorithms critical to proving discrimination.

Figure 1 – Areas covered by the AILD but not by the PLD



Source: Author.

- **From the AILD to a software liability instrument**. The current draft of the AILD addresses AI liability but does not tackle the similar complexities and challenges present in many types of non-AI software (e.g. proving fault and causality). The PLD, in turn, already applies to software more generally. To address this discrepancy, it is recommended that the AILD be expanded into a more comprehensive software liability instrument (see Table 1, below). This can take either the form of a directive or – preferably – a regulation (Part IV, below). It would cover not only AI but also all other types of software, such as the PLD. This expansion would ensure that the proof

[2] See also, in a similar vein, M. C. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, p. 18; J. De Bruyne, O. Dheu and C. Ducuing, 'The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive', *Computer Law & Security Review*, Vol. 51, Article 105894, 2023, p. 4: '[The AILD] may also be a missed opportunity, considering the importance of autonomous vehicles.'; S. Wachter, 'Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond', *Yale Journal of Law and Technology*, Vol. 26(3), 2024, p. 671, p. 716.

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

alleviations are applied uniformly to all software applications, regardless of whether they are classified as (high-risk) AI systems or not. Specifically, the evidence disclosure mechanism should be applicable to all types of software, and the rebuttable presumption for non-AI software should align with the rules for non-high-risk AI systems.

Table 1 – Types of software and harm covered by the revised PLD, the proposed AILD, and the recommended software liability instrument (SLI)

	Non-AI software	AI
Consumer property (PLD)	EDM, RP	EDM, RP
Health (PLD)	EDM, RP	EDM, RP
Life (PLD)	EDM, RP	EDM, RP
Discrimination (AILD/SLI)	EDM, RP	EDM, RP
Personality rights (AILD/SLI)	EDM, RP	EDM, RP
Other fundamental rights (AILD/SLI)	EDM, RP	EDM, RP
Professional property, such as IP rights (AILD/SLI)	EDM, RP	EDM, RP
Pure economic loss (AILD/SLI)	EDM, RP	EDM, RP
Sustainability harms (AILD/SLI)	EDM, RP	EDM, RP

Note: EDM: evidence disclosure mechanism; IP: intellectual property; RP: rebuttable presumption.

Source: Author.

Table 1 shows that, without the AILD and the SLI, protection would be inadequate in many areas, compared with the new PLD: in the green boxes, similar protection can only be achieved with the AILD; and in the red boxes, only with the SLI.

III. The AILD and the European Parliament resolution of 2020 on AI liability

- **Strict liability for illegitimate-harm models**. It is recommended that the strict liability framework proposed in the European Parliament's resolution of 2020 on AI liability,[4] particularly for high-risk AI systems, be considered for integration into a revised AILD. This would involve adopting a strict liability model that distinguishes between AI models causing legitimate and illegitimate harm in the proper course of their operation. If the AI systems are meant to cause justified harm, e.g. by correctly rejecting a job candidate, they cannot be subjected to truly strict liability. Otherwise, every single candidate, except for the one chosen, could successfully sue the operator of even a perfectly functioning system.
- **Arguments for and against strict liability**. Concerning models that should not cause harm if properly designed and deployed, arguments for and against strict liability must be thoroughly weighed. Truly strict liability for AI may set incentives for a socially optimal amount of AI deployment, streamline compensation processes, and ensure that those who primarily benefit economically from AI also bear the cost of potential harms. Conversely, truly strict liability might have a deterrent effect on AI investment and deployment in the EU and, thereby, reduce the availability of beneficial AI technologies. To the extent that this impacts critical services such as healthcare and education, it could potentially lead to a decrease in the enjoyment of related fundamental rights. Moreover, such a liability regime could increase vexatious litigation, particularly involving immaterial harms. This would impact small and medium-sized enterprises (SMEs) in particular, which represent the greatest part of the European AI ecosystem.

[4] Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), European Parliament.

- **Political choices and transparency**. These arguments should be discussed openly and transparently in the AILD legislative process. Whether strict liability is enacted for high-risk AI systems is, ultimately, a political and normative choice.
- **Joint liability along the value chain**. The fair sharing of liability in the AI value chain, particularly with general-purpose AI systems, requires a streamlined redress framework in the AILD, to reduce reliance on varied national laws and to foster a cohesive legal environment within the EU. Building on provisions in the PLD and the Data Act, three policy options – presumption of equal share, support of SMEs, and protection of downstream parties – offer different mechanisms to ensure fair compensation and liability distribution. They can be combined, and all require binding provisions in order to prevent contractual practices from undermining these protections.
- **Fault-based liability and evidence disclosure**. The AILD should align with the PLD by mandating that (evidence) disclosure be presented in a manner easily understandable to non-experts, such as consumers or their legal counsel. For claims by non-competitors, it should lower the barrier for triggering evidence disclosure by requiring only the demonstration of damage and involvement of an AI system.

IV. Choice of instrument

- **From directives to regulations**. Transitioning from a directive to a regulation would prevent market fragmentation, enhance clarity, and promote innovation and consumer protection by establishing consistent legal standards across the digital single market. It would also align with current trends in product safety law, where numerous directives are being replaced by regulations (e.g. General Product Safety Regulation; Medical Devices Regulation). These findings thus call for a revised Product Liability Regulation and an AI liability regulation (or rather: a software liability regulation, see above) instead of directives.
- **Steps forward**. Implementing this change requires: (i) legal assessments aligned with EU Treaties; (ii) stakeholder consultations, (iii) an impact assessment; (iv) amendments to the legal proposal; (v) following the ordinary legislative procedure; and (vi) developing detailed implementation guidelines for a smooth transition.

Table of contents

Table of figures

Table of tables

List of abbreviations

AI	Artificial Intelligence
AI Act	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024
AIDA	Canada's Artificial Intelligence and Data Act: Bill C-27. An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts
AILD	Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final
B2B	Business-to-business
Data Act	Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 2023/2854, 22.12.2023
EU	European Union
GDPR	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)
IA	Impact Assessment
OLF	Old Legislative Framework
PLD	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 [Product Liability Directive], as revised in 2024; text based on the European Parliament version adopted on 12 March 2024
SB 1047	California Senate Bill 1047: Safe and Secure Innovation for Frontier Artificial Intelligence Models Act
SLD	Software liability directive
SLI	Software liability instrument
SME	Small and medium-sized enterprise
TFEU	Treaty on the Functioning of the European Union

1. AI liability in the EU today

Liability for AI is at a critical juncture today, both in the EU and beyond. Across the globe, regulatory frameworks have been designed, proposed, and in some cases enacted, to address key risks of AI systems. Most specific AI laws adopt a procedural approach, venturing deeply into the terrain of regulating the AI pipeline, from training data to modelling and deployment. The Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence signed by US President Joe Biden,[5] for example, contains a vast range of obligations for AI developers and federal agencies deploying such models. Significantly, after several acts by China,[6] the EU formulated first comprehensive AI regulation worldwide with the AI Act.[7] Containing specific provisions for various use cases, general-purpose AI models (e.g. foundation models), and generative AI, the AI Act stands out as the epitome of direct AI legislation.

1.1. Direct and indirect AI regulation

These specific regulatory endeavours delineate a market access and market surveillance regime, contingent on highly granular obligations for AI providers and deployers. Next to these, different sets of laws determine who, if anyone, will be liable if harm is caused by the use of an AI system. Importantly, many laws written, and doctrines conceived, in technology-neutral ways – from the US product liability framework to the EU General Data Protection Regulation (GDPR), EU and national consumer and tort law, and non-discrimination directives – do apply to activities involving AI, at least in general. Nonetheless, the application of existing liability frameworks to AI can be challenging, due to a range of factors related to the complexity and opacity of AI systems and underlying models.[8]

Hence, in September 2022, the European Commission took a significant step towards completing its regulatory framework for AI by releasing two key proposals aimed at addressing AI liability. The proposals for an AI Liability Directive (AILD)[9] and the revised Product Liability Directive (PLD)[10] represent the dual approach adopted by the European Commission in tackling AI liability. The AILD aims to harmonise procedural aspects of AI liability across EU Member States, such as evidence disclosure and the burden of proof, linking these mechanisms closely with compliance to the AI Act. On the other hand, the PLD seeks to update the existing product liability framework. It extends its scope to include digital products and AI more specifically in a much-awaited demarche to adapt to the evolving nature of products in the digital age. While the PLD was enacted jointly with the AI Act, the legislative process on the AILD still needs to be completed.

The key differences between the AILD and the PLD are summarised in Table 2 (see table below).[11]

---

5 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, *The White House*, 30 October 2023.

6 See e.g. M. Sheehan, 'China's AI regulations and How They Get Made', *Horizons: Journal of International Relations and Sustainable Development*, 2023., p. 108; A. Huyue Zhang, *High Wire: How China Regulates Big Tech and Governs Its Economy*, Oxford University Press, 2024, particularly Chapter 11.

7 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

8 See e.g. Expert Group on Liability and New Technologies, Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies, European Commission, 2019; A. Bertolini, Artificial intelligence and civil liability, external study prepared for the European Parliament's Committee on Legal Affairs (JURI), 2020.

9 COM(2022) 496 final.

10 COM(2022) 495 final.

11 Table 2 is adapted from P. Hacker, 'The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 7.

Table 2 – Key differences between the AILD and the PLD

PLD	AILD proposal
Claim rooted in EU law	Claim rooted in Member State law
Material and procedural aspects of product liability	Procedural aspects of non-contractual civil liability for AI systems
Applicable to physical products and software, including AI systems	Applicable to AI systems only
Supposedly strict liability	Fault-based liability
Claims against manufacturers and other entities in the supply chain	Claims against manufacturers, professional users and consumers
Eligible damage: privately used property, death or personal injury, and data loss	Eligible damage: potentially also professionally used property, fundamental rights and primary financial loss
Full harmonisation	Minimum harmonisation

Source: P. Hacker, 'The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 7.

The methodological bifurcation between the AI Act on the one hand and the liability initiatives on the other reflects an understanding that both direct regulation, through specific AI laws, and indirect incentives, via liability frameworks, are necessary to ensure a balanced and effective approach to AI governance.[12] The interplay between the AI Act and the liability directives highlights the EU's holistic strategy towards AI regulation which emphasises complementarity between regulatory and liability measures. While the AI Act establishes a structured regulatory environment for high-risk (and other) AI systems, including oversight mechanisms and standards for development and deployment, the AILD proposal and the revised PLD aim to ensure that affected individuals have clear, actionable paths for redress in the event of harm. These legal instruments engage with existing acts in various and often still underappreciated ways, from sectoral regulation to non-discrimination and from data protection to copyright law.

1.2. International efforts: Canada's AIDA and California Senate Bill 1047

These European initiatives do not occur in a vacuum on the international scene. Perhaps closest to the AI Act, Canada's Artificial Intelligence and Data Act (AIDA), introduced as part of Bill C-27,[13] would regulate AI within the country. Like the AI Act, it follows a risk-based approach, with a focus on 'high-impact AI systems', which are systems with the potential to cause significant harm or influence public safety.[14] Under AIDA, organisations that develop or deploy these AI systems are required to conduct risk assessments, implement risk mitigation strategies, and continuously monitor their systems to ensure compliance with safety and ethical standards.

In terms of liability, AIDA emphasises holding entities accountable for the harm caused by their AI systems. AIDA relies on public enforcement, not private litigation, however (Sec. 29-30 and 40

[12] H. Zech, 'Liability for AI: public policy considerations', *ERA Forum*, Vol. 22, 2021, p. 147, p. 150; P. Hacker, 'The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 1.

[13] Parliament of Canada, 'An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Act', Bill C-27.

[14] M. Gallagher, Canada's Artificial Intelligence and Data Act (AIDA) 2024: A Comprehensive Guide, 2024.

AIDA). This includes substantial fines for negligent (Sec. 30(4) AIDA) non-compliance and the ability of the AI and Data Commissioner to oversee and enforce these regulations.

In the EU, by contrast, the AI Act is accompanied by legislation on private enforcement: the PLD and the AILD. Importantly, the PLD and the AILD are not the only options to structure AI liability under private law,[15] as recent developments in the US show. While the US generally relies on its tort law and product liability regime hold actors accountable involving AI-related accidents,[16] several states have introduced specific AI liability regulation. Most notably, the much-debated California Senate Bill 1047,[17] currently in the legislative process,[18] would place strict liability on developers of very advanced AI models. It covers AI models which cost at least $100 million and use large amounts of compute during training (Sec. 22602(e)(1)(A)(i) SB 1047)[19] and models created by fine-tuning such a covered model which cost at least $10 million and use significant amounts of compute during training (Sec. 22602(e)(1)(A)(i) SB 1047).[20] The act would require developers of such models to implement comprehensive safety measures, such as cybersecurity protocols, shutdown capabilities, and third-party testing (Sec. 22603 SB 1047). The bill focuses on preventing catastrophic harms, such as large-scale cyberattacks or events causing mass casualties (Sec. 22602 (g) SB 1047). If an AI model results in such significant damage, developers could face severe penalties, including fines, injunctions, and the deletion of the AI system (Sec. 22606 SB 1047).

The legislation would also introduce strict liability (Sec. 22606(a)(5) SB 1047).[21] Under this rule, developers may be held accountable for any harm caused by their AI systems, even if they followed all prescribed safety measures. This approach aims to ensure that developers take efficient precautions to avoid unintended consequences and mitigate risks associated with powerful AI technologies.

1.3. Strict liability in the EU and the European Parliament resolution of 2020 on AI liability

In EU and Member State law, strict liability covers certain products, such as nuclear power plants, railways, cars, whose legitimate use constitutes a significant but socially acceptable risk.[22]

Importantly, in the EU, the idea of a strict liability system for AI has already been introduced by one of the co-legislators. In October 2020, the European Parliament published a wide-ranging proposal (the European Parliament resolution of 2020 on AI liability[23]), in which an architecture with strict

---

15 For a general analysis of types of liability, see e.g. R. A. Epstein, 'A theory of strict liability', *The Journal of Legal Studies*, Vol. 2, 1973, p. 151; S. Shavell, 'Strict Liability versus Negligence', *The Journal of Legal Studies*, Vol. 9, 1980, p. 1; with a view to AI, see e.g. M. C. Buiten, 'Product liability for defective AI', *European Journal of Law and Economics*, 2024, p. 1; C. Wendehorst, 'Strict liability for AI and other emerging technologies', *Journal of European Tort Law*, Vol. 11, 2020, p. 150; and references in n. 2 and 11.

16 M. H. Pfeiffer, First, Do No Harm. Algorithms, AI, and Digital Product Liability, Center for Urban Policy Research, Rutgers University, 2023; E. Karner, B. Koch and M. A. Geistfeld, Comparative Law Study on Civil Liability for Artificial Intelligence, 2021, p. 120.

17 Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, California Senate Bill 1047, 2024.

18 M. Zeff, California weakens bill to prevent AI disasters before final vote, taking advice from Anthropic, TechCrunch, 15 August 2024.

19 Specifically, the computer threshold is 10^26 floating operation points (FLOPs).

20 The threshold here is three times 10^25 FLOPs.

21 Note, however, that some of the primary obligations only involve the application of reasonable care (Sec. 22603(a)(1) and (a)(3)(A) SB 1047).

22 See only E. Karner, B. Koch and M. A. Geistfeld, Comparative Law Study on Civil Liability for Artificial Intelligence, 2021, p. 58.

23 Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), European Parliament.

liability for high-risk AI systems and a presumption of fault for non-high-risk systems were combined. These three proposals, which were preceded by reports of the European Commission and expert groups,[24] have sparked a significant debate in the legal literature on the ideal structure and content of AI liability.[25]

On the policy side, the AILD proposal was accompanied by an IA[26] prepared by Directorate-General for Justice and Consumers of the European Commission. The Regulatory Scrutiny Board of the European Commission, in April 2022, issued an opinion (positive with reservations) on the IA.[27] In March 2024, the Ex-ante Impact Assessment Unit of the Directorate-General for Parliamentary Research Services (DG EPRS) of the European Parliament released an initial appraisal of the European Commission's IA, focusing on the IA's methodological strengths and weaknesses, which is summarised in Section 2.[28]

Against this background, this study will proceed in three steps. In Section 3, it will examine the interplay between the AILD, the PLD, and the AI Act, and ask if any legal loopholes remain. Section 4 then contrasts the AILD and the European Parliament resolution of 2020 on AI liability, highlighting key differences. Looking forward, Section 5 analyses to what extent a shift from a directive to a regulation, as a legal instrument, is warranted and can indeed be achieved for AI liability in the EU.

[24] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), European Commission, 2018; Expert Group on Liability and New Technologies, Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies, European Commission, 2019.

[25] See e.g. A. Bertolini, Artificial intelligence and civil liability, external study prepared for the European Parliament's Committee on Legal Affairs (JURI), 2020; S. Wachter, 'Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond', *Yale Journal of Law and Technology,* Vol. 26(3), 2024, p. 671, particularly p. 717; H. Zech, 'Liability for AI: public policy considerations', *ERA Forum*, Vol. 22, 2021; G. Wagner, 'Robot Liability', in S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019, pp. 27-62; P. Čerka, J. Grigienė and G. Sirbikytė, 'Liability for damages caused by artificial intelligence', *Computer Law & Security Review,* Vol. 31, p. 376; C. Wendehorst, 'Strict liability for AI and other emerging technologies', *Journal of European Tort Law*, Vol. 11, 2020, p. 150; C. Wendehorst, The Proposal for an Artificial Intelligence Act COM (2021) 206 from a Consumer Policy Perspective, Federal Ministry of Social Affairs, Health, Care and Consumer Protection, 2021; C. Wendehorst, AI liability in Europe: anticipating the EU AI Liability Directive, Ada Lovelace Institute, 2022; G. Spindler, 'User liability and strict liability in the Internet of Things and for robots', in S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019, pp. 125-143; E. Marchisio, 'In support of "no-fault" civil liability rules for artificial intelligence', *SN Social Sciences*, Vol. 1, 2021; F. P. Patti, 'The European road to autonomous vehicles', *Fordham International Law Journal*, Vol. 43, 2019, p. 125.

[26] 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, European Commission, 28 September 2022.

[27] Regulatory Scrutiny Board on Liability rules for Artificial Intelligence, SEC(2022) 344, European Commission, 8 April 2022.

[28] D. Frizberg, Adapting liability rules to artificial intelligence, EPRS, European Parliament, March 2024.

