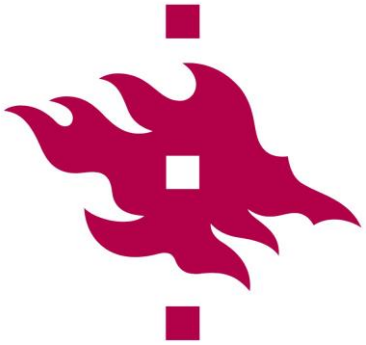

UNIVERSITY OF HELSINKI
FACULTY OF LAW

Damages Liability for Harm Caused by Artificial Intelligence – EU Law in Flux

BÉATRICE SCHÜTTE, LOTTA MAJEWSKI, KATRI HAVU

LEGAL STUDIES RESEARCH PAPER SERIES
Paper No 69

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

OIKEUSTIETEELLINEN TIEDEKUNTA
JURIDISKA FAKULTETEN
FACULTY OF LAW

Damages Liability for Harm Caused by Artificial Intelligence – EU Law in Flux

Béatrice Schütte, Lotta Majewski, Katri Havu*

Abstract: Artificial intelligence (AI) is an integral part of our everyday lives, able to perform a multitude of tasks with little to no human intervention. Many legal issues related to this phenomenon have not been comprehensively resolved yet. In that context, the question arises whether the existing legal rules on damages liability are sufficient for resolving cases involving AI. The EU institutions have started evaluating if and to what extent new legislation regarding AI is needed, envisioning a European approach to avoid fragmentation of the Single Market. This article critically analyses the most relevant preparatory documents and proposals with regard to civil liability for AI issued by EU legislators. In addition, we discuss the adequacy of existing legal doctrines on private liability in terms of resolving cases where AI is involved. While existing national laws on damages liability can be applied to AI-related harm, the risk exists that case outcomes are unpredictable and divergent, or, in some instances, unjust. The envisioned level playing field throughout the Single Market justifies harmonisation of many aspects of damages liability for AI-related harm. In the process, particular AI characteristics should be carefully considered in terms of questions such as causation and burden of proof.

I. Introduction

Artificial intelligence (AI) refers to a computer program or machine that can independently carry out tasks in a human-like manner, making independent conclusions and decisions. An AI application is 'trained' to carry out its tasks by utilising machine learning and large amounts of data.[1] AI is omnipresent in our everyday lives – sometimes even without our being aware of it. While AI is transforming our society, many legal issues related to this field have not been comprehensively resolved.

This is a potential problem regarding AI-related harm such as personal injuries, damage to property, and economic harm. If, for instance, a smart thermostat burns down the house or a robot makes a mistake in surgery, it is essential to know who bears the costs and under what conditions. Earlier rules or models of legal reasoning may not be easy to apply to factual settings involving AI, and the very essence of liability considerations is potentially affected by the involvement of AI. This applies, in particular, to situations where identifying the humans that 'caused' harm is challenging. The reason might be, for instance, the degree of autonomy that an AI system has, or the number of stakeholders – such as producers, other service providers and operators – that are involved.[2]

* Schütte (PhD, Postdoctoral Researcher) corresponding author, beatrice.schutte@helsinki.fi, Majewski (LLB, Research Assistant) and Havu (LLD, Assistant Professor) work at the University of Helsinki, Faculty of Law. This research has been conducted with the help of project funding granted by the Academy of Finland, decision number 330884 (2020). All online sources were last accessed on 30 April 2021. Relevant official documents published by 30 April 2021 have been taken into account in the drafting of this article.

[1] See eg Stuart J Russell and Peter Norvig, *Artificial Intelligence, A Modern Approach* (3rd ed Pearson 2016) 1–28; European Commission, 'Artificial Intelligence for Europe' (Communication) COM (2018) 237 final, 1. For the purposes of this article, it is not necessary to define and distinguish AI, intelligent automation and robotics in a detailed manner. More specific terminology is used in our text where necessary. See also eg Gerhard Wagner, 'Robot Liability' in Sebastian Lohsse, Rainer Schulze and Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things* (Hart 2019) 27–28.

[2] See also eg Gerald Spindler, 'User Liability and Strict Liability in the Internet of Things and for Robots' in Lohsse et al (n 1) 128, 130.

In the EU, national laws, as opposed to EU legislation, have traditionally played a major role within extra-contractual (tort) liability. Although existing national laws on damages liability and certain EU law rules – regarding, for example, product liability – can be applied to situations involving AI-related harm, the question arises whether the existing legal rules are sufficient for resolving AI-related cases efficiently, predictably and fairly. In this article, we explore preliminary plans and discussions about developing EU law in terms of liability for AI-related harm, and present comments on the desirability of new EU law rules and possible ways forward.

When considering the future of AI-related liability, the traditional approach of significantly relying on national damages liability laws and merely issuing field or situation-specific EU legislation covering certain specific questions[3] is not an automatically defective solution. AI-related harm does not necessarily differ from other harm so much that it would directly justify entirely new and comprehensive 'AI-liability legislation' from the standpoint of the substance of the law. The default system of extra-contractual liability in the EU Member States is fault-based liability, and for many situations involving AI-related harm these systems can be adequate.