2. Appraisal of the European Commission's AILD impact assessment

Several studies investigating the potential effects of different liability regimes for AI prepared the ground for the European Commission's IA, such as an economic study by Deloitte to support the European Commission's IA;[29] a behavioural economics study by Behavia et al.;[30] a comparative law study on civil liability for AI by Karner et al.;[31] and the EPRS study on a civil liability regime for AI.[32]

(Partially) based on these studies, the IA evaluates three policy options aimed at refining AI liability regulations.[33]

- Policy option 1 introduces measures to ease the burden of proof for AI liability claims, including mandatory disclosure of AI documentation, a rebuttable presumption of liability for non-compliance with AI Act safety measures, and an adjusted burden of proof relating to the internal workings of AI systems.
- Policy option 2 builds on policy option 1 by adding a strict liability regime for high-risk AI uses, and mandating insurance for those liable under the strict liability regime.
- Policy option 3 (preferred policy option) implements policy option 1 measures initially, with a later review to potentially add strict liability measures based on further AI developments.

Two options were discarded at an early stage: strict liability for all AI-enabled products and services (considered too hostile towards investment in AI, by the European Commission); and the harmonisation of the types of harm giving rise to civil liability claims in AI cases (deemed going beyond the level in non-AI cases, by the European Commission).[34] This cursory treatment is problematic as it excludes, albeit with references to pertaining parts of the Deloitte Study, two earnest proposals that rival the ultimately preferred policy option.[35] It would have been preferable to include these options in the comprehensive assessment: not only to allow for a broader comparative discussion of valid and serious options, but also to discuss ways in which the supposedly negative impacts of the discarded options could be mitigated (e.g. liability caps; guidelines; sandboxes). This omission is a key weakness of the IA.

The IA's preferred policy option, policy option 3, initially only implements the measures from policy option 1. This approach allows for a reassessment to potentially incorporate strict liability measures dependent on future developments in AI technology. According to the IA, this option strikes a balance between protecting EU citizens and fostering the AI industry's growth by boosting trust and reducing legal uncertainties.[36]

The IA mentions several advantages of the preferred policy option.[37] According to the document, it enhances victim protection, lifting it to a level on par with traditional technologies, and still boosts the uptake of AI through increased trust among users. The approach also aims to prevent legal

[29] Deloitte, Study to support the European Commission's IA on liability for artificial intelligence, 2021.

[30] Behavia, CEPS, Kantar, Behavioural study on the link between challenges of artificial intelligence for Member States' civil liability rules and consumer attitudes towards AI-enabled products and services, 2021.

[31] E. Karner, B. Koch and M. A. Geistfeld, Comparative Law Study on Civil Liability for Artificial Intelligence, 2021.

[32] T. Evas, Civil liability regime for artificial intelligence, EPRS, European Parliament, September 2020.

[33] IA, pp. 25-41.

[34] IA, pp. 41-42.

[35] See in this vein Regulatory Scrutiny Board Opinion, Liability rules for Artificial Intelligence, SEC(2022) 344, European Commission, 8 April 2022, point C.3.

[36] IA, p. 61.

[37] IA, pp. 57-61.

fragmentation across the EU. This is supposed to promote a more unified market especially beneficial to SMEs by lowering legal barriers and facilitating the broader deployment of AI products and services. While this option shifts the cost burden from victims to liable parties – potentially raising insurance premiums for businesses – it also positions European AI firms to be more competitive globally, the IA claims.[38] Finally, it aims to support the effective enforcement of fundamental rights and to establish the EU as a leader in AI liability regulation on the international stage.

While the IA rightly identifies and compares several core aspects of different approaches to AI liability, two key issues with the IA remain, extending to both substantive and methodological areas.

- **Incomplete Set of Options**. The IA fails to consider a comprehensive set of regulatory options. Notably, it does not give enough attention to the possibility of implementing an AI liability *regulation* instead of a directive,[39] a suggestion put forth by the European Parliament. Additionally, it does not explore in detail the potential for combining strict liability with liability caps, nor does it elaborate in depth on a broader range of negligence presumptions or a full reversal of the burden of proof that could be rebutted or met by demonstrating algorithmic due diligence.[40] These omissions suggest quite a narrow scope of potential solutions that may not fully address all relevant aspects, including from a fundamental rights and business perspective.[41]
- **Abridged Cost-Benefit Analysis of Options**. The investigation into the costs and benefits of other regulatory options beyond the preferred one, including the imposition of strict liability, is thorough at times, but lacks some detail and analysis when evaluating the promises and perils of a strict liability regime.
  - The IA does note, citing the Behavioural Economics Study and the Economic Study,[42] that strict liability can set incentives to prevent damages, and is likely to increase trust in AI products and their uptake. Referring again to the Economic Study, the IA details that the moderate compliance costs expected under strict liability regime for high-risk AI systems would be outweighed by cost savings based on legal certainty, easier compliance, and higher revenue.[43] Policy option 1 (rebuttable presumption) 'is estimated to entail an increase of the overall absolute amount of annual liability insurance premiums in the EU by 25 %,'[44] and Policy option 2 (strict liability for high-risk AI systems) by 35%.[45]
  - The main concern articulated in the IA is the coherence of strict liability for AI with fault-based liability for non-AI technologies,[46] and the proportionality of strict liability: it is unclear, according to the European Commission's IA, whether there is a need for strict liability beyond the procedural alleviations (now proposed in the AILD) and what the risk profile and deployment conditions of AI will be that

38 See IA, p. 25.

39 IA, p. 51. A directive is supposed to allow Member States to integrate the measures within their traditional legal systems in the 'politically sensitive field of civil law'; see also IA, p. 57.

40 See IA, p. 33.

41 See also Regulatory Scrutiny Board Opinion, Liability rules for Artificial Intelligence, SEC(2022) 344, European Commission, 8 April 2022, points C.1 and 3; D. Frizberg, Adapting liability rules to artificial intelligence, EPRS, European Parliament, March 2024, p. 4.

42 IA, p. 52-53.

43 IA, p. 53, referring to Deloitte, Study to support the European Commission's IA on liability for artificial intelligence, 2021, p. 164.

44 IA, p. 54.

45 ibid.

46 IA, p. 56.

should be covered by strict liability.[47] A third critique voiced by the IA is the lower expected legal certainty, based again on the supposedly unclear risk profile and development of AI.[48] These perceived shortcomings are the only reasons given in the main text why, in the comparison with the other policy options, the strict liability mechanism ranks lowest.[49] Annex X provides a more detailed multi-criteria analysis, drawing on the economic study by Deloitte;[50] here, however, a 'scarcity of quantified data or estimates' is rightly acknowledged.[51]

- It seems striking that these crucial points are not discussed in a more balanced way. For example, one could argue that the problem of defining appropriate risk categories equally applies to the AI Act – where, quite obviously, it did not stand in the way of sweeping regulation. In fact, risk categories can be pre-specified even if AI applications are still unknown. It is true that it would be imperative to include a mechanism for rapidly adjusting these categories; but this is easily feasible through delegated or implementing acts – again, like in the AI Act. Furthermore, legal certainty is not just about risk categories. Strict liability, arguably, provides *greater* legal certainty than procedural alleviations coupled with fault-based regimes as it dispenses of the need to establish specific standards for duties of care. Therefore, it seems questionable that the strict liability option should score *lower* on legal certainty than the procedural framework,[52] which does not contain any rules for reducing legal uncertainty concerning the substantive basis of fault-based liability (i.e. fault) (see below, 4.1.3.). This positive effect of strict liability on legal certainty is explicitly noted by the Deloitte study, too.[53]
- In addition, one may argue that strict liability *does* fill gaps left by the procedural alleviations: expensive expert witnesses are not necessary to determine fault;[54] the likelihood of court proceedings, which generally acts as a deterrent to injured parties, is lower as liability turns only on showing damage caused by an AI tool; and the pronounced role of insurers usually benefits injured parties and helps them to gain compensation, as seen in the automotive sector. The IA overlooks all of these counter-arguments.
- Regarding the concern that a strict liability regime for high-risk AI could go beyond the liability regime for non-AI products, the IA could have contemplated and evaluated the option of harmonising Member State tort law to a greater extent, particularly by introducing strict liability provisions for a range of high-risk products, including but not limited to AI.[55]
- This cursory examination of the disadvantages of the only truly different policy option (strict liability) undermines the IA's ability to fully assess and compare the

47 IA, pp. 56-57.

48 IA, p. 52.

49 IA, p. 60.

50 See particularly Deloitte, Study to support the European Commission's IA on liability for artificial intelligence, 2021, pp. 126-198, with the key Figure 66 on p. 198.

51 IA, p. 186.

52 See also M. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, pp. 8-9.

53 Deloitte, Study to support the European Commission's IA on liability for artificial intelligence, 2021, p. 197: 'clear and predictable liability regime for all stakeholders'.

54 Cf. also S. Wachter, 'Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond', *Yale Journal of Law and Technology,* Vol. 26(3), 2024, p. 671, p. 713.

55 See also Regulatory Scrutiny Board on Liability rules for Artificial Intelligence, SEC(2022) 344, European Commission, 8 April 2022, point C.1.

implications of different policy choices. It limits the potential to identify the most effective and efficient regulatory framework for AI liability.

- Finally, the assessment of environmental impacts is incomplete. While the IA expects the uptake of AI applications to be beneficial for the environment,[56] it fails to even consider the substantial environmental costs of increased AI development and deployment due to high water and energy consumption.[57]

Similar points of critique concerning the IA's scope and methodology were also voiced in the opinion of the Regulatory Scrutiny Board[58] and the EPRS initial appraisal of the European Commission IA.[59]

[56] IA, p. 59.

[57] See e.g. P. Hacker, 'Sustainable AI Regulation', *Common Market Law Review*, Vol. 61, 2024, p. 345; A. S. Luccioni, Y. Jernite and E. Strubell, 'Power Hungry Processing: Watts Driving the Cost of AI Deployment?', arXiv preprint arXiv:231116863, 2023; A. de Vries, 'The growing energy footprint of artificial intelligence', *Joule*, 2023; P. Li and others, 'Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models', arXiv preprint arXiv:230403271, 2023; Measuring the Environmental Impacts of AI Compute and Applications: The AI Footprint, OECD, 2022; M. Taddeo and others, 'Artificial intelligence and the climate emergency: Opportunities, challenges, and recommendations', *One Earth*, Vol. 4., 2021, p. 776; C. Freitag and others, 'The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations', *Patterns*, Vol. 2, Article 100340; Tech. Policy Council ACM, ACM TechBrief: Computing and Climate Change, 2021; B, Knowles and others, 'Our house is on fire: The climate emergency and computing's responsibility', *Communications of the ACM*, Vol. 65, 2022, p. 38.

[58] Regulatory Scrutiny Board on Liability rules for Artificial Intelligence, SEC(2022) 344, European Commission, 8 April 2022.

[59] D. Frizberg, Adapting liability rules to artificial intelligence, EPRS, European Parliament, March 2024.

3. The interplay between the AILD, the PLD, and the AI Act

Based on the findings of the studies mentioned in the last Section, and on relevant scholarly literature, the following Section investigates in detail the interplay between the AILD, the PLD, and the AI Act. It will cover the effects of the AI Act definitions on the AILD (Section 3.1); the treatment of high-risk AI systems in the AI Act and the AILD (Section 3.2); the adequacy of basing a presumption of causality on the violation of Articles 9 to 15 AI Act (Section 3.3); the effects of the AI Act rules on foundation models and generative AI on the AILD framework (Section 3.4); and the need for an AILD regime beyond the revised PLD (Section 3.5).

3.1. The effects of the new AI Act definitions on the AILD

The AI Act includes a range of important definitions with direct repercussions on the AILD. This concerns terms and concepts such as 'AI' and 'software,' 'provider' and 'deployer,' 'general-purpose AI system,' 'risk,' and 'AI literacy,' which are taken up in turn below.

3.1.1. AI and software

The definition

The European AI Act now provides a more specific definition of AI, positioning it in Article 3(1) as a **machine-based system**

- *with varying degrees of **autonomy** and that may show adaptiveness after deployment,*
- *that **infers***
- *from the **input** it receives,*
- *how to generate **outputs***
  - *such as predictions, content, recommendations or decisions,*
- *that can **influence** physical or virtual environments.*

Even though the formula was taken over from the revised OECD AI definition,[60] it is surprisingly broad and generic. Since the definition does not require a specific degree of autonomy, any software fulfils all the requirements – except the element of 'inference.' Distinguishing AI from traditional software will be a challenge under this definition and require a good understanding of what it means to 'infer' the AI output from input. Furthermore, a purposive interpretation of the definition will need to posit a 'sufficient degree' of autonomy for models to qualify as AI.

Recital 12 AI Act provides some further nuance and guidance. Autonomy is specified as 'some degree of independence of actions from human involvement and of capabilities to operate without human intervention.' This is, however, a definition of automation, not autonomy.[61] Operation without human control intervention is a necessary, but not a sufficient definition of autonomy: there are many devices operating without human control that do not contain AI. Electric toothbrushes function without human involvement once they have been switched on (i.e. provided with input); a standard kitchen machine makes dough once provided with the ingredients and turned on. These functionalities, quite clearly, do not involve AI or any advanced level of autonomy. Rather, they are the hallmarks of automated machines. A more refined concept of autonomy would have to include, in addition, some capacity of adapting to input the model has not seen before.[62]

---

60 'Explanatory memorandum on the updated OECD definition of an AI system', OECD, 2024.

61 See e.g. W. Xu, 'From automation to autonomy and autonomous vehicles: Challenges and opportunities for human-computer interaction', *Interactions*, Vol. 28(2), 2020, p. 48, p. 50.

62 id.

According to Recital 12, this distinguishing characteristic is built into the concept of 'inference.' The Recital mentions the two main current approaches to AI:[63] machine learning[64] and knowledge-based approaches.[65] While this does little to further narrow the concept, the text emphasises that the capacity to infer must 'transcend basic data processing' and enable 'learning, reasoning or modelling'. Hence, it may be deduced that AI, in the sense of the Act, must enable some adaptive functions to tackle more complex tasks, like intricate predictions or content creation.

Systems such as chatbots, which process and generate natural language, diffusion-based image generators, or advanced facial recognition technologies that can identify individuals, clearly fall under this AI definition. Significantly, Recital 12 expressly excludes systems that are based on rules defined solely by natural persons to automatically execute operations. This concerns simple mathematical operations, as found in spreadsheet programs (e.g. Excel), which lack the capability for adaptation or independent reasoning.

Critique of the AI Act's AI definition

Admittedly, defining AI is an almost impossible task. Even computer scientists agree to disagree on the concept.[66] One prominent definition describes AI as computer programs that emulate human, rational behaviour and thinking.[67]

Against this background, it is no surprise that the AI Act struggles to neatly delineate the boundaries of AI. The AI Act's definition of AI is notably broad, capturing a wide array of technologies from simple machine learning algorithms (e.g. regression models) executing specific tasks to sophisticated systems capable of learning, adapting, and making independent decisions. While comprehensive and hence reasonably future-proof, this broadness poses challenges, particularly in distinguishing between systems that should be considered AI and those that should not.[68] For instance, the exclusion of rule-based systems from the definition is clear, but knowledge-based systems rely on intricate, human-built rules as well, yet are meant to fall under the definition of inference and, hence, AI. Similarly, the line between advanced statistical algorithmic processing and true AI capabilities can be blurry, leading to ambiguities in regulatory applications. Statistical modelling based on regression, which has been applied for a long time in finance, likely falls under the definition of AI, for example.

Effect on the AILD

The broad definition of AI as outlined in the AI Act has direct implications for the AILD, necessitating the inclusion of a wide range of technologies under its purview. This comprehensive approach ensures that various AI systems, irrespective of their complexity or autonomy, are subject to the AILD's procedural alleviations. However, it also risks the application of laws to systems that, while technically sophisticated, may not pose the ethical or societal risks typically associated with AI.

---

63 I. Goodfellow, Y. Bengio and A. Courville, *Deep Learning*, MIT Press, 2016, p. 9 et seqq.; D. L. Poole, A. K. Mackworth, *Artificial Intelligence: Foundations of Computational Agents*, Cambridge University Press, 2nd ed. edn, 2017, p. 645 et seqq.

64 Machine learning comprises most current approaches to AI, including deep learning and generative AI; see also D. Foster, *Generative Deep Learning*, *O'Reilly*, 2022, p. 4 et seqq.

65 These approaches include expert systems that were primarily developed in the second half of the 20th century; see also N. J. Nilsson, *The Quest for Artificial Intelligence*, Cambridge University Press, 2009, p. 149 et seqq.

66 M. O'Shaughnessy, One of the Biggest Problems in Regulating AI Is Agreeing on a Definition, Carnegie Endowment, 2022.

67 See e.g. S. J. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, *Pearson Education*, 4th Global edition, 2022, pp. 19-22.

68 M. C. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, p. 17.

Recommendations

The concept of AI is obviously key to any regulation of that technology. It should, to the best extent possible, be future-proof, but also distinguish systems that exhibit the key risks of AI for society.[69] These risks chiefly include: privacy and data protection, opacity, discrimination, unforeseeability, manipulation, harmful and fake content, as well as environmental and climate costs.[70]

Arguably, these risks are intrinsic to machine learning to a greater extent than to knowledge-based systems, due to their dependence on vast data sets and extensive training runs. However, complex non-AI software poses similar challenges.[71] Faced with the extremely broad definition of the AI Act, the AILD could (i) opt for a different, narrower definition of AI; (ii) expand its scope to (complex) software in general; or (iii) still adopt the AI Act's definition of AI.

The coherence of EU law and the ease of compliance clearly speak for the latter two options.[72] Operating with a different concept of AI would only sow confusion among regulatees and be of little practical value. Significantly, the PLD covers any type of software. In the PLD, software is not defined;[73] rather, Recital 13 PLD provides a non-exhaustive list of examples by referring to 'operating systems, firmware, computer programs, applications or AI systems.' Hence, a narrower AI definition of the AILD would have little effect – except in some areas outside the PLD's scope (see below, Section 3.5) – since the PLD contains mechanisms very similar to the AILD.

From an AI Liability Directive to a Software Liability Directive

This leaves the European legislator with a crucial choice between the second and the third option: aligning the AILD with the broader scope of the PLD (software), or with the narrower scope of the AI Act (AI, even though with a broad concept of AI).

This question cannot be answered independently from a comparison of the AILD with the PLD, which is undertaken below in Section 3.5. There is, however, something to be said for aligning the AILD with the PLD in terms of material scope (software) since both share very similar legal consequences. To the extent that the AILD may cover some areas outside of the PLD's purview (for example, cases of discrimination or violations of personality rights[74]), it seems difficult to justify that one set of rules

---

69 See e.g. M. E. Kaminski, 'Regulating the Risks of AI', forthcoming, *Boston University Law Review*, Vol. 103, 2023; H. Zech, 'Risiken Digitaler Systeme', *Weizenbaum Series 1*, 2020; S. Bubeck and others, 'Sparks of artificial general intelligence: Early experiments with GPT-4', arXiv preprint arXiv:230312712, 2023; P. Hacker, 'Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law', *European Law Journal*, Vol. 27, 2023, p. 148-149.

70 See e.g. P. Hacker, 'Sustainable AI Regulation', *Common Market Law Review*, Vol. 61, 2024, pp. 350 et seqq.; T. Wischmeyer and T. Rademacher, Regulating Artificial Intelligence, *Springer*, 2020; I. Ulnicane 'Artificial Intelligence in the European Union: Policy, ethics and regulation', in T. Hoerber, G. Weber and I. Cabras, *The Routledge Handbook of European Integrations*, Taylor & Francis, 2022, p. 254.; P. Hacker, A. Engel and M. Mauer, 'Regulating ChatGPT and other Large Generative AI Models', *ACM Conference on Fairness, Accountability, and Transparency (FAccT '23), 2023;* N. Helberger and N. Diakopoulos, 'ChatGPT and the AI Act', *Internet Policy Review*, Vol. 12, 2023.

71 P. Hacker, 'The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 9.

72 See also I. Bratu, 'A first critical analysis of the European approach to damage caused by artificial intelligence enabled by global navigation satellite systems. A bridge to nowhere or a cloud with a silver lining?', *International Review of Law, Computers & Technology*, Vol. 37, 2023, p. 147, p. 156.

73 In computer science, software refers to programs and the algorithms they represent, and is contrasted to the machinery itself, the hardware. Algorithms, in turn, are defined steps for producing output from certain types of input; see e.g. J. G. Brookshear and D. Brylow, *Computer Science: An Overview*, 13th edition, *Pearson*, 2020, p. 18.

74 AI systems may perpetuate discrimination through their output or violate personality rights by generating insults and hate speech, for example; see e.g. S. Sterlie, N. Weng and A. Feragen, 'Non-discrimination Criteria for Generative Language Models', arXiv preprint arXiv:240308564, 2024; H. Kotek, R. Dockum and D. Sun, 'Gender bias and stereotypes in large language models', Proceedings of the ACM Collective Intelligence Conference, August 2023, p. 12; P. Hacker, F. Zuiderveen Borgesius, B. Mittelstadt and S. Wachter, 'Generative Discrimination. What Happens

(far-reaching alleviations of proof) applies to non-AI software triggering certain harms covered by the PLD and another set of rules (lack of these alleviations) applies to all other harms wrought by non-AI software.

Such a bifurcation would only be justifiable if the harms covered by the PLD were, from a legal and fundamental rights perspective, much more important than those covered by the AILD. However, as the discussion under Section 3.5 will show, this is not the case. Instances of discrimination or violation of personality rights equally, and in some cases perhaps even more strongly, impact fundamental rights as the typical PLD scenarios of damage to property or health. **The AILD should, therefore, be rebranded as a software liability instrument, and take over the definition of software from the PLD.**

Refining the broad concept of AI

If the co-legislators, by contrast, opt to maintain the focus on AI, the AI Act's definition of AI should be chosen for the AILD. However, to mitigate the challenges posed by the AI Act's broad AI definition, there is a pressing need for clear guidelines that delineate which systems are considered AI within the legal framework. These guidelines should include specific examples of technologies that are, and those that are not, covered by the AI definition, providing clarity to developers, regulators, and users alike. By offering a detailed interpretation accompanied by practical examples, and allowing for guidelines to be updated to reflect technical advances, stakeholders can better navigate the regulatory landscape, ensuring that systems requiring oversight are appropriately classified and managed, while avoiding unnecessary regulatory burdens on technologies that do not pose significant AI-related risks.

3.1.2. Provider and deployer

For the same reasons outlined above concerning AI, the concepts of 'provider' and 'deployer' (formerly: 'user') should be aligned with the respective definitions of the AI Act. Importantly, however, this implies that the shift from a deployer to provider, foreseen under Article 25(1) AI Act, will also be imported into the AILD framework. According to this provision, any deployer or any third party qualifies as a provider of a high-risk AI system if they (i) put their trademark on a high-risk AI system already on the market; (ii) make a substantial modification to such an AI system; or (iii) modify the intended purpose of a non-high-risk AI system, including a general-purpose AI system, such that it becomes a high-risk AI system. Under any of the above circumstances, the former provider ceases to be considered a provider, but must closely cooperate with the new provider (Article 25(2) AI Act).

While the first and the third scenario are fairly easy to delineate and can be avoided by persons and entities not wishing to be considered providers, the crux of the provision lies in the delineation of the substantial modification. Here again, the AILD should align with the AI Act. The latter defines a substantial modification, in Article 3(23) AI Act as a 'change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider and as a result of which the compliance of the AI system with the requirements [for high-risk AI systems] is affected or results in a modification to the intended purpose for which the AI system has been assessed.'

Recital 109 AI Act stresses that entities engaging in fine-tuning should be considered providers for that modification of the model only. Nonetheless, under Article 25(1) AI Act, a substantial modification will ultimately likely imply a significant change of the risk profile of the respective AI system. Importantly, the AILD could stress that the simple fine-tuning of general-purpose AI systems does not, generally, lead to substantial modification, unless specific circumstances obtain

When Generative AI Exhibits Bias, and What Can Be Done About It', in P. Hacker, A. Engel, S. Hammer and B. Mittelstadt, *Oxford Handbook on the Foundations and Regulation of Generative AI* (OUP, forthcoming).

(e.g. removal of safety layers or fine-tuning on a significantly biased data set).[75] Otherwise, the use of foundation models, or other general-purpose AI systems, in any setting could be greatly hindered if deployers who merely use standard techniques to tailor the model to their needs were considered providers and, hence, had to fulfil the wide-ranging rules for providers of high-risk AI systems.

3.1.3. General-purpose AI system

The AI Act now also contains rules on 'general-purpose AI systems'. These are defined as AI systems based on 'a general-purpose AI model'; this, in turn, is a model 'that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market' (Article 3(63) AI Act).

The concept of a general-purpose AI model, hence, closely aligns with the definition of a 'foundation model' in research.[76] Its effect on the AILD, however, is limited at the moment (except the change from a deployer to a provider outlined above) because the AILD, having been drafted before the integration of general-purpose AI models in the AI Act, does not contain this term yet (see below, Section 3.4).

3.1.4. Risk

Furthermore, as it behooves a piece of risk-based regulation, the AI Act also defines the concept of risk as 'the combination of the probability of an occurrence of harm and the severity of that harm' (Article 3(2) AI Act). This effectively enshrines current concepts of risk regulation and cost-benefit analysis in EU law.[77]

Again, the effect on the AILD is marginal since 'risk' is not explicitly referenced as a concept in it. However, the same reasons as above, pertaining to coherence and compliance, speak in favour of taking over the concept of 'risk' in the AILD from the AI Act. As we shall presently see, this does not necessarily imply that the concept of a 'high-risk AI system' needs to be identical in the AI Act and the AILD. For a more detailed discussion of the concept of risk, the inclined reader is referred to the literature.[78]

3.1.5. AI literacy

A final, novel and key provision of the AI Act is Article 4. It compels providers and deployers of all AI systems – irrespective of their risk status – to 'take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf'. Articles 4 and 3(56) AI Act further define the concept of AI literacy.

This raises the question of whether a (plausible) breach of Article 4 AI Act should trigger the evidence disclosure duty and the rebuttable presumption under Articles 3 and 4 AILD. Such rules would be, arguably, overly broad: one AI-illiterate staff member *anywhere* in the company would

---

75 C. Novelli and others, 'A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities', Working Paper, 2024, p. 9.

76 R. Bommasani and others, 'On the opportunities and risks of foundation models', arXiv preprint arXiv:210807258, 2021, pp. 2-3.

77 See M. E. Kaminski, 'Regulating the Risks of AI', *Boston University Law Review*, Vol. 103:1347, 2023, pp. 1403-1405.

78 See e.g. M. E. Kaminski, 'Regulating the Risks of AI', *Boston University Law Review*, Vol. 103:1347, 2023, pp. 1375 et seqq. and pp. 1390 et seqq.; E. J. Mishan and E. Quah, *Cost-Benefit Analysis,* Routledge, 6th edn, 2020, Ch. 34; P. Hacker, 'The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, pp. 9-10.

then lead to the severe consequences of Articles 3 and 4 AILD, without any evidence linking that individual to the damage at hand.

It seems preferable to sanction a breach of Article 4 AI Act in more tailored ways. For deployers of high-risk systems, Article 26(2) of the AI Act mandates that human oversight be assigned to individuals with the necessary competence, training, and authority. Any breach of this specific requirement already triggers the evidence disclosure mechanism (Article 3(1) AILD) and, in certain cases, a rebuttable presumption (Article 4(2) AILD).[79] This would ensure that only the individual implicated in the damaging actions will be concerned. Similarly, for providers of high-risk AI systems, breaches of Article 4 AI Act that relate to the direct duties outlined in Articles 9-16 AI Act, such as risk management, performance and data governance, are also subject to these same sanctions. These provisions ensure that accountability is focused on individuals directly involved in oversight of the AI system at issue. Hence, they offer more targeted and relevant protection than a broad rule referencing any breach of Article 4 AI Act.

For non-high-risk AI systems, general rules like Article 4(5) AILD offer protections: if the complainant faces excessive difficulties in proving the causal link between a breach of Article 4 AI Act and some specific output, or lack thereof. If, by contrast, any breach of Article 4 AI Act led to an access right under Article 3 AILD, this might enable excessive scrutiny of individual staff members' training and competence levels. Furthermore, such demands might conflict with GDPR provisions and would generally raise concerns about the data protection and privacy of said individuals.

Introducing an additional evidence disclosure rule and a rebuttable presumption for AI literacy breaches across all staff, therefore, seems unnecessary and could lead to excessive demands on companies. The existing legal mechanisms already address the specific responsibilities of those directly involved in AI-related incidents. Arguably, they make further provisions for lack of AI liability superfluous. Overall, the link between the lack of AI literacy concerning a staff member who does not relate to the damaging actions and actual damage is too weak to justify such a broad obligations and presumptions, as any direct involvement can already be tackled through the specific duties outlined in Articles 9 ff. and 26(2) of the AI Act, and the respective consequences of their breach in the AILD.

3.1.6. Recommendation

The main conclusion is to largely adopt the definitions from the AI Act for the sake of coherence. Additional rules for sanctioning the breach of Article 4 AI Act do not seem advisable. However, as the next section will show, some new concepts will have to be included in the AILD to accommodate the idiosyncrasies of liability versus direct AI regulation.

3.2. High-risk AI systems in the AI Act and in the AILD

3.2.1. Societal versus individual risk

The alignment of high-risk AI system classifications between the AI Act and the AILD is a subject of debate.[80] While ensuring consistency in defining AI across regulations is crucial, the direct transplantation of high-risk classifications from the AI Act into the AILD raises concerns. Specifically,

[79] See also the amended proposal for an Artificial Intelligence Liability Directive, circulated by the European Commission, and discussed in L. Bertuzzi, 'Updated AI liability proposal sent to EU legislators, with some significant changes', MLex, 26 July 2024.

[80] See M. C. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, p. 18; J. De Bruyne, O. Dheu and C. Ducuing, 'The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive', *Computer Law & Security Review*, Vol. 51, Article 105894, 2023, p. 4 (both on autonomous vehicles); P. Hacker, 'The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Article 105871, Vol. 51, 2023, pp. 9-10.

the AI Act's focus on certain high-risk use cases – such as biometric identification and emotion recognition, employment, credit scoring, or health and life insurance – does not encompass the full spectrum of AI applications that could pose significant liability risks to individuals. Notably, applications like autonomous vehicles and broader insurance models, which are not be covered under the current high-risk categories of the AI Act, demonstrate that the potential for harm can extend beyond the prescribed classifications.[81]

Hence, the current approach to categorising high-risk AI systems under the AI Act may not fully align with the necessities of an AI liability framework. This is because the AI Act primarily considers societal-level risks without adequately addressing the variances in individual risk exposure. For instance, a scenario where a small number of individuals in a larger population are significantly harmed by an AI system might not meet the threshold for a high-risk classification under the AI Act. Yet, from a liability perspective, the impact on those individuals underscores the need for a more nuanced approach to risk classification that acknowledges both societal and individual perspectives on risk.

Therefore, while the AI Act and the AILD share a foundational goal of regulating AI to safeguard against potential harms, their criteria for classifying high-risk AI systems could diverge to better address the complexities of AI-related damages and ensure effective legal redress for affected individuals. This divergence would allow the AILD to provide a more comprehensive framework that captures a wider range of AI applications with significant risk potentials to individuals.

3.2.2. Recommendation

The upshot of the previous analysis is that, either, high-risk AI systems could be defined differently under the AILD than under the AI Act, or the legal consequences currently reserved for high-risk systems under the AILD could be extended to other use cases, while maintaining the alignment of the concept of high-risk systems between the two acts.

The latter approach is preferable for the following reasons. On the one hand, as with the other concepts reviewed, it seems imperative to maintain the identity of the foundational concept of 'high-risk AI system' between the AI Act and the AILD, for the sake of clarity and coherence. On the other hand, to address the comprehensive spectrum of potentially individually harmful AI applications and their potential impacts, the scope of application for Articles 3 and 4(2-4) of the AILD should be moderately expanded. As mentioned, this expansion is critical for including a wider array of AI applications, which present significant risk potentials not fully encapsulated by the current AI Act high-risk categories. This primarily concerns:[82]

- general-purpose AI systems
- OLF systems
  - autonomous vehicles
  - transportation-related AI applications more generally
  - other AI systems falling under Annex I Section B AI Act
- and insurance applications beyond health and life insurance.

To effectively encompass these varied use cases under a unified conceptual framework, it would be prudent to introduce a new category in the AILD, such as 'high-impact AI systems',[83] to replace the

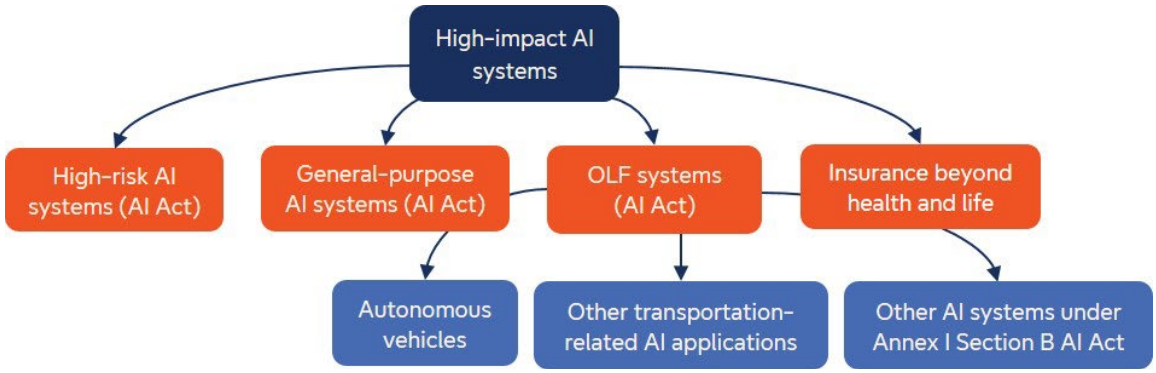
[81] id.

[82] See e.g. S. Wachter, 'Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond', *Yale Journal of Law and Technology,* Vol. 26(3), 2024, p. 671, p. 716: 'the risk categories in Annex III are insufficient. AI in media, science and academia, most financial services and trading, and most types of insurance, as well as recommender systems, chatbots, pricing algorithms, and G[enerative] AI, exhibit well-known and systemic risks for both individuals and society.'

[83] The Canadian AIDA, for example, uses the term 'high-impact AI system' instead of 'high-risk AI system' to delineate those systems that it is subject to specific scrutiny and regulation (Sec- 7-12 AIDA). The definition is, however, left to

current focus on high-risk AI systems. This category would encompass *both* the existing high-risk systems, as per Article 6 AI Act, and the newly identified areas of concern, as visualised below in Figure 2.

Figure 2 – Visualisation of the new 'high-impact AI systems' category



Source: Author.

3.3. Articles 9-15 AI Act and the AILD presumption of liability

3.3.1. Presumption of causality

The AILD aims to simplify the process for individuals seeking compensation for damages caused by AI systems, especially when these damages result from non-compliance with a duty of care established by Union or national laws. However, identifying the specific fault causing an AI's output can be challenging, due to the opacity and autonomy of AI systems. The proposed directive, therefore, introduces a rebuttable presumption of causality in Article 4(1), aiding claimants in linking non-compliance to the AI's harmful output or lack thereof.

This presumption approach represents a significant advancement in enforcing the AI Act and compensating affected individuals. Generally, the presumption of causality under the AILD for breaches of Articles 9-15 AI Act by providers is largely appropriate. Nevertheless, it does not fully encapsulate the complex nature of AI functionality and accountability, particularly in scenarios where post-output processes could mitigate initial non-compliance or where actions must be taken, according to the AI Act, after the output was produced.[84]

First, the framework should allow for the presumption to be rebutted in instances where initial violations of the AI Act are effectively 'cured' in subsequent stages of the AI development or deployment process, such as through the application of post-processing mechanisms that rectify biases in training data.

Second, the presumption of a causal link between fault and the subsequent output of an AI system becomes particularly problematic in cases involving a violation of Article 14 AI Act. Article 14 emphasises the necessity of incorporating mechanisms for human oversight into AI systems, allowing for the correction or modification of outputs after they have been produced. Given this focus, establishing a direct link between the fault – specifically, the omission of human oversight capabilities in the AI model's design – and the output itself does not logically hold, as the output

further implementing acts ('high-impact system means an artificial intelligence system that meets the criteria for a high-impact system that are established in regulations', Article 5(1) AIDA; see also Sec. 36(b) AIDA).