However, additional legislation might be needed where existing damages liability rules would, for instance, be highly unpredictable in terms of case outcomes, or otherwise insufficient to efficiently and fairly resolve AI-related cases, or where broader policy goals concerning AI should be supported with a certain kind of liability rules. It could be wise to issue legislation at the EU level instead of relying on piecemeal – and divergent – steps taken by Member State legislators and courts. The latter will resolve issues concerning AI-caused harm on their own – a fact of which we already see multiple signs today – unless EU law addresses those issues first by introducing uniform rules across the Union. The goal of avoiding market fragmentation within the EU can be seen as justifying even comprehensive EU-level harmonisation of AI-related private liability.

In the following sections, we shall give an overview of preliminary plans and discussion regarding liability for AI-related harm on the EU level and in selected Member States. We will begin by addressing selected preliminary plans for legislation and policy papers issued by the European Commission (Commission) and the European Parliament (EP) (section II). We will also cover certain particular EU law rules already in force and discuss the significance of these rules in addressing AI-related harm as well as existing plans for developing those rules (section III). In terms of Member States, we will highlight some interesting examples of ongoing legislation under preparation and related discussions in section IV.

In section V, we take a broader view on AI-related harm and the status quo and the future of EU law. In terms of substance, we explain, for instance, how the involvement of AI can affect the evaluation of conditions for damages liability such as causation and fault, and whether this appears to signify that certain kinds of EU law rules are needed to avoid divergent or unpredictable application of existing national laws. Furthermore, we highlight problems and challenges in terms of plans concerning future EU legislation and discuss the desirability of

[3] For discussion see eg European Commission, 'Report on the safety and liability implications of AI, the Internet of Things and Robotics' COM (2020) 64 final, 12 (Safety and Liability Report) <https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en>; Sebastian Lohsse, Rainer Schulze and Dirk Staudenmayer, 'Liability for Artificial Intelligence' in Lohsse et al (n 1) 19; Wagner (n 1) 33–34; see also more broadly eg Walter van Gerven, 'Harmonization of Private Law: Do We Need It?' (2004) 41 (2) *Common Market Law Review* 505.

different kinds of amendments to existing EU law. The contribution closes with brief concluding remarks in section VI.

II. Plans for developing EU law

At the EU level, the need for legislation concerning AI has been recognised in diverse documents. In 2018, the Commission issued a Communication regarding a Strategy for AI,[4] accompanied by a Commission Staff Working Document on Liability for Emerging Digital Technologies.[5] In February 2020, a White Paper on AI[6] was published, as well as a report on the safety and liability implications of AI, the internet of things and robotics[7] and an Expert Group Report on Liability for AI and other Emerging Technologies.[8] The EP adopted a resolution on civil liability for AI-related harm in October 2020.[9] In April 2021, the Commission published a proposal for a regulation laying down harmonised rules on AI.[10] No final EU rules addressing general civil liability for AI-related harm have been adopted yet. A legislative proposal on liability for AI-related harm by the Commission is tentatively expected in 2022.[11]

A. Commission

(i) White Paper on AI

The Commission considers it necessary to make the policy decisions concerning novel technologies at the EU level, and aims at creating an ecosystem of excellence and trust with regard to AI.[12] A regulatory and investment-oriented approach will promote the uptake of AI while addressing the risks related to use of these emerging technologies. Close cooperation with Member States is also considered important in key areas such as research, investment, market uptake, skills and talent, data, and international cooperation.[13]

According to the Commission, it must be considered how the existing legal frameworks applicable to AI systems should be amended. Moreover, any future regulation must be flexible

---

[4] European Commission, 'Artificial Intelligence for Europe' (Communication) COM(2018) 237 final <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF>.

[5] European Commission, 'Liability for emerging digital technologies' SWD(2018) 137 final (Staff Working Document) <https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies>.

[6] European Commission, 'On Artificial Intelligence – A European Approach to excellence and trust' COM (2020) 65 final (White Paper) <https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en>.

[7] Safety and Liability Report (n 3).

[8] Expert Group on Liability and New Technologies, 'Liability For Artificial Intelligence And Other Emerging Digital Technologies' (European Union 2019) <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>.

[9] EP, 'Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence' 2020/2014(INL) (Resolution on Civil Liability or Parliamentary Resolution) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html#title1>.

[10] European Commission Proposal for a Regulation of the European Parliament and of the Council laying down harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) 2021/0106 (COD) ('Draft AI Act').

[11] See European Commission 'Coordinated Plan on Artificial Intelligence, 2021 Review' 35.

[12] White Paper (n 6) 3, 5–6.

[13] Ibid 1, 5.

enough to accommodate technological developments. Future rules concerning liability for AI-related harm should cover both products and services.[14]

The Commission wishes to create an effective regulatory framework, which at the same time does not create inappropriate burdens, especially for SMEs. This will be achieved by following a risk-based approach.[15] In this regard, an AI application should be considered high-risk when two cumulative criteria are met: (1) *AI is employed in a sector where significant risks are likely to materialize, such as healthcare or transport*. These sectors should be exhaustively listed in a prospective legal instrument and the list should be regularly reviewed and amended. (2) *The manner in which the application is used makes it likely that significant risks will materialize.* Risk assessments should be based on the possible impact on affected parties. Where there is an imminent risk of injury, death or significant other harm or where the rights of an individual or a company are significantly affected, an AI system should be deemed to be high-risk. Certain AI applications could be considered high-risk due to their intended use alone, for instance AI used in recruitment of employees and remote biometric identification technologies.[16]

The Commission states that obligations and responsibility related to the utilisation of AI should be placed on the actor most able to control a specific risk. In addition, it is considered crucial that providers of AI products in the EU are subject to its regulatory framework, regardless of where the operator is established.[17]

(ii) Safety and Liability Report

The Safety and Liability Report published in February 2020 deals with key issues then identified. It acknowledges the potential of new technologies, but also recognises the risk of causing harm to legally protected interests. The Report notes that AI, the Internet of Things (IoT) and robotics share several properties, such as the ability to combine connectivity, autonomy and data dependency to perform tasks with little to no human intervention. Further, these systems owe their high degree of complexity to the plurality of stakeholders involved in the supply chain and the number of different components.[18] When AI systems are part of complex IoT environments, it may be difficult or even impossible to pinpoint the origin of damage and thus the person responsible for it. A harm-sufferer is then probably unable to prove the necessary conditions for a successful damages claim.[19]

The Report explains that the Commission is indeed considering adopting a strict liability regime to address AI applications with a certain risk profile. Such a regime could be linked to an insurance scheme comparable to the rules in place for motor vehicle liability. This would ensure that harm-sufferers can obtain compensation regardless of a wrongdoer's solvency.[20]

(iii) Commission draft: harmonised rules for the utilisation of AI

[14] Ibid 16.
[15] Ibid 10–17.
[16] Ibid 18.
[17] Ibid 22.
[18] Safety and Liability Report (n 3) 2.
[19] Ibid 14.
[20] Ibid 16.

The proposed rules in the 'Draft AI Act' – which cover several issues previously raised in policy papers – will apply to both private and public actors and address the utilisation of AI (without providing comprehensive liability rules). Through the Draft AI Act, the Commission seeks to ensure a high level of protection of fundamental rights while pursuing four main goals, namely (1) to ensure that AI systems are safe and respect Union values and fundamental rights, (2) to ensure legal certainty, (3) to enhance governance and effective enforcement and to (4) facilitate the development of a Single Market for lawful, safe and trustworthy AI.[21] A clear focus is placed on procedural and administrative issues, such as the establishment of supervisory bodies or the laying down of duties to be held by different actors in value chains.[22]

The proposal underlines the need for regulating the utilisation of AI according to a risk-based approach.[23] However, in this new document the Commission no longer relies on open criteria to define high risk items, as was done in the White Paper, but instead on an exhaustive list of high-risk AI systems.[24] The objective to cover the entire life-cycle of an AI system is central in the Commission proposal and, therefore, a monitoring scheme for high-risk AI systems is proposed.[25] Liability is only addressed in relation to the regulatory sandbox scheme, that is, a controlled environment to test innovative AI technologies.[26] The proposal sets out (Article 53 (4)) that participants in the regulatory sandbox should be liable under EU and Member States liability legislation for any harm inflicted on third parties as a result of experimentation taking place in the sandbox.

B. European Parliament

The EP has published several documents regarding AI. The Resolution on Civil Liability was adopted in October 2020,[27] alongside a resolution related to an intellectual property rights system concerning AI as well as a resolution on a framework on ethical principles. Earlier, in May 2020, the Committee on Legal Affairs issued a draft report with recommendations to the Commission on a civil liability regime for AI.[28] In July 2020, the JURI Committee of the EP released a study on AI and civil liability, commissioned by the Policy Department for Citizens' Rights and Constitutional Affairs.[29]

(i) Resolution on Civil Liability

The Parliamentary Resolution of 2020 entails a proposal for a future regulation (the Draft Regulation).[30] In Article 3 of the Draft Regulation, the EP defines an AI system as a 'system that is either software-based or embedded in hardware devices, and that displays behaviour

[21] Draft AI Act (n 10), Explanatory Memorandum, see in particular 11, 3.
[22] See eg Articles 16–29, 30–39, 56–59 of the Draft AI Act (n 10).
[23] Draft AI Act (n 10), Explanatory Memorandum, 13; Title III of the Commission draft legislation concerning the utilisation of AI.
[24] Draft AI Act (n 10), Article 6 and Annex III to the Commission draft legislation concerning the utilisation of AI.
[25] See Articles 61, 62 of the Draft AI Act (n 10).
[26] Recital 72, Articles 53–55 of the Draft AI Act (n 10).
[27] Resolution on Civil Liability (n 9).
[28] EP, 'Draft report with recommendations to the Commission on a civil liability regime for artificial intelligence' 2020/2014(INL) (Draft Report) <https://www.europarl.europa.eu/doceo/document/JURI-PR-650556_EN.pdf>.
[29] Andrea Bertolini, 'Artificial Intelligence and Civil Liability' (European Union 2020) (EP JURI Study) <https://www.europarl.europa.eu/thinktank/fi/document.html?reference=IPOL_STU%282020%29621926>.
[30] Resolution on Civil Liability (n 9), see eg Introduction para 5.