84 ibid, p. 24.

does not depend on this particular fault.[85] The same problem arises concerning the monitoring duty of the deployer, now established in Article 26(2) and (5) AI Act, mentioned in Article 4(3) AILD.

An explanation for this peculiarity is that Article 14's and 26's breach relates to the structural features of the AI system, namely its capacity for post-production intervention by humans, rather than the specific characteristics of the output generated. Thus, if an AI system lacks designed-in opportunities for human oversight, this deficiency does not inherently affect the output's nature or its potential to cause damage. Instead, the fault lies in the failure to provide a means for rectifying or altering outputs that might be identified as problematic or harmful post-generation, a scenario distinct from the direct causation typically associated with output-related damages. Similarly, the failure to monitor AI output cannot influence that output as it precedes it.

3.3.2. Recommendations

First, to ensure clarity for providers and reflect the dynamic nature of AI technologies, it is recommended that Article 4 of the AILD explicitly include the possibility for a rebuttal based on safeguards introduced in the AI pipeline that 'heal' the previous violation of a specific rule (e.g. post-processing mechanisms). This addition would acknowledge the potential for AI systems to evolve and improve throughout the pipeline without constraining providers to pick the solution they deem best.

Second, a new presumption should be incorporated within Article 4 AILD, explicitly establishing a causal link between the output of an AI system and any resultant damage in instances of non-compliance with Articles 14 and 26(2) and (5) AI Act (instead of the link between fault and output). The reason for this addition is grounded in the recognition, mentioned above, that a breach of Article 14 directly impedes the possibility of human intervention that could otherwise rectify an erroneous output and, thereby, prevent the damage. In scenarios where Article 14's provisions are violated, the direct opportunity to alter or halt a damaging output before it manifests harm is effectively removed. Similarly, the failure to effectively monitor the output or system behaviour (Article 26(2) and (5) AI Act) renders it all but impossible to intervene before damage is done. The presumptions could be rebutted by showing that is highly unlikely that appropriate oversight would have spotted or corrected the output, or otherwise prevented the damage.

Third, the proposed framework necessitates amendments to address damages caused by deploying prohibited AI systems as outlined in Article 5 of the AI Act.[86] In an ideal scenario, such cases would invoke a regime of strict liability, solely predicated on establishing a causal relationship between deploying the banned system and the ensuing harm (see Section 3.5).

As a practical yet equally effective alternative, the AILD could automatically assume both fault and a direct causal link between this fault and the outcome produced by the AI, without room for rebuttal. Injured persons then would only have to demonstrate the use of a prohibited system, and the causal damage resulting from its output.

---

[85] See P. Hacker, 'The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Article 105871, Vol. 51, 2023, pp. 23-24; J. Laux, 'Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of AI governance under the European Union AI Act', *AI & SOCIETY*, 2023, p. 1, p. 10.

[86] G. Wagner, 'Liability Rules for the Digital Age – Aiming for the Brussels Effect', *Journal of European Tort Law*, Vol. 13(3), 2022, p. 191.

3.4. The effects of the new general-purpose AI system rules on the AILD

3.4.1. Risks of GPAI

Foundation models and generative AI, such as ChatGPT, qualify as 'general-purpose AI models/systems' (GPAI) under the AI Act. However, these technologies are not classified as high-risk under the current AI Act framework. While there are good reasons for this framing within the AI Act,[87] it has significant consequences for the AILD, which almost exclusively focuses on high-risk applications where only the very limited causality presumption under Article 4(5) and (6) would apply. Hence, arguably, GPAI is not adequately covered by the AILD, despite their significant potential for both good and harm.[88]

General-purpose AI systems can immediately lead to various liability-relevant issues, such as insults, discrimination, and violations of personality rights, as numerous examples of hate speech,[89] libel,[90] non-consensual intimate images, deep fake porn and CSAM,[91] and other harmful content generated by AI demonstrate.

The inherent unpredictability in generative AI output, often based on the inclusion of random variables,[92] combined with the opacity concerning model development as well as safety and security layers, further exacerbates the challenge of supporting injured parties. Unlike non-generative AI systems, which are generally deterministic, generative AI systems operate probabilistically.[93] They offer different types of output for the same input over time, making the establishment of a causality link between the – potentially faulty – design of these systems and specific harmful outputs particularly difficult. The risks for important fundamental rights in the non-discrimination and personality field are comparable to those posed by high-risk AI systems to physically grounded rights (property, health and life) – but the alleviations offered to injured parties currently are not.

3.4.2. Recommendation

Given these considerations, there is a pressing need for new liability rules in the AILD to address the risks posed by general-purpose AI systems.[94] It is recommended that these AI systems be categorised under the new 'high-impact' classification, which would bring them within the ambit of

---

87 See e.g. P. Hacker, A. Engel and M. Mauer, 'Regulating ChatGPT and other Large Generative AI Models', *ACM Conference on Fairness, Accountability, and Transparency (FAccT '23), 2023, p.* 1112; but see also N. Helberger and N. Diakopoulos, 'ChatGPT and the AI Act', *Internet Policy Review*, Vol. 12, 2023.

88 Quite obviously, GPAI has tremendous potential for socially beneficial applications, too. Those are not the focus of this study, though.

89 See e.g. C. Stokel-Walker and R. Van Noorden, 'The Promise and Peril of Generative AI', *Nature*, Nature Research, Vol. 614, pp. 214-215; J. Von Lindern, 'Braucht die deutsche Vorzeige-KI mehr Erziehung?' Zeit Online, 11 September 2023.

90 P. Verma and W. Oremus, 'ChatGPT invented a sexual harassment scandal and named a real law prof as the accused' *The Washington Post*, 5 April 2023; K. McGuffie and A. Newhouse, 'The radicalization risks of GPT-3 and advanced neural language models', arXiv preprint arXiv:200906807, 2020.

91 See e.g. K. Mania, 'Legal protection of revenge and deepfake porn victims in the European Union: Findings from a comparative legal study', *Trauma, Violence, & Abuse*, Vol. 25, December 2022, p. 117; A. Mahdawi, 'Nonconsensual deepfake porn is an emergency that is ruining lives', *The Guardian,* 1 April 2023; D. Thiel, Identifying and Eliminating CSAM in Generative ML Training Data and Models, Stanford University, December 2023.

92 D. Ganguli and others, 'Predictability and surprise in large generative models', *ACM Conference on Fairness, Accountability, and Transparency*, 2022, p. 1747.

93 D. Foster, *Generative Deep Learning*, *O'Reilly*, 2022, pp. 4-5.

94 See also C. Novelli and others, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity', arXiv preprint arXiv:240107348, Working Paper, March 2024, p. 4.

more stringent regulatory requirements, as discussed above (see Section 3.2). Essentially, they would be treated as high-risk AI systems are treated in the current AILD draft.

1. Evidence disclosure requirement: generative AI, including technologies like ChatGPT, should be explicitly included in the rules of Article 3 of the AILD, which currently only applies to high-risk systems. This adjustment would ensure that evidence disclosure mechanisms are in place to aid in the legal processes involving generative AI, acknowledging the opaque and probabilistic nature of these systems and the challenges they pose in litigation.[95]

2. Presumption of causality for violations: a breach of Article 55 AI Act, which lays down safety rules for general-purpose AI systems, should trigger a presumption of a causal link between the violation and any concrete harmful output produced by the system. This presumption would facilitate the process for claimants seeking redress for damages caused by such AI systems by acknowledging the difficulty in directly linking design decisions to specific instances of harm.

Importantly, under such an approach, injured parties should still be able to show fault by the providers of GPAI beyond the violation of Article 55 AI Act: this provision only applies to a very small set of GPAI with systemic risk (potentially only GPT-4 and some Gemini and/or Claude versions[96]), unless the Commission explicitly designates further models as exhibiting systemic risk. Elements of fault, in this context, could be: insufficient content moderation policies during development and deployment; lack of continued testing for harmful content; and the lack of notice and action mechanisms enabling user feedback on particularly harmful forms of output.[97] Injured parties would still, with the help of the disclosed evidence, have to prove fault, but would be relieved of proving the causal link to the specific output under an expanded Article 4 AILD.

3.5. The scope of the PLD and of the AILD – remaining loopholes?

Perhaps the most important question concerning the relationship between the revised PLD and the AILD addresses their respective scope of application, areas of overlap, and of unique added value.

At first glance, since the PLD has been enacted, the AILD might indeed seem superfluous as it contains primarily procedural elements, such as evidence disclosure mechanisms and rebuttable presumptions, already contained in the PLD. Such an analysis would, however, be incomplete. The scope of the PLD, and of the AILD, is not unidimensional, but multifaceted. Indeed, concerning the material scope of 'AI,' no liability loophole exists anymore once the PLD has been extended to software, including AI.

Similarly, concerning the personal scope of liable parties, the relevant actors in the AI value chain are covered by the PLD: chiefly, the providers, typically the technical developers or those having models developed for them. This makes sense as they control the risk profile of the AI model. From an economic perspective, they should be incentivised to act with the required care.

[95] See for more details, ibid, p. 6 et seqq.

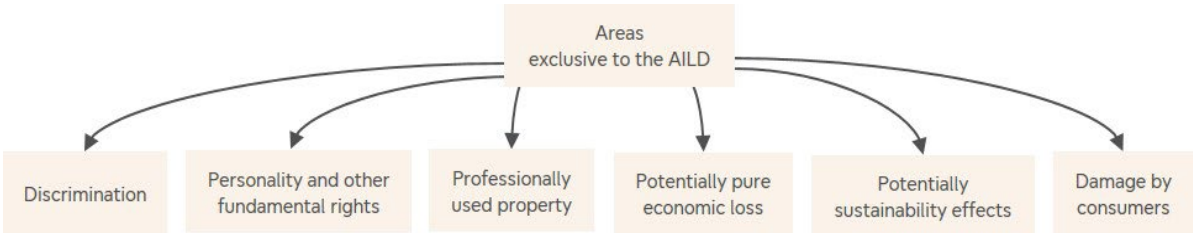
[96] The Future Society, EU AI Act Compliance Analysis: General-Purpose AI Models in Focus, December 2023.

[97] See C. Novelli and others, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity', arXiv preprint arXiv:240107348, Working Paper, March 2024, pp. 5-6.

Two critical areas remain unaddressed, however, by the PLD,[98] necessitating the enactment of the AILD to bridge these gaps, as visualised below in Figure 3.[99]

1. **Personal scope of application**. The PLD's provisions are explicitly tailored for professionals and economic operators, leaving a regulatory void when it comes to non-professional users. Unlike the PLD, the AILD is designed to encompass not only professional but also non-professional users of AI. This inclusion is crucial for ensuring comprehensive liability coverage across all user types, including consumers who interact with AI technologies (e.g. generative AI applications). Furthermore, the AILD would also apply to professional users whose property is damaged, who are excluded by the PLD.
2. **Eligible Damage**. The PLD currently specifies a narrow range of damages eligible for compensation, creating significant loopholes in coverage. Key areas omitted include:[100]
    - **discrimination**: instances where AI systems lead to discriminatory outcomes, impacting individuals or groups unfairly;
    - **personality and other fundamental rights**: violations involving personal rights, as in toxic, non-consensual intimate, and other harmful content. Other fundamental rights coming into play are privacy; dignity; and potentially family-related rights;[101]
    - **professionally used property**: infringements related to property used in a professional context. This includes intellectual property rights potentially violated by the training or use of generative AI systems;
    - **pure economic loss**: damages not associated with physical harm or property damage but with direct financial losses, critical in many AI-related incidents (e.g. finance);
    - **sustainability**: questions relating to the environmental and climate impact of AI systems.

Figure 3 – Areas covered by the AILD but not by the PLD



Source: Author.

98 See ibid, p. 5 Fn. 9; G. Spindler, 'Die Vorschläge der EU-Kommission zu einer neuen Produkthaftung und zur Haftung von Herstellern und Betreibern Künstlicher Intelligenz', *Computer und Recht*, Verlag Dr. Otto-Schmidt, Vol. 38(11) 2022, p. 689, p. 704; P. Hacker, 'The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 11, pp. 27 et seqq., pp. 36 et seqq.; A. M. Marinkovic, Liability for AI-related IP infringements in the European Union, *Journal of Intellectual Property Law & Practice*, 2024, pp. 5-6.

99 See also pp. 9-10 of the Explanatory Memorandum of the AILD proposal.

100 See e.g. S. Wachter, 'Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond', *Yale Journal of Law and Technology*, Vol. 26(3), 2024, p. 671, p. 717.

101 See also pp. 9-10 of the Explanatory Memorandum of the AILD proposal.

3.5.1. Discrimination

Discrimination under the PLD

Within the context of the PLD, discriminatory outputs by AI systems are not explicitly ruled out as constituting a product defect, yet the proposal does not directly incorporate references to non-discrimination directives.[102] This omission suggests a reluctance to integrate EU non-discrimination law into the defectiveness concept under the PLD framework, with the European Commission[103] and some scholars[104] viewing discrimination issues as outside the scope of PLD claims. Conversely, given the strong public and user expectations around non-discrimination in AI systems, an argument can be made for considering these aspects on a case-by-case basis within the AI liability framework to ensure it doesn't become ineffective in areas where enforcement is crucial.[105]

Discrimination under the AILD

The causality presumption in Article 4(2) AILD proposal refers to Article 10 (data governance) and 15 AI Act (feedback loops), which cover non-discrimination cases. However, the extent to which the AILD applies to liability for discrimination by AI systems remains unclear, and deserves further scrutiny. The AILD establishes a clear distinction between strict and fault-based liability, with implications for applying the causality presumption to non-discrimination cases. As the CJEU has repeatedly pointed out,[106] liability for discrimination follows a strict liability regime. This does not align well with the fault-based premises of Article 4 AILD.

By contrast, the European Commission[107] and some scholars[108] seem to regard discrimination as fault. This does not necessarily have to be the case, though. Clearly, there will be instances where a duty of care was breached, leading to discrimination by an AI system: for example, if heavily biased training data was used (violation of Article 10 AI Act). Nevertheless, there will probably also be cases involving a discriminating output that cannot be linked to any specific breach of a behavioural duty on the part of the provider. Generative AI systems, for example, may come up with unexpected and harmful output even if all the state-of-the-art security, safety and moderation policies were heeded.[109] In such cases, it seems difficult to locate an element of fault in the actions of the provider

---

102 These directives include, for example, Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin; Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation; Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services; and Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation.

103 European Commission, Questions and answers on the revision of the Product Liability Directive, 2022, under point 5.

104 G. Wagner, 'Liability Rules for the Digital Age – Aiming for the Brussels Effect', *Journal of European Tort Law*, Vol. 13(3), 2022, p. 241.

105 P. Hacker, 'The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 37.

106 CJEU, Case C-177/88, Dekker, ECLI:EU:C:1990:383; CJEU, Case C-180/95, Draehmpaehl, ECLI:EU:C:1997:208; see also Thüsing, '§ 15 AGG', in Münchener Kommentar BGB, 9th ed. (Beck, 2021), para. 24; Stoffels, 'Grundprobleme der Schadensersatzverpflichtung nach § 15 Abs. 1 AGG', RdA 2009, 204, 210.

107 European Commission, Questions and answers on the revision of the Product Liability Directive, 28 September 2022, under point 5; G. Spindler, 'Die Vorschläge der EU-Kommission zu einer neuen Produkthaftung und zur Haftung von Herstellern und Betreibern Künstlicher Intelligenz', *Computer und Recht*, Verlag Dr. Otto-Schmidt, Vol. 38(11) , 2022, p. 704.

108 G. Spindler, 'Die Vorschläge der EU-Kommission zu einer neuen Produkthaftung und zur Haftung von Herstellern und Betreibern Künstlicher Intelligenz', *Computer und Recht*, Verlag Dr. Otto-Schmidt, Vol. 38(11) , 2022, p. 704.

109 Cf. S. Sterlie, N. Weng and A. Feragen, 'Non-discrimination Criteria for Generative Language Models', arXiv preprint arXiv:240308564, 2024; A. Haim, A. Salinas and J. Nyarko, 'What's in a Name? Auditing Large Language Models for Race and Gender Bias', arXiv preprint arXiv:240214875, 2024; H. Kotek, R. Dockum and D. Sun, 'Gender bias and stereotypes in large language models', Proceedings of the ACM Collective Intelligence Conference, 2023, p. 12.

or deployer. Strict liability for discrimination, however, suggests that liability still follows from such a scenario (possibly joint and several liability of the provider and deployer).

Article 3 AILD, in contrast, does not presuppose fault, at least not according to its wording. However, with its focus on high-risk systems, it currently does not cover generative AI, which should be changed (see Section 3.4).

Recommendation

It should be made clear that the AILD applies to cases of liability for discrimination. The necessity for evidence disclosure mechanisms and a rebuttable presumption in discrimination cases is underscored by existing enforcement challenges[110] and the legal precedent set by the CJEU, which currently restricts access to data and algorithms critical for proving discrimination (as seen in the Meister case[111]).[112] These challenges highlight the need for the AILD to explicitly cover discrimination.[113] With this, the AILD would offer a comprehensive framework that includes provisions for evidence disclosure and shifts the burden of proof concerning causality in discrimination cases involving fault.

Such measures are essential for addressing the practical barriers faced in litigating discrimination claims within the AI context, where access to underlying data and decision-making processes is crucial for establishing a prima facie case. To the extent that an element of fault can be located, and may be needed under certain national transpositions (in spite of the CJEU jurisprudence), the causality presumption will indeed be helpful.

3.5.2. Generative AI and personality rights

The PLD and personality rights

Whether the EU's product liability framework encompasses *information* has been contested among scholars.[114] This debate is especially relevant given the CJEU's distinction of information (such as content in a print newspaper) from the concept of a 'product' in the Krone verdict.[115] Whether that differentiation actually applies to generative AI content is, however, questionable: the output from generative AI, unlike a newspaper article, is deeply integrated with the AI model itself (i.e. the product); hence, the PLD could still be relevant.[116] However, the PLD does not compensate for

---

110 S. Wachter, B. Mittelstadt and C. Russell, 'Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI', *Computer Law & Security Review*, Vol. 41, Article 105567, 2021, p. 10; F. J. Zuiderveen Borgesius, 'Strengthening legal protection against discrimination by algorithms and artificial intelligence', *The International Journal of Human Rights*, Vol. 24(10), Taylor & Francis Online, 2020, p. 1572, pp. 1577 et seqq.; P. Hacker, 'Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law', *Common Market Law Review*, Vol. 55, 2018, pp. 1143, p. 1168.