simulating intelligence by, inter alia, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals'. The Resolution notes that a full revision of existing liability regimes is not necessary but that aspects of AI which challenge existing regimes such as opacity, connectivity and modification through updates should be addressed by new rules.[31]

Regarding cases where harm is inflicted through interference by a third party, for instance through a cyber-attack, the EP considers the existing fault liability regimes of the Member States sufficient.[32] However, a comprehensive harmonised regime setting out the liability of the operator of an AI application is central to the proposal. The notion of 'operator' is to be understood broadly. If there is more than one operator, all of them should be jointly and severally liable.[33]

(ii) Draft Report

Many points presented in the Draft Report were later incorporated and further elaborated on in the Parliamentary Resolution of 2020. The EP opined in the Draft Report that national fault-based liability rules already offer sufficient protection in cases where a third person interferes. Furthermore, the document discusses possible modifications to the EU product liability regime, and for example states that 'backend developers' should be liable as producers under the Product Liability Directive (PLD).[34] The Draft Report also proposes a strict liability regime for high-risk AI systems. It is evident that the definition of 'high-risk' adopted in the Resolution on Civil Liability has been based on the definition in the Draft Report.[35]

While the Resolution on Civil Liability focuses on the liability of the operator, the Draft Report mainly discusses the liability of the 'deployer', defined as the person 'who decides on the use of the AI system, who exercises control over the risk and who benefits from its operation'.[36] This definition corresponds in most parts to that of the 'frontend operator' in the Resolution.[37]

(iii) European Parliament JURI Study – AI and civil liability

The EP JURI study states that regulation of technology should be minimally invasive. Emerging new technologies should be monitored by an expert group or a dedicated agency. Further, liability should be placed upon the party who is in control of risks and therefore in the best position to manage risk.[38] In this study, an attempt to define and regulate all existing and possible future uses of AI is deemed ineffective.[39] The study also discusses AI applications as products and whether AI or robots should be assigned legal personhood.[40]

---

[31] Ibid Annex, A. Principles and aims of the Proposal para 5.
[32] Ibid para 9.
[33] Ibid, para 13; Arts 4, 8 and 11 of the Draft Regulation.
[34] Draft Report (n 28) para 7, Annex Rec 7.
[35] Ibid para 14.
[36] Ibid para 11.
[37] See Resolution on Civil Liability (n 9), para 12; Art 3(e) of the Draft Regulation.
[38] EP JURI Study (n 29) 12.
[39] Ibid 31–32.
[40] Ibid 33–46.

III. Existing and planned EU rules that address liability in specific situations

While no harmonised civil liability regime is in place for AI applications in the EU, several pieces of particular legislation affect liability for AI-related harm in specific situations. The PLD of 1985[41] is one of those instruments. Additionally, EU product safety legislation – significantly harmonised within the Single Market[42] – is relevant as well. Liability rules applicable to AI-related harm are also included, for instance, in EU legislation on data protection as well as in provisions addressing medical devices. We will now take a closer look at certain particular rules and future plans that are relevant to AI-related harm.

A. Product liability and product safety

The PLD imposes no-fault liability on European producers. Where a defective product causes damage to a consumer, the producer may be liable irrespective of negligence or fault on their part.[43] Ever since the PLD entered into force, discussions have been ongoing regarding whether the framework is fit for its purpose and whether it can sufficiently accommodate new developments in line with technical progress. These issues have also been taken up in policy papers and in the Resolution on Civil Liability.[44]

The rules on product safety and product liability complement each other. Product safety rules[45] are mainly intended to ensure that unsafe products do not become available in the first place. Product liability rules have a dual function: they are an ex-post corrective to apply when harm has already occurred and provide harm-sufferers with a legal basis for their damages claim. Due to the deterrent effect of liability rules, they provide producers with an additional incentive to ensure the safety of their products.[46]

According to the Commission, individuals suffering damage through new technologies should have the same level of protection as victims of traditional technologies.[47] The White Paper states that 'all options to ensure this objective should be carefully assessed, including possible amendments to the Product Liability Directive and possible further targeted harmonisation of national liability rules'.[48] However, the points brought forward by the Commission in this regard are vague and do not include any concrete proposals to solve deficits.

---

[41] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products OJ L 210 (PLD).

[42] See in particular Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety OJ L 11.

[43] See also eg European Commission, 'Liability of defective products' <https://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en>.

[44] See eg Safety and Liability Report (n 3) 14; Resolution on Civil Liability (n 9) para 8; EP JURI Study (n 29) 47–62.

[45] See eg Directive 2001/95/EC; Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 OJ L 218; Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) OJ L 157.