111 CJEU, Case C-415/10, Meister, ECLI:EU:C:2012:217, paras. 46-47.

112 P. Hacker, 'The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 18 and p. 37.

113 This is also supported by G. Wagner, 'Liability Rules for the Digital Age - Aiming for the Brussels Effect', *Journal of European Tort Law*, Vol. 13(3), 2022, p. 237.

114 See e.g. G. Howells, C. Twigg-Flesner and C. Willett, 'Product liability and digital products', in Synodinou T.-E. and others (eds), *EU Internet Law* (Springer 2017), p. 183; G. Wagner, 'Liability Rules for the Digital Age - Aiming for the Brussels Effect', *European Journal of Tort Law*, Vol. 13(3), 2022, p. 200.

115 Judgment in CJEU, Case C-65/20 - Krone, ECLI:EU:C:2021:471, para. 42; see also V. Mantrov, 'Newspaper Advice That Causes Damage Is Not Covered by the Product Liability Directive: The Court of Justice of the European Union's Clarification in Krone', *European Journal of Risk Regulation*, Vol. 14, 2023, p. 416.

116 A. Haftenberger, *Die Produkthaftung für künstlich intelligente Medizinprodukte*, Nomos, 2023, p. 87 et seqq.; J. van Staalduinen,'The Doctor and the Missing Link-EU Product Liability for Clinical (AI) Decision Support Systems', 2023 p. 11; P. Hacker, F. Zuiderveen Borgesius, B. Mittelstadt and S. Wachter, 'Generative Discrimination. What Happens When Generative AI Exhibits Bias, and What Can Be Done About It', in P. Hacker, A. Engel, S. Hammer and B. Mittelstadt, *Oxford Handbook on the Foundations and Regulation of Generative AI* (OUP, forthcoming).

infringements on personality rights[117] or other fundamental rights, such as privacy, data protection, dignity, family-related rights, and others that may be protected by Member State tort law.[118] This highlights a significant limitation in its applicability.

While Article 82 of the GDPR offers a pathway for addressing violations of personality rights stemming from personal data processing,[119] precedents in this specific context are lacking. EU law providing compensation for the violation of the other fundamental rights just mentioned (e.g. personality rights) does not exist. This gap underscores the necessity for the AILD to provide coverage, particularly regarding evidence disclosure mechanisms and the causality presumption. Situations such as the absence of advanced content moderation policies during an AI system's training and deployment phase, the omission of continuous testing, and the failure to implement a notice and action mechanism could all potentially lead to the recognition of fault engendering violations of personality rights.[120]

Recommendations

Given these considerations, it is recommended that the AILD be applied to the violation of personality rights sanctioned by Member State law to bridge the mentioned gap. Again, this would necessitate the inclusion of general-purpose AI models and systems in the provisions for evidence disclosure and causality presumption, mirroring the legal approach to addressing discrimination.

3.5.3. Pure economic loss and professionally used property

It is debatable whether the PLD itself should cover pure economic loss and damage to professionally used property.[121] Ultimately, the PLD revision will not apply to either of these categories (Article 5a(1) PLD). Pure economic loss is particularly important for AI products in finance and insurance, two high-risk areas of the AI Act (credit scoring, health and life insurance) which are, ironically, not covered by the PLD at all. Similarly, professionally used property is obviously crucial in industrial and general B2B applications of AI.

However, to the extent that the tort law of Member States does extend AI liability to pure economic loss and professionally used property, these categories should also benefit from the same protections and alleviations of proof as damage to consumer property. There is no convincing reason justifying a different degree of protection for these assets, equally protected by fundamental rights. Even professional parties merely using AI products typically do not have better access to data and algorithms of AI providers than consumers. Hence, Articles 3 and 4 AILD are needed, in addition to the provisions of the PLD, in this context as well.

Notably, this brings the entire suite of intellectual property (IP) rights within the ambit of the AILD: they are usually used professionally, hence not covered by the PLD; but the AILD would alleviate the burden of proof for IP rights holders as it may be argued that any infringement of national IP laws

---

117 G. Wagner, 'Liability Rules for the Digital Age – Aiming for the Brussels Effect', *Journal of European Tort Law*, Vol. 13(3), 2022, p. 236.

118 See also pp. 9-10 of the Explanatory Memorandum of the AILD proposal.

119 P. Hacker, Datenprivatrecht: Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB, Mohr Siebeck, 2020, p. 520 et seqq.

120 P. Hacker, F. Zuiderveen Borgesius, B. Mittelstadt and S. Wachter, 'Generative Discrimination. What Happens When Generative AI Exhibits Bias, and What Can Be Done About It', in P. Hacker, A. Engel, S. Hammer and B Mittelstadt *Oxford Handbook on the Foundations and Regulation of Generative AI* (OUP, forthcoming), p. 35; see also G. Kastl-Riemann, 'Regulation of Generative AI Speech: an EU perspective', in P. Hacker, A. Engel, S. Hammer and B. Mittelstadt, *Oxford Handbook on the Foundations and Regulation of Generative AI* (OUP, forthcoming).

121 See e.g. G. Wagner, 'Liability Rules for the Digital Age – Aiming for the Brussels Effect', *Journal of European Tort Law*, Vol. 13(3), 2022, p. 235 et seqq.; P. Hacker, 'The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 28; S. A. Nawaz, 'The Proposed EU AI Liability Rules: Ease or Burden?', European Law Blog, 2022.

breaches the relevant duty of care.[122] The violation of these rights is a major concern particularly in the development of generative AI models.[123]

3.5.4. Sustainability harms

Finally, climate harms and sustainability risks arising from the mass deployment of large AI models,[124] such as soaring energy and water consumption during both training and inference and the use of toxic materials, are not adequately covered in the AI Act or the PLD.[125] For example, the rendering of one image with a state-of-the-art image generator consumes as much energy as fully charging a smartphone;[126] a longer conversation with ChatGPT consumes ca. 500 ml of water;[127] and the estimated GHG emissions for AI will equal those of the entire Netherlands in 2027.[128] Again, Member States may introduce novel ways of linking climate costs to liability, or the judiciary may use or extend existing liability frameworks to environmental harms possibly traced to AI.[129] While this is only an option for Member States, in these cases, again, such litigation should also benefit from the alleviations contained in the AILD, reinforcing the need for a separate AILD framework beyond the PLD.

3.5.5. Overall recommendations: Beyond the PLD

The enactment of the revised PLD marks a significant step in the evolution of EU liability law, particularly in the context of new technologies. However, the PLD presents notable gaps, especially in areas such as protection against discrimination, personality rights, and coverage for professionally used property. It also lacks measures for addressing pure economic loss and sustainability harms, as well as damage caused by consumers, which are contingent on Member State laws. These limitations

---

122 A. M. Marinkovic, Liability for AI-related IP infringements in the European Union, *Journal of Intellectual Property Law & Practice*, 2024, pp. 5-6.

123 G. Marcus and R. Southen, Generative AI Has a Visual Plagiarism Problem, IEEE Spectrum, 2024; P. Samuelson, Generative AI meets copyright, Science, American Association for the Advancement of Science, Vol. 381(6654), 2023, p. 158; C. Novelli and others, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity', arXiv preprint arXiv:240107348, 2024, pp. 15-22; K. de la Durantaye, Garbage In, Garbage Out. Regulating Generative AI Through Copyright Law, *ZUM*, Vol. 10, 2023, p. 645; A. M. Marinkovic, Liability for AI-related IP infringements in the European Union, *Journal of Intellectual Property Law & Practice*, 2024, p. 3 et seqq.

124 See e.g. A. S. Luccioni, Y. Jernite and E. Strubell, 'Power Hungry Processing: Watts Driving the Cost of AI Deployment?', arXiv preprint arXiv:231116863, 2023; A. de Vries, 'The growing energy footprint of artificial intelligence', *Joule*, 2023; B. Knowles and others, 'Our house is on fire: The climate emergency and computing's responsibility', *Communications of the ACM*, Vol. 65, 2022; C. Freitag and others, 'The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations', *Patterns*, Vol. 2, Article 100340, 2021; M. Taddeo and others, 'Artificial intelligence and the climate emergency: Opportunities, challenges, and recommendations', *One Earth*, Vol. 4., 2021; Tech. Policy Council ACM, ACM TechBrief: Computing and Climate Change, 2021; P. Li and others, 'Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models', arXiv preprint arXiv:230403271, 2023.

125 P. Hacker, 'Sustainable AI Regulation', *Common Market Law Review*, Vol. 61, 2024.

126 A. S. Luccioni, Y. Jernite and E. Strubell, 'Power Hungry Processing: Watts Driving the Cost of AI Deployment?', arXiv preprint arXiv:231116863, 2023, p. 5 (on Stable Diffusion XL).

127 P. Li and others, 'Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models', arXiv preprint arXiv:230403271, 2023; see also G. Zuccon, H. Scells and S. Zhuang, 'Beyond CO2 Emissions: The Overlooked Impact of Water Consumption of Information Retrieval Models', *Proceedings of the 2023 ACM SIGIR International Conference on Theory of Information Retrieval*, 2023, p. 283.

128 A. de Vries, 'The growing energy footprint of artificial intelligence', *Joule*, 2023; D. Erdenesanaa, 'A.I. Could Soon Need as Much Electricity as an Entire Country', *New York Times*, 10 October 2023.

129 See e.g. M. Doelle and S. Seck, 'Loss & damage from climate change: from concept to remedy?', in M. Broberg and B. M. Romera (eds), *The Third Pillar of International Climate Change Policy*, Routledge, 2021, p. 59; F. Simlinger and B. Mayer, 'Legal responses to climate change induced loss and damage', in R. Mechler and others (eds), Loss and Damage from Climate Change: Concepts, methods and policy options, Springer, 2019, p. 179; D. A. Kysar, 'What climate change can do about tort law', Environmental Law, Vol. 41, 2011.

underscore the necessity for adopting the AILD, which proposes procedural alleviations akin to those in the PLD and extends its scope to address these areas.

The AILD's implementation is crucial because the position of injured parties regarding the ability to prove fault or causality remains challenging irrespective of the specific rights or assets harmed; indeed, it is generally independent of them. By mirroring the procedural facilitations of the PLD, the AILD enhances the legal framework and provides support for those impacted by the intricacies of AI operations. This includes procedural tools like the evidence disclosure mechanism and the rebuttable presumption, which are indispensable for claimants facing the opaque nature of AI decision-making processes.

However, addressing AI-specific issues alone may not sufficiently capture the broader challenges presented by digital technologies. The current draft of the AILD focuses exclusively on harms caused by AI systems, overlooking the similar complexities associated with many types of non-AI software. In fact, the same difficulties related to proving fault and causality exist across all software types, not just those driven by AI. The PLD's approach to encompass any software underlines the importance of a uniform legal treatment across different technological mediums.

To rectify this, it is recommended that the AILD be expanded into a more encompassing software liability instrument (SLI). This broader instrument (a directive or regulation, see below, Section 5) would not only cover AI but also all other types of software, reflecting the PLD's approach. Such an expansion would ensure that the evidence disclosure mechanisms and the principles of rebuttable presumptions apply universally to all software applications, not just to AI or high-risk AI systems. In such an SLI, the evidence disclosure mechanism should apply to all types of software; the rebuttable presumption for non-AI software should be equivalent to the rules for non-high-risk AI systems.

The necessity of going beyond the PLD is summarised by the table below. It lists the areas in which alleviations of proof, while needed, would only be afforded by the AILD (in green) and, beyond that, only by the recommended SLI (in red). The table shows that, without the AILD and the SLI, protection would be inadequate in many areas, by comparison with the new PLD: in the green boxes, comparable protection can only be achieved with the AILD; and in the red boxes, only with the SLI. Only the AILD would expand the alleviations of proof afforded contained in the PLD – evidence disclosure mechanism and the rebuttable presumption – to cases of discrimination, violations of personality rights, other fundamental rights, professionally used property, and potentially pure economic loss and sustainability harms. If such rights are violated by non-AI software, however, even the AILD does not offer redress; hence, a SLI is needed.

Table 3 – Types of software and harm covered by the revised PLD, the proposed AILD, and the recommended software liability instrument (SLI)

	Non-AI software	AI
Consumer property (PLD)	EDM, RP	EDM, RP
Health (PLD)	EDM, RP	EDM, RP
Life (PLD)	EDM, RP	EDM, RP
Discrimination (AILD/SLI)	EDM, RP	EDM, RP
Personality rights (AILD/SLI)	EDM, RP	EDM, RP
Other fundamental rights (AILD/SLI)	EDM, RP	EDM, RP
Professional property, such as IP rights (AILD/SLI)	EDM, RP	EDM, RP
Pure economic loss (AILD/SLI)	EDM, RP	EDM, RP
Sustainability harms (AILD/SLI)	EDM, RP	EDM, RP

EDM: evidence disclosure mechanism; IP: intellectual property; RP: rebuttable presumption.

Source: Author.

4. The AILD and the European Parliament resolution on AI liability

While the previous section scrutinised the interactions between the AILD, the PLD and the AI Act, the legislative options do not end there. Rather, in October 2020, the European Parliament adopted its own resolution on AI liability (the European Parliament resolution of 2020 on AI liability)[130], formally asking the European Commission to adopt a framework on AI liability based on a two-track approach: truly strict liability for high-risk AI systems, and a presumption of negligence for all other AI systems. The resolution specified claims both against providers and operators of AI systems. However, this architecture was not taken up in the PLD or AILD frameworks. Hence, the following section will analyse specifically the differences between the European Parliament resolution of 2020 on AI liability and the PLD and AILD, focusing on questions of strict liability (4.1), joint liability (4.2), and fault-based liability with the respective alleviations for proving the required elements (4.3).

4.1. Strict liability

The European Parliament resolution of 2020 on AI liability suggested a specific framework of strict liability for high-risk AI systems. In theory, such a framework could still be integrated into a fundamentally revised AILD (or SLI). To analyse its desirability, the study first elaborates on different modes of strict liability (4.1.1) before situating the European Parliament's requests under the 2020 resolution within that spectrum (4.1.2) and discussing the potential for integrating these proposals in the AILD/SLI framework (4.1.3).

4.1.1. Modes of strict liability

Strict liability is a concept with a long tradition,[131] having inspired much economically focused analysis.[132] However, at the European level, it is crucial to distinguish two fundamentally different modes of strict liability: liability for *defects* causing harm (e.g. PLD), and for mere *actions* causing harm (e.g. European Parliament resolution of 2020 on AI liability).

'Strict liability' for defects

While the European Commission[133] and parts of the legal scholarship[134] qualify the PLD as a strict liability framework, it actually provides for fault-based liability in disguise.[135] The process of identifying a defect generally implicitly involves elements of fault, not through demonstrating intent

---

130 Legislative own-initiative report, Article 225 TFEU.

131 See for a comparative overview, E. Karner, B. Koch and M. A. Geistfeld, Comparative Law Study on Civil Liability for Artificial Intelligence, 2021, p. 58 et seqq. and p. 112 et seqq.

132 See e.g. R. A. Epstein, 'A theory of strict liability', *The Journal of Legal Studies*, Vol. 2, 1973, p. 151; S. Shavell, 'Strict Liability versus Negligence', *The Journal of Legal Studies*, Vol. 9, 1980, p. 1; M. C. Buiten, 'Product liability for defective AI', *European Journal of Law and Economics*, 2024, p. 1.

133 Rec. 2 and 3 PLD: 'liability without fault'; PLD proposal, 2; AILD proposal, 2.

134 See e.g. for manufacturing and design defects: H. C. Taschner, 'Produkthaftung - Noch einmal: Verschuldenshaftung oder vom Verschulden unabhängige Haftung?', *Zeitschrift für europäisches Privatrecht (ZEuP)*, 2012, p. 560, p. 563; S. A. Nawaz, 'The Proposed EU AI Liability Rules: Ease or Burden?', European Law Blog, 2022; E. Karner, B. Koch and M. A. Geistfeld, Comparative Law Study on Civil Liability for Artificial Intelligence, 2021, pp. 50-51.

135 D. G. Owen, Products Liability Law, 3rd edition, *Thomson West*, 2015, p. 315 et seqq.; H. Zech, 'Liability for AI: public policy considerations', *ERA Forum*, Vol. 22, 2021, p. 147, p. 154; G. Wagner, 'Robot Liability', in S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019, p. 27, p. 34; G. Wagner, 'Einleitung zum Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz – ProdHaftG)', *Münchner Kommentar BGB*, 9th edition, Verlag C.H. Beck, 2021, paras. 22-25; P. Hacker, 'The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, pp. 29-30; for a nuanced account from a law and economics perspective, see M. C. Buiten, 'Product liability for defective AI', *European Journal of Law and Economics*, 2024, p. 1, p. 13.

or negligence, but rather through proving an objective breach of duty. Particularly, the concept of defectiveness under both the current and proposed PLD frameworks frequently aligns with a breach of duty of care.[136] For example, in the area of design defects, injured parties must show that a manufacturer chose a particular design over safer alternatives, thereby violating established standards of conduct.

This interpretation means that, despite the theoretical label of 'strict liability,' the PLD often functions like a fault-based framework, especially in the context of design or warning defects[137] (e.g. the design of airbags[138] or the warning of certain dangers from machinery[139]). Importantly, those are the most common types of defect in AI-related cases.[140] In practice, claimants must establish that there was a breach of duty, effectively proving fault, to succeed in their claims. This requirement positions the PLD as a framework where fault re-emerges, disguised as the need to establish product defectiveness.

Truly strict liability for actions

Truly strict liability, as a distinct legal concept, occurs when liability requires only an action causing the harm,[141] imposing liability regardless of fault in certain high-risk industries. Examples of this approach in action include liability for genetically modified organisms or damages caused by certain perilous establishments (e.g. power plants).[142] Similarly, the European Parliament's Resolution of 2020 on AI liability advocates for truly strict liability for high-risk AI systems, based on the challenges posed by these technologies (Article 4 European Parliament resolution of 2020 on AI liability).

To effectively implement truly strict liability for AI systems, however, it is necessary to distinguish between illegitimate-harm and legitimate-harm models:[143]

- **Illegitimate-harm models**: these AI systems should not cause harm during their proper operation. Examples include medical AI (e.g. cancer recognition systems) or AI in transportation systems (e.g. autonomous vehicles).
- **Legitimate-harm models**: conversely, these are systems designed to cause harm under correct functioning conditions, e.g. by ranking and selecting individuals, such as models used for credit scoring, insurance or recruitment. Since such models inherently need to reject some candidates, or assign a low score to them, their

136 H. Zech, 'Liability for AI: public policy considerations', *ERA Forum*, Vol. 22, 2021, p. 147, p. 150 et seqq.; G. Wagner, 'Robot Liability', in S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019, p. 25, p. 31 et seqq.; G. Wagner, 'Einleitung zum Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz – ProdHaftG)', *Münchner Kommentar BGB*, 9th edition, Verlag C.H. Beck, 2021, paras. 18-23.

137 M. Reimann, 'Product liability', *Comparative Tort Law, Edward Elgar Publishing*, 2021, *p.* 238; A.-C. Mayrhofer, 'Product liability in the age of AI – Proposal for a "two track" solution', *Revista Electrónica de Direito*, Vol. 33, 2024, p. 106, p. 110; for manufacturing defects, strict liability indeed exists to some extent: it imposes liability for outliers which cannot be prevented with a very high duty of care, see G. Wagner, 'Produkthaftung für autonome Systeme', *Archiv für die civilistische Praxis*, Vol. 217(6), 2017, p. 707, p. 712; G. Wagner, 'Einleitung zum Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz – ProdHaftG)', *Münchner Kommentar BGB*, 9th edition, Verlag C.H. Beck, 2021, para. 22.

138 Cf. BGH Case VI ZR 107/08, Airbag, BGHZ 181, 253 para. 15.

139 A.-C. Mayrhofer, 'Product liability in the age of AI – Proposal for a "two track" solution', *Revista Electrónica de Direito*, Vol. 33, 2024, p. 115.

140 M. A. Geistfeld, 'A roadmap for autonomous vehicles: State tort liability, automobile insurance, and federal safety regulation', *California Law Review*, Vol. 105, 2017, p. 1611, p.1619; M. C. Buiten, 'Product liability for defective AI', *European Journal of Law and Economics*, 2024, p. 19.

141 G. Wagner, 'Vorbemerkung (Vor § 823)', *Münchner Kommentar BGB*, 9th edition, Verlag C.H. Beck, 2021, para. 18.

142 See e.g. regulations like §§ 32 ff. German GenTG (genetically modified organisms) and §§ 1 ff. German UmweltHG (particularly dangerous establishments concerning damage to the environment).

143 P. Hacker, 'The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 31.

decisions can negatively impact individuals. Generally speaking, a significant proportion of outputs (e.g. more than 20%) in these models could lead to unavoidable damage, even under optimal operation conditions.[144] This damage, however, is not necessarily a harm that needs to be compensated for; rather, it merely reflects the fact that a person was not chosen, or awarded a higher score, based on the available data.

4.1.2. Strict liability in the European Parliament resolution of 2020 on AI liability

In the European Parliament resolution of 2020 on AI liability, the concept of truly strict liability was envisaged for high-risk AI systems, combined with significant financial caps for damages per incident. Specifically, it suggests a cap of 2 million euros for personal injury and 1 million euros for property damage (Article 5 European Parliament resolution of 2020 on AI liability). The resolution also calls for a mandatory insurance requirement for these high-risk AI systems (Article 4(4) European Parliament resolution of 2020 on AI liability).

For non-high-risk AI systems, the resolution outlines a fault-based liability system, based on a presumption of negligence. However, there is an opportunity for exculpation in cases where 'algorithmic due diligence' can be demonstrated. The caps for damages and the statute of limitations in these cases would defer to the laws of the individual Member States. This two-tiered approach recognises the varying levels of risk associated with different AI systems and attempts to balance the need for accountability with the desire for innovation and AI development.

Concerning liable entities, the resolution focused on 'operators', distinguishing between front-end and back-end operators. The former denotes natural or legal persons exercising a degree of control over a risk connected with the operation and functioning of the AI-system and benefitting from its operation; the latter refers to an entity who, on a continuous basis, defines the features of the technology and provides data and an essential backend support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI-system. To avoid confusion among regulated entities, and enhance coherence**, it is recommended that the terminology of the PLD and/or the AI Act be used in the AILD henceforth (i.e. economic operator/manufacturer or provider/deployer).**

4.1.3. Strict liability in the AILD: Present and future

Truly strict liability, as advocated by the European Parliament resolution of 2020 on AI liability, was not taken up in the liability proposals – neither in the PLD nor in the AILD. This begs the question if truly strict liability should be included in future versions of the AILD (or even future updates of the PLD).

The benefits of truly strict liability

Four key arguments can be advanced in favour of truly strict liability.[145]

---

144 P. Hacker, 'The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 31; see also, taking this up, A.-C. Mayrhofer, 'Product liability in the age of AI – Proposal for a "two track" solution', *Revista Electrónica de Direito*, Vol. 33, February 2024, p. 119 (focusing on products with high risk and low societal value); and references in footnote 2; cf. also C. Wendehorst, 'Strict liability for AI and other emerging technologies', *Journal of European Tort Law*, Vol. 11, 2020, p. 167.

145 See e.g. M. C. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, pp. 3-4 and pp. 8-9; M. C. Buiten, 'Product liability for defective AI', *European Journal of Law and Economics*, 2024, pp. 8-10; C. Wendehorst, 'Strict liability for AI and other emerging technologies', *Journal of European Tort Law*, Vol. 11, 2020, p. 179; H. Zech, 'Liability for AI: public policy considerations', *ERA Forum*, Vol. 22, 2021, p. 147, p. 155; A.-C. Mayrhofer, 'Product liability in the age of AI – Proposal for a "two track" solution',

a. **Regulation of activity levels**. Unlike negligence-based systems, truly strict liability can regulate not only the level of care but also the activity level of the liable parties, as standard economic analysis shows.[146] If operators know that they will have to pay for any harm, they will not engage in the activity, e.g. by selling AI products, more often than economically necessary (to avoid risking more damages). This is crucial for high-risk AI systems where the optimal activity level—such as the number of AI products deployed—should be influenced by potential liability. Even the socially optimal duty of care does not necessarily lead to an optimal level of damage under negligence law as the opacity and autonomy of AI systems make it extremely difficult for AI developers and deployers to estimate the severity and probability of harm. Hence, controlling the activity level through strict liability ensures that the societal costs of these activities are accounted for effectively. However, it should be noted that the optimal effects of those incentives via the liability system hinge on many assumptions (adequate information, attention, rationality of parties)[147] that are at least doubtful in practice, as opposed to economic theory.

b. **Simplification of legal processes**. Truly strict liability eliminates the need for costly and complex investigations into whether a duty of care was breached or a product was defective.[148] This is particularly advantageous in the AI context, where technological intricacies can make judicial assessments challenging and error-prone.[149] This may reduce overall administration cost and helps injured parties claim compensation, particularly in cases with relevance to fundamental rights (non-discrimination, personality rights; other fundamental rights). Additionally, strict liability doesn't rely on the slow evolution of technical standards operationalising the duty of care.[150] Rather, strict liability systems 'automatically' adapt to technological advancements.

c. **Internalisation of costs**. Following the principle that the beneficiaries of a risky activity should also bear its costs, strict liability ensures that the parties profiting from AI technologies are responsible for compensating any harm these technologies cause.[151] This full internalisation of external costs aligns with principles of economic and distributive justice (*qui habet commoda ferre debet onera*).[152]

d. **Effective enforcement**. In the EU context more specifically, non-discrimination law already contains a system of strict liability, but insufficient enforcement tools, as seen (2.5.1). These deficiencies could be remedied by including truly strict liability in the AILD, in combination with the alleviations for proving fault and causation.

Revista Electrónica de Direito, Vol. 33, February 2024, pp. 117-119; cf. also G. Wagner, 'Robot Liability', in S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019, p. 47; see also M. Ziosi and others, 'The EU AI Liability Directive (AILD): Bridging Information Gaps', *European Journal of Law and Technology*, Vol. 14(3), 2023, p. 8; but see also Y. Bathaee, 'The artificial intelligence black box and the failure of intent and causation', *Harvard Journal of Law & Technology*, Vol. 31, 2018, p. 889, p. 932 et seqq.; for a compensation fund, see e.g. N. E. Vellinga, 'Rethinking compensation in light of the development of AI', *International Review of Law, Computers & Technology*, Vol. 38(1), 2024, p. 4 et seqq.

146 S. Shavell, Foundations of Economic Analysis of Law, *Harvard University Press*, 2004, p. 196.

147 See again S. Shavell, 'Strict Liability versus Negligence', *The Journal of Legal Studies*, Vol. 9, 1980.

148 ibid, p. 188 et seqq.; S. Wachter, 'Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond', *Yale Journal of Law and Technology,* Vol. 26(3), 2024, p. 671, p. 717.

149 Cf. also E. Karner, B. Koch and M. A. Geistfeld, Comparative Law Study on Civil Liability for Artificial Intelligence, 2021, pp. 46-47.

150 G. Spindler, 'User liability and strict liability in the Internet of Things and for robots', in S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019.

151 M. C. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, p. 9.

152 R. Zimmermann, The Law of Obligations: Roman Foundations of the Civilian Tradition, *Juta and Company Ltd*, 1990, p. 201 and p. 209.

In scenarios involving illegitimate-harm high-risk models, strict liability could be justified, based on these observations, as the system exhibits significant risks and, when functioning correctly, should not cause harm.[153] This includes use cases like autonomous driving or medical diagnostics AI, where a cap on liability might be necessary to maintain insurability.[154] For legitimate-harm models, however, operators should have the opportunity to demonstrate that the system operated as intended and that any harm caused was justified, thus potentially exculpating them from liability.

The downsides of truly strict liability

Conversely, the argument against truly strict liability posits that it may act as a barrier to innovation but could also negatively impact fundamental rights.

a. **Industry policy and innovation**: first, fault-based liability, e.g. negligence, can effectively act as a liability shield, 'subsidising' innovation in and deployment of AI in the EU: if the provider or deployer fulfil their duties of care, they are absolved from liability, irrespective of any harms ensuing. This is particularly relevant for SMEs, as many EU AI companies are. SMEs are more vulnerable to the deterrent effects of potential litigation. Start-ups, in particular, are typically backed by venture capitalists who may withdraw or abstain from further funding if the company is faced with lawsuits. Already, obtaining funding for an AI is more difficult in the EU than in the US; yet, these particular deterrence effects on SMEs can be mediated by excluding truly strict liability for SMEs, as argued elsewhere.[155]

The overarching concern is that a strict liability regime could be perceived globally as a strong stance against AI investment and deployment in the EU,[156] potentially leading to a 'chilling effect'[157] and reduced AI offerings in critical sectors like healthcare and education. There is a significant risk of a compounding negative effect on innovation with the AI Act, which is, arguably, not particularly strict *de iure* but has a strong reputation for being an obstacle to innovation and investment in the venture capital arena.

b. **Ambivalent effects on fundamental rights**: importantly, even from a fundamental rights perspective, the effects of truly strict liability are complex. We should distinguish between direct and indirect effects on fundamental rights.

Direct effects: truly strict liability leads to easier compensation, bolstering the effective safeguarding of fundamental rights to the extent that liability is connected to fundamental rights risks or violations.

Indirect effects: however, truly strict liability for AI would be quite unique, globally. As mentioned, it could be perceived as a significant move against AI investment, development, and deployment in the EU. This, in turn, may have negative consequences for fundamental rights. First, to the extent that this leads to less AI products offered in the EU in areas in which they can be societally beneficial, consumers and citizens could be deprived of novel ways of safe driving (future autonomous

---

153 See references in note 144.

154 G. Spindler, 'User liability and strict liability in the Internet of Things and for robots', in S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019, p. 137; A. Bertolini, Artificial intelligence and civil liability, external study prepared for the European Parliament's Committee on Legal Affairs (JURI), 2020, p. 41, p. 93.

155 P. Hacker, 'The European AI Liability Directives - Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, p. 33.

156 See e.g. H. Zech, 'Liability for AI: public policy considerations', *ERA Forum*, Vol. 22, 2021, p. 147, p. 153; Mayrhofer, 'Product liability in the age of AI – Proposal for a "two track" solution', p. 119.

157 K. A. Chagal-Feferkorn, 'Am I an algorithm or a product: when products liability should apply to algorithmic decision-makers', *Stanford Law & Policy Review*, Vol. 30, 2019, p. 61, p. 82; for empirical data, suggesting chilling effects only under some conditions (only on downstream innovation, not on innovation concerning the product itself), see A. Galasso and H. Luo, 'When does product liability risk chill innovation? Evidence from medical implants', *American Economic Journal: Economic Policy*, Vol. 14, 2022, p. 366.

vehicles), learning (in education), developing medication (drug discovery), or of new treatment methods (healthcare).[158] In some areas, and in the light of a growing shortage of skilled labour, one might even say that not facilitating the use of responsible AI may amount to fundamental rights risk, too.

Of course, not every AI product is socially desirable, particularly not in such high-impact sectors as the ones mentioned. However, the AI Act is precisely designed to channel AI development and deployment into socially beneficial products in these areas, and to severely sanction any models falling behind its standards. A reduction in offerings of those models could inadvertently impact the effective enjoyment of fundamental rights associated with these sectors.

Second, higher expected legal costs may lead to higher prices for AI products, even if they are not withheld entirely from the EU market. This may hinder market penetration of AI products that are actually safer than current human practices.[159] Both effects, the partial reduction in the offer of beneficial AI and higher costs, may be considered detrimental to the effective enjoyment of certain fundamental rights, such as rights to education, health, or research, to name just a few.

This shows that the fundamental rights aspects of liability are deeply intertwined with industrial policy choices which, in turn, have repercussions on the effective enjoyment of fundamental rights in our societies.

c. **Vexatious litigation**: another risk associated with the adoption of truly strict liability is the potential increase in vexatious litigation,[160] especially in domains where harm is immaterial, such as cases involving discrimination and violations of personality rights. These areas are particularly susceptible because the harm is often less tangible and immediate, making it more challenging to verify and quantify.

Under the current framework of the PLD, which predominantly deals with material harm – specifically to health and property – claims are, arguably, less likely to be frivolous or unfounded because material damage can typically be observed and verified directly and objectively. However, the shift towards a truly strict liability model, especially without careful and precise legal safeguards, could inadvertently encourage meritless claims in areas where harm is less concrete and more subjective.

In cases of immaterial harm, the difficulty in substantiating the occurrence and extent of harm can lead to disputes being more open to interpretation, potentially giving rise to litigation that is pursued not for reasons of harm suffered but rather for opportunistic or strategic purposes. This could impose an undue burden on the legal system and on the parties involved (e.g. SMEs), particularly on AI developers and deployers who may find themselves facing a significant number of claims. Again, such a risk may also have a negative effect on innovation and the deployment of AI technologies due to the increased risk and potential costs associated with defending against such claims.

---

158 See also H. Dawid and G. Muehlheusser, 'Smart products: Liability, investments in product safety, and the timing of market introduction', *Journal of Economic Dynamics and Control*, Vol. 134, 2022, Article 104288; M. C. Buiten, 'Product liability for defective AI', *European Journal of Law and Economics*, 2024, p. 10; M. C. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, p. 9.

159 H. Dawid and G. Muehlheusser, 'Smart products: Liability, investments in product safety, and the timing of market introduction', *Journal of Economic Dynamics and Control*, Vol. 134, 2022, Article 104288; M. C. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, p. 9.

160 B. Schütte, L. Majewski and K. Havu, 'Damages liability for harm caused by Artificial Intelligence–EU law in flux', *Helsinki Legal Studies Research Paper*, 2021, p. 26; J. De Bruyne, O. Dheu and C. Ducuing, 'The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive', *Computer Law & Security Review*, Vol. 51, Article 105894, 2023, p. 7.

To mitigate this risk, any introduction of truly strict liability for immaterial harm would need to be accompanied by robust mechanisms that ensure only legitimate claims are brought forward to prevent the misuse of the legal system for vexatious purposes.

Recommendation

While truly strict liability could simplify compensation processes and regulate activity levels, it must be balanced against its potential to reduce AI innovation and deployment, particularly among SMEs.[161] Positive and negative repercussions on fundamental rights and the EU's position as a competitive hub for AI development must also be considered. Any decision to establish truly strict liability would need to account for its multi-dimensional impacts, making it ultimately a political choice that must be carefully weighed.

4.2. Joint liability

The European Parliament's suggestion (in its resolution of 2020 on AI liability) for a system of joint liability could be strategically incorporated into the AILD to facilitate operators in seeking redress from various entities within the AI value chain.

4.2.1. Current situation analysis

Under the current framework, redress in cases of joint liability is primarily governed by national law.[162] The PLD also stipulates that multiple economic operators can be held jointly and severally liable for the same damage (Article 12(1) PLD). However, it also allows for certain exceptions, particularly to encourage innovation among microenterprises and small enterprises in the software sector (Article 12(2) PLD). These entities can contractually agree with manufacturers to waive the right of recourse in cases of defective software components, thus shifting the liability to the manufacturers who integrate these components into their products. This arrangement is meant to support the innovative capacity of smaller software enterprises without diminishing the overall liability towards the injured party. However, it remains unclear if manufacturers (particularly large developers with market power) would actually agree to such provisions.

The main conundrum at the heart of joint liability is the allocation of liability along the AI value chain.[163] Article 25 AI Act, which was included only at a later stage in the AI Act, defines certain situations in which a deployer becomes the new provider, assuming primary responsibility for AI Act compliance. A similar provision is missing both from the revised PLD and the AILD. The core problem for liability along the value chain can, arguably, be stated as follows: to safeguard effective compensation, the last actor in the chain – the one facing the injured party, often a deployer (the downstream actor) – should be held liable if the liability conditions of national law are met. That entity or person is often the easiest point of contact for the injured person. However, other entities upstream along the chain should also be liable, under certain conditions defined primarily by national law: first, because the last actor might be insolvent; and second, because the actual fault might lie with other entities in the value chain.

---

161 M. C. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, p. 9.

162 See Article 20 Rom-II-Regulation; for a general overview of different legal systems cf., W.V.H. Rogers (Ed.), *Unification of Tort Law: Multiple Tortfeasors*, Kluwer Law International, 2004; for the relevant law in, e.g. Ireland see s 11-33 of the Civil Liability Act 1961.