[46] The prevailing approach suggests that liability rules have a deterrent effect – despite criticism of this assumption. The EU institutions consider that the deterrent effect is relevant. See eg Resolution on Civil Liability (n 9) lit. A; Safety and Liability Report (n 3) 12. For discussion see also eg Helmut Koziol, *Basic Questions of Tort law from a Germanic Perspective* (Jan Sramek Verlag 2012) 78.

[47] Safety and Liability Report (n 3) 13, 16–17.

[48] White Paper (n 6) 15.

The PLD has several evident shortcomings in terms of adjudicating cases involving AI-related harm which stem in particular from its scope of application as well as the concepts of 'product', 'defect' and 'damage'.[49]

Pursuant to its wording, the scope of application of the PLD is *limited to relations between business and consumer (B2C)*, at least in terms of addressing harm to property.[50] Thus, its strict liability regime is relevant, in particular, in cases concerning AI systems for private use, such as private vehicles, computers, smartphones, or smart home devices. It has been argued that this is contradictory to the legal basis of the PLD, which was harmonisation of laws to ensure the functioning of the internal market (corresponding to today's Article 114 of the TFEU).[51]

As per Article 2 of the PLD, the term *product* refers to all movables, including electricity. The scope as such is broad, covering agricultural products as well as complex industry products. The idea behind the broad notion of a 'product' was to create 'future-proof' legislation.[52] AI applications are, as a starting point, products under the PLD if they are movable items or incorporated in movable items. Classification as a product is more difficult in relation to software and data.

Article 6(1) of the PLD establishes that 'a product is *defective* when it does not provide the safety which a person is entitled to expect, taking all circumstances into account'. The presentation of a product and its reasonably expected use are relevant here. In this context, questions arise in terms of the expected degree of safety and whether the producer should anticipate certain possible misuse.[53] According to the Commission, the producer must indeed consider foreseeable misuse.[54] The notion of 'defect' can be problematic when a case concerns algorithms or software.

Pursuant to Article 9 of the PLD, *damage* refers to harm caused by death or personal injury as well as harm to property items other than the defective product itself, provided that the item of property was intended for private use or consumption and actually used or consumed privately. Pure economic loss or non-material harm are not covered by the Directive. However, these types of harm may occur when AI systems are used. Harm-suffers must rely on national laws to recover losses not covered by the PLD (if no other particular EU liability rules apply).

Evaluation reports concerning the PLD indicate that it appears difficult for harm-sufferers to *prove* a defect in a product and a causal link between the defect and the damage suffered. This issue has been particularly discussed in the context of pharmaceuticals and complex technical products, noting that harm-sufferers lack the necessary expertise to prove a defect and its causal link to damage.[55] Additionally, several recent documents published by EU bodies underline

[49] See also section V.B.(i) below.
[50] See eg Art 9 PLD stating that damage to property is only recoverable if it relates to damage caused to items intended for private use.
[51] See eg Willem H van Boom, Jean-Sébastien Borghetti, Andreas Bloch Ehlers, Ernst Karner, Donal Nolan, Ken Oliphant, Alessandro Scarso, Vibe Ulfbeck and Gerhard Wagner, 'Product Liability in Europe' in Helmut Koziol, Michael D. Green, Mark Lunney, Ken Oliphant, and Lixin Yang (eds), *Product Liability: Fundamental Questions in a Comparative Perspective* (De Gruyter 2017) 257. See also Safety and Liability Report (n 3) 12.
[52] European Commission, 'Evaluation of Council Directive 85/374/EEC' (Working document) (2020) 23.
[53] EP JURI Study (n 29) 57.
[54] Safety and Liability Report (n 3) 6.
[55] European Commission, 'Evaluation of Council Directive 85/374/EEC' (Working document) (2020) 25; European Commission, 'Third report on the application of Council Directive on the approximation of laws, regulations and

that due to the complexity of new technologies, it will be highly challenging for harm-sufferers to prove the link between defect and damage.[56]

B. GDPR

Some existing legislation may have further-reaching scope than is immediately obvious. The particular legislation contained in the General Data Protection Regulation (GDPR)[57] is applicable when processing personal data. AI applications in data processing are ubiquitous, and a seemingly minor personal data processing task may bring an entire AI system under the scope of the GDPR's liability rules.

Article 82 of the GDPR states that any person who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to compensation from the controller or processor for the damage suffered. Article 82 establishes the liability of the controller[58] when the damage is caused by processing which infringes the GDPR. The processor[59] is liable for damage caused by processing only when it has not complied with the obligations set in the Regulation or where it has acted outside or contrary to the lawful instructions of the controller.

While drafting the GDPR liability rules, some similar issues had to be considered as is the case when contemplating legislation on AI-related harm, most notably the asymmetry of information between the potential claimant and the defendant.[60] The controller or processor must prove that they are not in any way responsible for the event giving rise to the damage in order to be exempt from liability.[61] Additionally, Article 80 of the GDPR allows for relevant NGOs to lodge complaints on data subjects' behalf, which increases the likelihood of holding data controllers or processors accountable for breaching the Regulation.