163 See e.g. S. Li, M. Faure and K. Havu, 'Liability rules for AI-related harm: law and economics lessons for a European approach', *European Journal of Risk Regulation*, Vol. 13, 2022, p. 618; M. C. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, p. 4.

Typically, if the injured party seeks redress from the last actor, that entity can turn around and seek recourse from those other upstream actors who were jointly and severally liable, and/or who delivered a defective or non-conforming product. This was foreseen in Articles 11 and 12 of the European Parliament resolution of 2020 on AI liability. However, particularly when it comes to AI and certain software applications, those upstream markets can be dominated by a few select players, like the market for foundation models/general-purpose AI systems.[164] Hence, a certain risk exists that upstream actors might (ab)use their dominant market position to impose contractual liability waivers on downstream actors, preventing the latter from seeking recourse.[165]

Notably, the European Parliament, in paragraph 22 of the resolution of 2020 on AI liability, requested the European Commission to 'evaluate the need for legal provisions at Union level on contracts to prevent contractual non-liability clauses, including in Business-to-Business and Business-to-Administration relationships'.

4.2.2. Recommendation

The fair sharing of the liability burden along the AI value chain has gained additional urgency with the arrival of general-purpose AI systems that are, typically, fine-tuned and otherwise modified post-training by various actors.

Another challenge in AILD redress cases lies in transnational cases, which are currently addressed through a complex mesh of national laws and international private law, often leading to legal complications. To streamline this process, the AILD should incorporate an explicit framework for redress that allows for (partial) recovery based on several key principles. Different policy options exist to deal with these scenarios:

Option 1: Presumption of equal share

1. **Presumption of equal share**. Initiate with the presumption that each liable entity in the AI value chain contributing to the damage bears an identical share of the liability.
2. **Burden of proof on actors seeking adjustment**. Only when an entity seeks to challenge this presumption and argues for a higher or lower degree of contribution should litigation over the exact contribution of each actor be initiated. The entity challenging the presumption should carry the burden of proof.
3. **Binding character**. These provisions should be binding and not subject to modification by contractual agreement.

This recommendation could simplify the recovery process by default while providing an avenue for adjustment where necessary. By implementing this framework in the AILD, it would create a more transparent and predictable system of redress within the EU, reduce reliance on varied national and international laws, and foster a more cohesive legal environment for AI liability. The binding character is necessary to prevent contractual practices, particularly in settings of imperfect competition, from undermining the presumptions and protection provided by the provisions.

[164] See e.g. J. Vipra and A. Korinek, 'Market concentration implications of foundation models: The Invisible Hand of ChatGPT', Working Paper, 79th Economic Policy Panel Meeting, 2023; cf. also D. Rubinfeld and M. Gal, 'Access barriers to big data', *Arizona Law Review*, Vol. 59, 2017, pp. 339-381; L. Bertuzzi, 'Are EU regulators ready for concentration in the AI market?', EURACTIV, 3 November 2023.

[165] Cf. C. S. Hutchinson, 'Potential abuses of dominance by big tech through their use of Big Data and AI', *Journal of Antitrust Enforcement*, Vol. 10, 2022, pp. 443-468.

Option 2: Support of SMEs

1. **Support of SMEs**. The exemptions in favour of SMEs contained in Article 12(2) PLD should be copied into the AILD redress system.
2. **Binding character**. These provisions should be binding and not subject to modification by contractual agreement.

This option would also provide specific protection for SMEs deemed vulnerable in contractual settings, like in the PLD. However, the protection hinges on the highly uncertain premise that the manufacturer would actually contractually agree to the SME protection. A variety of this clause would, therefore, make protections for SMEs (but not full liability exemptions to avoid moral hazard) binding (cf. Option 3). The reasons for the binding character are the same as under Option 1.

Option 3: Protection of downstream parties

1. **Prohibition of recourse waivers**. Enact a prohibition on contractual clauses that waive or significantly and negatively modify the right of recourse for downstream actors in the AI value chain. This means any agreement attempting to limit or eliminate the downstream party's ability to seek redress from upstream actors shall be considered null and void.
2. **Binding character**. These provisions should, quite logically, be binding and not subject to modification by contractual agreement.

This policy option aims to address the issue of imperfect competition in upstream markets, where dominant players might impose unfair contractual terms on downstream actors. By outlawing such waivers or modifications, the policy ensures that downstream actors retain their right to seek compensation from those may actually be at fault. This policy may contribute to maintaining fairness in the liability chain and safeguarding effective compensation for injured parties.

Importantly, such provisions would not be a novelty in EU Digital law. Rather, Article 13(5)(a) Data Act contains precisely one such clause which protects parties from inappropriate liability limitations or extensions. The European Commission could even be tasked, as foreseen also Article 41 Data Act, to develop model contractual terms and standard contractual clauses for the allocation of AI liability along the value chain.

All of these options, which may also be combined, would seek to ensure that downstream actors, often the easiest point of contact for injured parties, are not left without recourse due to the market power of upstream actors. While the PLD only implements Option 2, there is room in the AILD to potentially include other options – or all of the above. This is because it is sufficient for those actors seeking recourse to have one valid claim at their disposal (in the AILD framework), even if the PLD does not provide a valid recourse option in a specific scenario. Hence, the AILD may effectively compensate another gap in the PLD – the value chain problem. Option 3 arguably comes closest to the suggestion in paragraph 22 of the original European Parliament resolution of 2020 on AI liability. Option 1, in turn, potentially reduces transactional and litigation costs by introducing a presumption of equal quota.

4.3. Fault-based liability and proof alleviations

Irrespective of whether, ultimately, a system of truly strict liability is integrated into the AILD (or an SLI), some fault-based systems will certainly remain in Member States that have to be dealt with,

too. In this context, the question arises whether the tools foreseen in the current AILD proposal are suitable for balancing effective compensation with the quest for innovation and AI deployment.[166]

4.3.1. Disclosure of evidence

Disclosure of evidence and access to information are critical issues in both the old PLD and AILD, with the burden of proof for key liability triggers, such as fault and defectiveness, resting generally on the claimant without much alleviation (i.e. barring the PLD revision and the AILD). In typical product liability cases, and even more so with AI systems due to their technical complexity, opacity, and autonomy, a stark information asymmetry exists between the manufacturer and the injured party. To address this, both directives include mechanisms for evidence disclosure.

The AILD contains Article 3, which obliges potential defendants to disclose evidence. This provision allows courts to order a disclosure procedure that enables potential claimants to determine the viability of their case and potential defendants. Despite its similarities to US pretrial discovery, it is notably distinct and applies even to strict liability claims, though it is limited to high-risk AI systems. The court order of disclosure is contingent on the claimant providing plausible evidence of damages and the defendant's refusal to grant access to necessary information. Disclosure must be proportional, considering the legitimate interests of all parties, and can extend to third parties under the same conditions. Non-compliance with a court-ordered disclosure leads to a rebuttable presumption of non-compliance with the relevant duty of care.

Advantages

The disclosure process is vital for effective enforcement, enabling claimants to make informed decisions on litigation and thereby enhancing compliance with the AI Act. It also serves as an early filter, deterring baseless lawsuits and reducing social costs. Furthermore, the information requested broadly aligns with the AI Act's existing transparency obligations. This implies a reduced additional burden for high-risk AI providers.

Shortcomings and recommendations

In this context, however, the directive's alignment with the AI Act could be its downfall, as the evidence disclosure is aimed at non-experts like consumers or their legal counsel, distinct from the expert audience of the AI Act. Information needs, to the extent possible, to be understandable to laypersons to be useful in litigation. The final version of the PLD revision now contains language for the court 'to require the evidence to be presented in an easily accessible and easily understandable manner, if such presentation is deemed proportionate by the national court in terms of costs and effort for the required party.'[167] The same provisions should be integrated into the AILD.

Another issue is the requirement for potential claimants to provide enough evidence to support the plausibility of their claim, a threshold that often deters legitimate claims,[168] as seen in discrimination law. The directive should lower this barrier, allowing the evidence disclosure mechanism to be triggered by the mere demonstration of damage and the involvement of an AI system, as well as, potentially, the showing that it is not implausible for the AI to have caused the damage. The plausibility requirement should, however, be maintained for cases brought by potential or actual competitors to prevent vexatious litigation and to protect trade secrets.

---

166 See also P. Hacker, 'The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, Article 105871, 2023, pp. 17-20.

167 See Resolution of 12 March 2024 on the proposal for a directive of the European Parliament and of the Council on liability for defective products, European Parliament.

168 Cf. F. G'sell, 'An Overview of the European Union Framework Governing Generative AI Models and Systems', Working Paper, 2024, p. 94.

4.3.2. Burden of proof

The AILD and PLD proposals aim to ease the claimants' burden of proof, a critical aspect when dealing with complex AI systems. In a typical scenario, proving fault or defectiveness falls heavily on the claimant.

Critique of the current AILD proposal

The AILD proposal tackles this by introducing a rebuttable presumption specifically for the causal link between a breach of duty of care and the output of the AI system. However, this presumption does not address the actual establishment of fault, the AI system's output, the extent of the damage, or the direct causal link between the output and damage. It is activated only after the claimant demonstrates all the latter elements.

To apply the causality presumption, the claimant must prove the fault, show it is reasonably likely that the fault influenced the output, and demonstrate that the output caused the damage. These conditions could require expert input; this may add complexity and potentially cost to the claimant's case.

Despite these steps forward, challenges persist. For instance, the AILD doesn't capture obligations post-AI output creation, such as required actions under Articles 14 and 26(2) and (5) AI Act (human oversight, see Section 3.3).

In addition, the AILD restricts the causality presumption in certain situations, like when the defendant proves that evidence and expertise are accessible for the claimant to demonstrate the causal link, possibly again necessitating costly AI experts.

Importantly, the AILD also extends the causality presumption to consumers in certain cases. This raises questions about the application in everyday use versus situations where a consumer knowingly operates the AI system under inappropriate conditions.

Furthermore, while the AILD does offer an evidence disclosure system, it does not provide a comprehensive rebuttable presumption for establishing fault. Claimants might still face significant challenges in showing fault in the AI's training, possibly requiring expert analysis—a costly and daunting prospect.[169] On the other hand, a full rebuttable presumption, or even reversal of the burden of proof, for fault would be quite a significant intervention.

Recommendations

Article 4 AILD should be amended to include a presumption of causality between fault and damage for cases of a violation of the AI Act occurring during the post-processing stage by either the provider or deployer. Furthermore, a clarifying statement should be incorporated into the recitals concerning Article 4 AILD, stipulating that a mere acknowledgment of the inherent fallibility of machine learning models – including those that are nearly flawless – should not automatically serve as a valid defence. This clarification would assert that the potential for a machine learning model to make an error, which might lead to damage, cannot be a default argument to refute the presumption of causality.

[169] J. De Bruyne, O. Dheu and C. Ducuing, 'The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive', *Computer Law & Security Review*, Vol. 51, Article 105894, 2023, p. 5; A. Bertolini, Artificial intelligence and civil liability, external study prepared for the European Parliament's Committee on Legal Affairs (JURI), 2020, p. 84.

5. From a directive to a regulation on AI liability

Beyond the intricacies of the AILD's individual stipulations, the question finally arises of whether the choice of a directive, rather than a regulation, is suitable to achieve the goals of AI regulation and liability.

5.1. Choosing the instrument: Directive or regulation?

5.1.1. Lessons from market regulation and product safety law

While a more comprehensive harmonisation of AI liability may break with some Member State traditions in tort law,[170] these disadvantages would likely be outweighed. Choosing the instrument of a regulation, not a directive, for the AI liability framework could be a prudent decision for several reasons. The experience with the Data Protection Directive highlighted the risks associated with directives, even fully harmonising ones: notably the emergence of a fragmented legal landscape as a result of diverging national transpositions. This fragmentation was a key factor in the decision to adopt the GDPR, which aims for a unified regulatory approach across the EU;[171] it is highlighted by scholars as a considerable risk for the AILD, as well.[172]

Adopting a comprehensive *regulation* for AI liability would similarly benefit the AI industry and citizens by providing a consistent and coherent legal framework. The varied transpositions of directives into national laws have previously led to discrepancies across Member States, complicating the legal environment for both AI developers and consumers. For consumers, in particular, this legal diversity can make it challenging to understand applicable legal protections and pursue remedies against providers in different jurisdictions.

Enacting a regulation instead of a directive would also fit with the general trend in important and adjacent parts of EU law. In addition to capital markets law, where, inter alia, the Market Abuse Regulation and the Prospectus Regulation have replaced directives, there are other areas in EU market law where directives have been superseded by regulations to prevent fragmentation – particularly in the product safety space, which is intimately linked to product liability. A notable example is in the medical device sector, where the Medical Device Regulation

---

170 See the discussions in J. De Bruyne, O. Dheu and C. Ducuing, 'The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive', *Computer Law & Security Review*, Vol. 51, Article 105894, 2023, pp. 3-4; B. Schütte, L. Majewski and K. Havu, 'Damages liability for harm caused by Artificial Intelligence – EU law in flux', *Helsinki Legal Studies Research Paper*, 2021, pp. 25-26.

171 B. Van Alsenoy, 'Liability under EU data protection law: from Directive 95/46 to the General Data Protection Regulation', *Journal of Intellectual Property, Information, Technology and E-Commerce Law*, Vol. 7(3), 2016, p. 271, para. 2.

172 F. G'sell, 'An Overview of the European Union Framework Governing Generative AI Models and Systems', Working Paper, 2024, p. 94: 'However, this limited harmonization could result in a significant divergence in legal decisions, considering that the concept of fault (negligence) is not uniformly defined and interpreted under member states' national laws.'; I. Bratu, 'A first critical analysis of the European approach to damage caused by artificial intelligence enabled by global navigation satellite systems. A bridge to nowhere or a cloud with a silver lining?', *International Review of Law, Computers & Technology*, Vol. 37, 2023, p. 147, p. 156: 'the definition [for standards of care] is too broad, and it does not contain sufficient elements that would fulfil the purpose of a harmonization process. Moreover, the role of national law remains predominant, which may lead to fragmentation and different court interpretations.'; M. C. Buiten, A. De Streel and M. Peitz, 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, Article 105794, 2023, pp. 18-19: 'It remains to be seen [...] what level of uniformity for liability throughout the EU can really be achieved [through the AILD]. [...] a strict liability regime may be more predictable. It would likely lead to fewer interpretation variations across national courts in the Member States.'; M. Ziosi and others, 'The EU AI Liability Directive (AILD): Bridging Information Gaps', *European Journal of Law and Technology*, Vol. 14(3), 2023, p. 4.

(EU) 2017/745 replaced several directives concerning medical devices, including Directive 93/42/EEC.

The transition from directives to regulations can be further observed with the introduction of the General Product Safety Regulation (GPSR), set to replace the current General Product Safety Directive and the Food Imitating Product Directive from 13 December 2024. In the same vein, the European Machinery Regulation (EU) 2023/1230 is set to substitute the Machinery Directive 2006/42/EC. This significant change of legal instruments aims to modernise the EU's product safety framework and tackle new challenges brought about by the digitalisation of economies.

The move towards a regulation format in capital markets and product safety law thus, arguably, reflects an overarching EU strategy to avoid fragmentation and ensure uniform application of safety standards across all Member States. As the European Commission rightly pointed out in the IA accompanying the GPSR: 'The current legal form, a **Directive, creates several problems linked especially to the implementation and national differences** regarding the date and/or manner of transposition.'[173]

The same analysis, however, holds concerning AI liability, as scholars have noted,[174] and should have been included in the IAs accompanying the PLD revision and the AILD. It is particularly noteworthy that the areas most closely linked to product liability – product safety and market regulation – are now transitioning to the use of regulations instead of directives. This rightly highlights the EU's commitment to creating a more coherent and effective legal framework that can adapt to the rapid advancements and complexities of the digital age.

5.1.2. Recommendation

Given the significance of AI as a driver of innovation and its implications for the digital single market, a uniform approach is essential. It would benefit both industry and consumers by providing clarity, preventing fragmentation, and offering one regime for cross-border cases.[175] Moving away from the traditional reliance on Member States' competences in liability regimes, especially in the non-contractual sphere, acknowledges the need for an EU-wide framework that reflects the digital single market's integrated nature. It reflects an understanding that, especially in highly integrated and rapidly evolving areas such as AI and digital technologies, consistent and direct application of law is essential for fostering innovation and consumer trust.

Leveraging Article 114 TFEU to establish a comprehensive, EU-wide regulation for AI liability and software would ensure such a harmonised approach. **These findings would thus call for a revised Product Liability Regulation and an AI liability regulation (or rather: a software liability regulation, see Section 3.5.5) instead of the respective directives.**

5.2. Concrete steps towards a regulation

Changing the legal instrument from a proposed directive to a regulation would involve several steps, including:

- legal assessment: an assessment to ensure the proposed changes align with the EU Treaties and principles, particularly considering the legal basis (Article 114 TFEU);

[173] European Commission, Impact Assessment Accompanying the document 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, SWD(2021) 168 final, 2021.

[174] See the references in note 172.

[175] See also C. Wendehorst, AI liability in Europe: anticipating the EU AI Liability Directive, Ada Lovelace Institute, 2022, p. 8; L. Bertuzzi, 'The new liability rules for AI', EURACTIV, The Tech Brief (podcast), accessed 30 March 2024.

- stakeholder consultation: engaging with EU Member States, industry stakeholders, academia, and civil society to gather feedback and build consensus. This could, however, build on previous stakeholder consultations concerning AI liability;
- impact assessment: thoroughly evaluating the potential effects of a regulation versus a directive on the internal market, Member States' legal systems, and innovation. This impact assessment could draw heavily on the existing IAs concerning AI liability, with the necessary updates to meet the constantly changing nature of AI;
- proposal revision: amending the legal text to reflect the change from a directive to a regulation;
- legislative procedure: the revised proposal must undergo the ordinary legislative procedure, involving negotiation and approval by both the European Parliament and the Council of the European Union.
- implementation measures: developing detailed implementation guidelines and support measures for Member States to ensure a smooth transition to the new legal framework.

REFERENCES

ACM Tech. Policy Committee, ACM TechBrief: Computing and Climate Change, 2021.

Bathaee Y., 'The artificial intelligence black box and the failure of intent and causation', *Harvard Journal of Law & Technology*, Vol. 31, 2018, pp. 889-938.