The GDPR does not, however, lay down exhaustive rules on damages liability; national laws of Member States play a complementary role.[62] Therefore, private liability for breaching this Regulation is not entirely harmonised within the EU and diverging case outcomes are possible. The GDPR requires full compensation and states that the notion of damage should be interpreted broadly. But there are no exhaustive definitions of relevant harm and causation, nor are rules available for proving these.[63] National rules and traditions regarding, for instance, compensation for non-material harm, or requirements in terms of showing causation, can have a significant impact on whether and what kind of compensation is ultimately awarded.

---

administrative provisions of the Member States concerning liability for defective products (85/374/EEC of 25 July 1985, amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999)' COM (2006) 496 final 9. Even though harm-sufferers' (arguable) difficulties in terms of proving defect and causation were noted, eg, already in the PLD evaluation report of 2006, this matter did not lead to revising legislation.

[56] See eg White Paper (n 6) 13.

[57] 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 (2016) OJ L 117 (GDPR).

[58] As per Art 4(7) GDPR, the controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data.

[59] The processor is defined in Art 4(8) GDPR as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[60] See GDPR Recs 39, 58, and Art 12.

[61] See GDPR Art 82(3).

[62] See GDPR Art 82, Art 79(2), and Rec 146.

[63] See GDPR Art 82, and Rec 146.

C. Digital Services Act and the E-Commerce Directive

In early 2020 the Commission announced its intention to table a new Digital Services Act and gave its proposal for a new regulation in December 2020.[64] The aim of the new legislation is to modernise the legal framework surrounding digital services by replacing rules now contained in the E-Commerce Directive (ECD).[65] The proposal maintains the general framework on the responsibilities of providers of intermediary services set out in the ECD.[66]

The new legislation is – as are the existing rules – relevant for some situations where AI-related harm occurs, since, for example, different kinds of platforms moderate content utilising AI in the process.[67] Illegal or harmful online content includes crime-related content (such as child pornography, libel) and, for example, false statements concerning certain products or companies.[68] In this context, non-material and economic harm can be caused either by blocking content which should not have been blocked, or by *not* blocking illegal content which could then cause illicit harm.[69] Existing EU law addresses the question when platforms can escape liability, but details of damages liability are governed by national laws.[70]

The Commission has outlined two key objectives for the new Digital Services Act. First, to propose clear rules framing the responsibilities of digital service providers to ensure effective supervision and enforcement. Secondly, to propose ex ante rules to make sure that 'gatekeeper platforms' behave fairly and to promote competition.[71] As no law has yet been finalised, it remains to be seen what kind of EU law rules the Digital Services Act will ultimately set out that are relevant for damages liability. In any event, it seems as though details of damages liability would, to a notable extent, remain governed by national laws (or other EU law).

D. Rules on medical devices

The Medical Devices Regulation (MDR)[72] is another sector-specific piece of legislation which contains provisions applicable to the use of new software technology. The Regulation

---

[64] European Commission, 'Annexes to the Commission Work Programme' COM (2020) 440 final <https://ec.europa.eu/info/sites/info/files/cwp-2020-adjusted-annexes_en.pdf>; European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM/2020/825 final (Digital Services Act Proposal).

[65] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (2000) OJ L 178 (ECD).

[66] Digital Services Act Proposal (n 64) 3.

[67] See also eg European Commission, 'Recommendation of 1.3.2018 on Measures to Effectively Tackle Illegal Content Online' C (2018) 1177 final, Recs 24, 36, 37, and Recommendation paras 19, 20, 36, 37.

[68] See also eg C (2018) 1177 final.

[69] See also eg Maja Brkan, 'Freedom of Expression and Artificial Intelligence: on Personalisation, Disinformation and (lack of) Horizontal Effect of the Charter' (SSRN 2019) 1, 3–6, 13–14, 17 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354180>.

[70] See the ECD, and eg Alexandre de Streel, Miriam Buiten and Martin Peitz, *Liability of online hosting platforms: should exceptionalism end?* (Centre on Regulation in Europe 2018) 13–16.

[71] European Commission, 'The Digital Services Act package' <https://ec.europa.eu/digital-single-market/en/digital-services-act-package>.

[72] Regulation 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (2017) OJ L 117 (MDR).

succeeded the Medical Devices Directive,[73] and aimed for more comprehensive harmonisation within the Single Market than its predecessor. The Regulation applies to software classified as a medical device or software working with a medical device. Software in its own right, when specifically intended by the manufacturer to be used for one or more medical purposes, qualifies as a medical device.[74]

Under the MDR, medical device manufacturers are liable for all claims arising from their product. The MDR sets out, in Article 10(16): 'Natural or legal persons may claim compensation for damage caused by a defective device in accordance with applicable Union and national law. Manufacturers shall, in a manner that is proportionate to the risk class, type of device and the size of the enterprise, have measures in place to provide sufficient financial coverage in respect of their potential liability [under the PLD] without prejudice to more protective measures under national law.'[75] The provision signifies, in practice, that there must be adequate liability insurance for covering no-fault liability.[76]

As noted above, under the PLD a product is defective when it does not provide the safety which a person is entitled to expect. Notably, the European Court of Justice (CJEU) has established that patients are entitled to expect a higher standard of safety from medical devices, such as pacemakers. Furthermore, the cost of replacing a potentially problematic medical device can be recoverable.[77] Therefore, some sectoral divergence can be seen here in terms of what constitutes a defect and recoverable harm under the PLD.

The MDR contains a risk-based classification system which determines, for example, the level of safety requirements and sufficient financial coverage for potential liability.[78] High-risk products, if defective, are more likely than low-risk products to cause personal injury to or death of a patient. All software is classified as class I, lowest risk, unless it is intended to provide information which is used to take decisions for diagnostic or therapeutic purposes or intended to monitor physiological processes.[79] Software which drives a device or influences the use of a device falls within the same class as the device.[80] This kind of categorisation based on intended purpose is also evident, for example, in the White Paper on AI in terms of when utilisation of AI is seen as high-risk.[81]

While manufacturers of medical devices are generally familiar with strict quality control and liability concerns, the MDR brought further responsibilities to a broader scope of software

[73] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (1993) OJ L 169.
[74] MDR Rec 19 and Art 2(1).
[75] The new requirements concerning financial safeguards originate, in part, from a 'breast implant scandal'. See eg European Commission, 'Medical devices: European Commission calls for immediate actions - tighten controls, increase surveillance, restore confidence' (Press release 9.2.2012) <https://ec.europa.eu/commission/presscorner/detail/el/IP_12_119> ; Victoria Martindale and Andre Menache, 'The PIP scandal: an analysis of the process of quality control that failed to safeguard women from the health risks' (2013) 106(5) *Journal of the Royal Society of Medicine* 173–177; Case C-581/18 *TÜV Rheinland LGA Products & Allianz IARD*, ECLI:EU:C:2020:453.
[76] See also eg European Commission, 'Implementation Model for medical devices Regulation – Step by Step Guide' (European Union 2019) part 4 <https://ec.europa.eu/docsroom/documents/33661>.
[77] See Joined Cases C-503/13 and C-504/13 *Boston Scientific Medizintechnik*, ECLI:EU:C:2015:148. The Court found that a patient's pacemaker was defective under the PLD even though no defect had been detected in that particular pacemaker. This was because the pacemaker belonged to a product group that had been determined as posing a higher risk of failure. See also discussion by eg Martin Peiffer, 'Defective Medical Devices – How New European Legislation is Shaping German Liability Laws' [2019] *GenRe Casualty Matters*.
[78] MDR Rec 31.
[79] Ibid annex VIII, chapter III, 6.3. Rule 11.
[80] Ibid annex VIII, chapter II, 3.3.
[81] White Paper (n 6) 17.

manufacturers. The MDR also made manufacturers responsible for issues arising from their software being incompatible with devices that fit their intended use.[82] This can be seen as broadening software manufacturers' liability, and also extending liability to an area which is not entirely in their control after they have released their software. The rule nevertheless resolves the problem of allocating responsibility in value chains that have different manufacturers for software and hardware.

IV. In the meanwhile in Member States

As the EU still lacks comprehensive law on AI-related private liability and allocation of risk, Member States can create their own liability rules and make decisions in terms of how the involvement of AI should be taken into account in applying existing law to court cases. At the same time, many Member States have held back from creating new comprehensive national frameworks due to the work currently being done by EU bodies. National published strategies concerning AI-related legislation express the need for preparing or waiting for EU-level legislation. In any event, individuals and companies utilising AI applications need legal certainty. While national systems attempt to fill this need, the EU runs the risk of a quickly fragmenting Single Market. As regards ongoing developments and discussions, one can highlight certain interesting examples.

A. Automated driving

In 2017, the German Bundestag adopted amendments to the Road Traffic Act relating to automated driving. German legislation previously already covered assisted and partially automated driving as at these levels the driver has control over the vehicle. However, as from automation level 3 onwards,[83] the driver may pay attention to other issues. This was not covered by legislation and was thus prohibited or at least problematic.[84] The government added § 1a and § 1b to the German Road Traffic Act establishing requirements for the permissibility of highly and fully automated driving as well as the driver's rights and obligations. Liability remains governed by § 7 of the Road Traffic Act. The keeper[85] is strictly liable to pay compensation if during operation of the vehicle a person is killed or injured, or damage is caused to property. In addition, pursuant to § 18 of the Road Traffic Act, also the driver is liable to compensate damage unless he proves that harm was caused without his fault.[86] Thus, the introduction of autonomous vehicles in road traffic will not lead to changes in related liability law.

---

[82] MDR annex I, chapter I, 14.5.

[83] There are five automation levels: Level 1 means assisted driving with systems like cruise control. Level 2 is partially automated driving where the system performs tasks like parking or keeping the vehicle on course. The driver must pay attention at all times. Level 3 refers to highly automated driving where the driver need not pay full attention to traffic but must be prepared to resume control. At level 4, fully automated driving, the driver may be asked to resume control; however, the system is able to safely stop the vehicle if the driver does not resume control. Level 5 means autonomous driving where the vehicle has only passengers but no drivers. See Wissenschaftliche Dienste des Deutschen Bundestages 'Autonomes und automatisiertes Fahren auf der Straße – rechtlicher Rahmen' (2018) *Ausarbeitung WD 7-3000 -111/18* 4.