Behavia, CEPS, Kantar, Behavioural study on the link between challenges of artificial intelligence for Member States' civil liability rules and consumer attitudes towards AI-enabled products and services, 2021.

Bertolini A., Artificial Intelligence and Civil Liability, European Parliament, 2020.

Bertuzzi L., 'Are EU regulators ready for concentration in the AI market?', EURACTIV, 3 November 2023.

Bertuzzi L., 'The new liability rules for AI', The Tech Brief (podcast), EURACTIV, 30 September 2022.

Bertuzzi L., 'Updated AI liability proposal sent to EU legislators, with some significant changes', MLex, 26 July 2024.

Bommasani R. and others, 'On the opportunities and risks of foundation models', arXiv preprint, 2021.

Bratu I., 'A first critical analysis of the European approach to damage caused by artificial intelligence enabled by global navigation satellite systems. A bridge to nowhere or a cloud with a silver lining?', *International Review of Law, Computers & Technology*, Vol. 37, 2023, pp. 147-165.

Brookshear J. G. and Brylow D., *Computer Science: An Overview*, 13th edition, Pearson, 2020.

Bubeck S. and others, 'Sparks of artificial general intelligence: Early experiments with GPT-4', arXiv preprint, 2023.

Buiten M., De Streel A. and Peitz M., 'The law and economics of AI liability', *Computer Law & Security Review*, Vol. 48, 2023, Article 105794.

Buiten M., 'Product liability for defective AI', *European Journal of Law and Economics*, 2024, Vol. 1, pp. 239-273.

Čerka P., Grigienė J. and Sirbikytė G., 'Liability for damages caused by artificial intelligence', *Computer Law & Security Review*, Vol. 31, 2015, pp. 376-389.

Chagal-Feferkorn K.A., 'Am I an algorithm or a product: when products liability should apply to algorithmic decision-makers', *Stanford Law & Policy Review*, Vol. 30, 2019, pp. 61-114.

Dawid H. and Muehlheusser G., 'Smart products: Liability, investments in product safety, and the timing of market introduction', *Journal of Economic Dynamics and Control*, Vol. 134, 2022, Article 104288.

De Bruyne J., Dheu O. and Ducuing C., 'The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive', *Computer Law & Security Review*, Vol. 51, 2023, Article 105894.

de la Durantaye K., Garbage In, Garbage Out. Regulating Generative AI Through Copyright Law, *ZUM*, Vol. 10, 2023, pp. 645-660.

Deloitte, Study to support the Commission's impact assessment on liability for artificial intelligence, European Comission, July 2021.

Doelle M. and Seck S., 'Loss & damage from climate change: from concept to remedy?', in Broberg M. and Romera B. M. (eds), *The Third Pillar of International Climate Change Policy*, Routledge, 2021.

Erdenesanaa D., A.I. Could Soon Need as Much Electricity as an Entire Country, *New York Times*, 10 October 2023.

European Commission, Impact Assessment Accompanying the document 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, SWD(2021) 168 final, 2021.

European Commission, Questions and answers on the revision of the Product Liability Directive, 28 September 2022.

European Commission, Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the

approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), 2018.

Evas T., Civil liability regime for artificial intelligence, European Parliament, September 2020.

Expert Group on Liability and New Technologies – New Technologies Formation, Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies, European Commission, 2019.

Foster D., *Generative Deep Learning*, 2nd edition, O'Reilly, 2023.

Freitag C. and others, 'The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations', *Patterns*, Vol. 2, 2021, Article 100340.

Frizberg D., Adapting liability rules to artificial intelligence, EPRS, European Parliament, March 2024.

Galasso A. and Luo H., 'When does product liability risk chill innovation? Evidence from medical implants', *American Economic Journal: Economic Policy*, Vol. 14, 2022, pp. 366-401.

Gallagher M., Canada's Artificial Intelligence and Data Act (AIDA) 2024: A Comprehensive Guide, Cox & Palmer, 2024.

Ganguli D. and others, 'Predictability and surprise in large generative models', *ACM Conference on Fairness, Accountability, and Transparency*, 2022, pp. 1747-1764.

Geistfeld M. A., 'A roadmap for autonomous vehicles: State tort liability, automobile insurance, and federal safety regulation', *California Law Review*, Vol. 105, 2017, pp. 1611-1694.

Goodfellow I., Bengio Y. and Courville A., *Deep Learning*, MIT Press, 2016.

G'sell F., 'An Overview of the European Union Framework Governing Generative AI Models and Systems', Working Paper, 2024.

Hacker P., *Datenprivatrecht: Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB*, Mohr Siebeck, 2020.

Hacker P., Engel A. and Mauer M., 'Regulating ChatGPT and other Large Generative AI Models', *ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)*, 2023, pp. 1112-1123.

Hacker P., Zuiderveen Borgesius F., Mittelstadt B. and Wachter S., 'Generative Discrimination. What Happens When Generative AI Exhibits Bias, and What Can Be Done About It', in Hacker P., Engel A., Hammer S. and Mittelstadt B., *Oxford Handbook on the Foundations and Regulation of Generative AI*, OUP, forthcoming.

Hacker P., 'Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law', *European Law Journal*, Vol. 29, 2023.

Hacker P., 'Sustainable AI Regulation', *Common Market Law Review*, Vol. 61, 2024, pp. 345-386.

Hacker P., 'Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law', *Common Market Law Review*, Vol. 55, 2018, pp. 1143-1185.

Hacker P., 'The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future', *Computer Law & Security Review*, Vol. 51, 2023, Article 105871.

Haftenberger A., *Die Produkthaftung für künstlich intelligente Medizinprodukte*, Nomos, 2023.

Haim A., Salinas A. and Nyarko J., 'What's in a Name? Auditing Large Language Models for Race and Gender Bias', arXiv preprint arXiv:240214875, February 2024.

Helberger N. and Diakopoulos N., 'ChatGPT and the AI Act' (2023) 12, *Internet Policy Review*, February 2023.

Howells G., Twigg-Flesner C. and Willett C, 'Product liability and digital products', in Synodinou T.-E. and others (eds), *EU Internet Law* (Springer 2017), pp. 183-195.

Hutchinson C. S., 'Potential abuses of dominance by big tech through their use of Big Data and AI', *Journal of Antitrust Enforcement*, Vol. 10, March 2022, pp. 443-468.

Kaminski M. E., 'Regulating the Risks of AI' (2023), *Boston University Law Review*, Vol. 103, August 2022.

Karner E., Koch B. and Geistfeld M. A., 'Comparative Law Study on Civil Liability for Artificial Intelligence', 2021.

Knowles B. and others, 'Our house is on fire: The climate emergency and computing's responsibility', *Communications of the ACM*, Vol. 65, May 2022, pp. 38-40.

Kotek H., Dockum R. and Sun D., 'Gender bias and stereotypes in large language models', Proceedings of the ACM Collective Intelligence Conference, August 2023.

Kysar D.A., 'What climate change can do about tort law', Environmental Law, Vol. 41, 2011.

Laux J., 'Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of AI governance under the European Union AI Act', *AI & SOCIETY*, October 2023.

Li P. and others, 'Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models', arXiv preprint arXiv:230403271, October 2023.

Li S., Faure M. and Havu K., 'Liability rules for AI-related harm: law and economics lessons for a European approach', *European Journal of Risk Regulation*, Vol. 13, December 2022, pp. 618–634.

Luccioni A. S., Jernite Y. and Strubell E., 'Power Hungry Processing: Watts Driving the Cost of AI Deployment?', arXiv preprint arXiv:231116863, June 2024.

Mahdawi A., 'Nonconsensual deepfake porn is an emergency that is ruining lives', *The Guardian*, April 2023.

Mania K., 'Legal protection of revenge and deepfake porn victims in the European Union: Findings from a comparative legal study', *Trauma, Violence, & Abuse*, Vol. 25, December 2022.

Mantrov V., 'Newspaper Advice That Causes Damage Is Not Covered by the Product Liability Directive: The Court of Justice of the European Union's Clarification in Krone', *European Journal of Risk Regulation*, Vol. 14, March 2023, pp. 416–421.

Marchisio E., 'In support of "no-fault" civil liability rules for artificial intelligence', SN Social Sciences, Vol. 1, January 2021.

Marcus G. and Southen R. 'Generative AI Has a Visual Plagiarism Problem', IEEE Spectrum, January 2024.

Marinkovic A. M., 'Liability for AI-related IP infringements in the European Union', *Journal of Intellectual Property Law & Practice*, August 2024.

Mayrhofer A.-K., 'Product liability in the age of AI – Proposal for a "two track" solution', *Revista Electrónica de Direito*, Vol. 33, February 2024.

McGuffie K. and Newhouse A.,'The radicalization risks of GPT-3 and advanced neural language models', arXiv preprint arXiv:200906807, September 2020.

Mishan E. J. and Quah E., *Cost-Benefit Analysis,* Routledge, 6th ed., August 2020.

Nawaz S. A. , 'The Proposed EU AI Liability Rules: Ease or Burden?', European Law Blog, November 2022.

Nilsson N. J., *The Quest for Artificial Intelligence*, Cambridge University Press, October 2009.

Novelli C and others, 'A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities', Working Paper, May 2024.

Novelli C and others, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity', arXiv preprint arXiv:240107348, Working Paper, March 2024.

O'Shaughnessy M., One of the Biggest Problems in Regulating AI Is Agreeing on a Definition, Carnegie Endowment, 2022.

OECD, Explanatory memorandum on the updated OECD definition of an AI system, March 2024.

OECD, Measuring the Environmental Impacts of AI Compute and Applications: The AI Footprint, 2022.

Owen D., *Products Liability Law*, 3rd edition, Thomson West, 2015.

Patti F., 'The European road to autonomous vehicles', *Fordham International Law Journal*, Vol. 43(1), 2019, 125–162.

Pfeiffer M., 'First, Do Harm. Algorithms, AI, and Digital Product Liability', Center for Urban Policy Research, Rutgers University, September 2023.

Poole D. and Mackworth A., *Artificial Intelligence: Foundations of Computational Agents*, 2nd edition, Cambridge University Press, 2017.

Regulatory Scrutiny Board Opinion, Liability rules for Artificial Intelligence, SEC(2022) 344.

Reimann M., 'Product liability', *Comparative Tort Law*, Edward Elgar Publishing, 2021.

Rogers W. (Ed.), *Unification of Tort Law: Multiple Tortfeasors*, Kluwer Law International, 2004

Rubinfeld D. and Gal M., 'Access barriers to big data', Arizona Law Review, Vol. 59, 2017, pp. 339-381.

Russell S. and Norvig P., *Artificial Intelligence: A Modern Approach*, 4th Global edition, Pearson Education, 2022.

Samuelson P., 'Generative AI meets copyright', Science, American Association for the Advancement of Science, Vol. 381(6654) , 2023, 158-161.

Schütte B., Majewski L. and Havu K., 'Damages liability for harm caused by Artificial Intelligence – EU law in flux', Helsinki Legal Studies Research Paper, 2021.

Shavell S., *Foundations of Economic Analysis of Law*, Harvard University Press, 2004.

Shavell S., 'Strict Liability versus Negligence', *The Journal of Legal Studies*, Vol. 9(1), The University of Chicago Press, 1980, pp. 1-25.

Sheehan M., 'China's AI regulations and how they get made', *Horizons: Journal of International Relations and Sustainable Development*, Vol. 24, Center for International Relations and Sustainable Development, 2023, pp. 108-125.

Simlinger F. and Mayer B., 'Legal responses to climate change induced loss and damage', *Loss and Damage from Climate Change: Concepts, methods and policy options*, Springer, 2019, pp. 179-203.

Spindler G., 'Die Vorschläge der EU-Kommission zu einer neuen Produkthaftung und zur Haftung von Herstellern und Betreibern Künstlicher Intelligenz', *Computer und Recht*, Verlag Dr. Otto-Schmidt, Vol. 8(11) , 2022, pp. 689-704.

Spindler G., 'User liability and strict liability in the Internet of Things and for robots', *Liability for artificial intelligence and the internet of things*, Nomos, 2019, pp. 125-144.

Sterlie S., Weng N. and Feragen A., 'Non-discrimination Criteria for Generative Language Models', arXiv preprint, arXiv:240308564, March 2024.

Stoffels M., 'Grundprobleme der Schadensersatzverpflichtung nach § 15 Abs. 1 AGG', *Recht der Arbeit*, Verlag C.H. Beck, Vol. 62(4), 2009, pp. 204-214.

Stokel-Walker C. and Noorden R., 'The Promise and Peril of Generative AI', *Nature*, Nature Research, Vol. 614, pp. 214-216.

Taddeo M. and others, 'Artificial intelligence and the climate emergency: Opportunities, challenges, and recommendations', *One Earth*, Cell Press, Vol. 4(6), 2021, pp. 776-779.

The Future Society, EU AI Act Compliance Analysis: General-Purpose AI Models in Focus, The Future Society, December 2023.

Thiel D., Identifying and Eliminating CSAM in Generative ML Training Data and Models, Stanford University, December 2023.

Thüsing G., '§ 15 AGG', *Münchener Kommentar BGB*, 9th edition, Verlag C.H. Beck, 2021.

Ulnicane I., 'Artificial Intelligence in the European Union: Policy, ethics and regulation', *The Routledge Handbook of European Integrations*, Taylor & Francis, 2022.

Van Alsenoy B., 'Liability under EU data protection law: from Directive 95/46 to the General Data Protection Regulation', *Journal of Intellectual Property, Information, Technology and E-Commerce Law*, Vol. 7(3), 2016, pp. 271-288.

van Staalduinen J., 'The Doctor and the Missing Link-EU Product Liability for Clinical (AI) Decision Support Systems', Working Paper, November 2023.

Vellinga N., 'Rethinking compensation in light of the development of AI', *International Review of Law, Computers & Technology*, Vol. 38(1), March 2024, pp. 1–22.

Verma P. and Oremus W., 'ChatGPT invented a sexual harassment scandal and named a real law prof as the accused', *The Washington Post*, 5 April 2023.

Vipra J. and Korinek A., 'Market concentration implications of foundation models: The Invisible Hand of ChatGPT', Working Paper, November 2023.

von Lindern J., 'Braucht die deutsche Vorzeige-KI mehr Erziehung?', Zeit Online, 11th September 2023.

Vries A. de, 'The growing energy footprint of artificial intelligence', *Joule*, Vol. 7(10), October 2023, pp. 2191-2194.

Wachter S., Mittelstadt B. and Russell C., 'Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI', *Computer Law & Security Review*, Vol. 41, 2021, 105567.

Wachter S., 'Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond', *Yale Journal of Law and Technology*, Vol. 26(3), 2024, pp. 671-718.

Wagner G., 'Einleitung zum Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz–ProdHaftG)', *Münchner Kommentar BGB*, 9th edition, Verlag C.H. Beck, 2021.

Wagner G., 'Liability Rules for the Digital Age – Aiming for the Brussels Effect', *European Journal of Tort Law*, Vol. 13(3), 2022, pp. 191-243.

Wagner G., 'Produkthaftung für autonome Systeme', *Archiv für die civilistische Praxis*, Vol. 217(6), 2017, pp. 707-765.

Wagner G., 'Robot Liability', *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019, pp. 27-62.

Wagner G., 'Vorbemerkung (Vor § 823)', *Münchner Kommentar BGB*, 9th edition, Verlag C.H. Beck, 2021.

Wendehorst C., 'AI liability in Europe: anticipating the EU AI Liability Directive', Ada Lovelace Institute, 2022.

Wendehorst C., 'Strict liability for AI and other emerging technologies', *Journal of European Tort Law*, Vol. 11(2), 2020, pp. 150-180.

Wendehorst C., 'The Proposal for an Artificial Intelligence Act COM (2021) 206 from a Consumer Policy Perspective', Study commissioned by the Austrian Federal Ministery of Social Affairs, Health, Care and Consumer Protection, 2021.

Wischmeyer T. and Rademacher T., *Regulating Artificial Intelligence,* Springer, 2020.

Xu W., 'From automation to autonomy and autonomous vehicles: Challenges and opportunities for human-computer interaction', *Interactions,* Vol. 28(2), 2020, pp. 48-53.

Zech H., 'Liability for AI: public policy considerations', *ERA Forum*, Vol. 22, 2021, pp. 147-158.

Zech H., 'Risiken Digitaler Systeme', *Weizenbaum Series*, Vol. 2, 2020.

Zeff M., California weakens bill to prevent AI disasters before final vote, taking advice from Anthropic, TechCrunch, 15 August 2024.

Zhang A., *High Wire: How China Regulates Big Tech and Governs Its Economy,* Oxford University Press, April 2024.

Zimmermann R., *The Law of Obligations: Roman Foundations of the Civilian Tradition*, Juta and Company Ltd, 1990.

Ziosi M. and others, 'The EU AI Liability Directive (AILD): Bridging Information Gaps', *European Journal of Law and Technology*, Vol. 14(3), December 2023.

Zuccon G., Scells H. and Zhuang S., 'Beyond CO2 Emissions: The Overlooked Impact of Water Consumption of Information Retrieval Models', *Proceedings of the 2023 ACM SIGIR International Conference on Theory of Information Retrieval*, August 2023, pp. 283-289.

Zuiderveen Borgesius F., 'Strengthening legal protection against discrimination by algorithms and artificial intelligence', *The International Journal of Human Rights*, Vol. 24(10), Taylor & Francis Online, 2020, pp. 1572-1593.

QA-01-24-010-EN-N

In September 2022, the European Commission presented a proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence (AILD), with an accompanying impact assessment. The European Parliament's Committee on Legal Affairs (JURI) requested the present complementary impact assessment of the proposal, which focuses on specific research questions. The study critique identifies key shortcomings in the European Commission's impact assessment, not least an incomplete exploration of regulatory policy options and an abridged cost-benefit analysis, in particular of the strict liability regime.

The complementary impact assessment study proposes that the AILD should extend its scope to include general-purpose and other 'high-impact AI systems', as well as software. It also discusses a mixed liability framework that balances fault-based and strict liability. Notably, the study recommends transitioning from an AI-focused directive to a software liability regulation, to prevent market fragmentation and enhance clarity across the EU.

This is a publication of the Ex-ante Impact Assessment Unit
EPRS | European Parliamentary Research Service

PDF ISBN 978-92-848-2244-7 | doi:10.2861/1723734 | QA-01-24-010-EN-N