[84] Ibid 5.

[85] The keeper of the vehicle is the person operating it in their own name and on their own account. See eg Michael Burmann, Rainer Heß, Kathrin Hühnermann and Jürgen Jahnke, Straßenverkehrsrecht (C.H. Beck 2020) § 7 para 5; BGH [1997] *Neue Juristische Wochenschrift*, 660; BGH [1983] *Neue Juristische Wochenschrift* 1492. As per § 7 (3), the keeper is not liable if a third person used their vehicle without their knowledge of it.

[86] This will mainly be the case if the cause of the accident was a technical problem, such as a malfunction of the brakes. See eg Burmann et al (n 85) § 18 para 8.

In Estonia, the discussion relates to whether autonomous vehicles can be classified as motor vehicles under the scope of the Estonian Traffic Act; however, they do count as motor vehicles under the Estonian Law of Obligations Act (LOA).[87] The current approach is that strict liability could be applied to damage caused by autonomous vehicles and that this does not require an overhaul of the LOA regime.[88]

Academics estimate that mandatory motor insurance schemes will lose relevance as autonomous vehicles become common while manufacturers' product liability will gain more importance. The exact relationship between the keeper's liability for road traffic accidents and product liability remains to be determined.[89] From an EU point of view, treating traditional and autonomous vehicles differently insurance-wise is not envisioned.[90]

B. Austria – draft of new civil liability rules

In 2005, a working group of the Austrian Federal Ministry of Justice presented the draft of a new set of civil liability rules. This includes, for example, contractual and non-contractual liability for technical support mechanisms that replace a human agent.[91]

In terms of non-contractual liability, draft § 1306(4) states that the principal is liable for the failure of technical aids employed in the same way as the principal would be liable for the conduct of an agent if the principal fails to meet the standard of care in selecting and monitoring a technical aid or when a technical aid was not fit for the purpose. A reversed burden of proof should apply in B2C relationships. The working group argues that a person should not be able to circumvent liability by simply employing a machine instead of a human servant.[92] However, equal treatment of human agents and machines has been criticised. As liability for damage caused by an agent requires misconduct by the latter, the question arose as to how to determine 'misconduct' by a machine. As the draft refers to a failure, it has been asked whether the principal should be exonerated in the case of the unavoidable breakdown of an otherwise reliable machine.[93]

C. Finland: administrative accountability

In Finland, ongoing discussion focuses on automated administrative decision-making. The lack of cohesive legislation around it has been noted by the Constitutional Law Committee, which has called for updated legislation.[94] The Ministry of Justice published an assessment memorandum on whether, for example, current legislation guarantees compensation for harm caused in office within the public administration. The Ministry noted that from the standpoint

[87] Janno Lahe and Taivo Liivak, 'Strict liability for damage caused by self-driving vehicles: the Estonian perspective' (2019) 12(2) *Baltic Journal of Law & Politics* 1, 6.
[88] Ibid 15–16.
[89] Gerhard Wagner, 'Produkthaftung für autonome Systeme' (2017) 217 *Archiv für die civilistische Praxis* 707, 709.
[90] Safety and Liability Report (n 3) 13.
[91] See eg 'Diskussionsentwurf der beim Bundesministerium für Justiz eingerichteten Arbeitsgruppe für ein neues österreichisches Schadenersatzrecht' [2008] *Juristische Blätter* 365–372.
[92] Gerhard Wagner, 'Reform des Schadensersatzrechts' [2008] *Juristische Blätter* 12.
[93] Ibid 13.
[94] See eg Constitutional Law Committee, *'Valiokunnan lausunto PeVL 7/2019 vp—HE 18/2019 vp'* (2019) 8–9.

of ensuring compensation for harm suffered by individuals, it may be sufficient to hold the relevant public office accountable as a whole.[95]

D. Estonia

Estonia installed an AI taskforce which pointed out certain key aspects to be addressed by future legislation. These include liability and allocation of risks between the creator, manufacturer, and user of autonomous AI. They suggested that the party who benefits from use of self-learning AI software should also bear liability for errors, even if the system itself was unpredictable.[96] They urged reviewing the rules on burden of proof as regards consumer protection.[97] Estonia's general approach focuses primarily on tearing down the barriers in the way of further adoption of AI in business and administration.[98]

V. Discussion

In this section, we will first explore key issues in terms of applying liability rules, and general liability laws in particular, to harm caused by AI. After that, we will move on to discuss the future of the European legal landscape, covering, among other things, the desirability of certain amendments to existing EU law. We will also present comments regarding liability rules that have been proposed recently.

A. Substantive questions concerning AI-caused harm

Currently, considerable uncertainty and discussion surrounds the theme of whether and to what extent existing legal doctrines already resolve the issue of liability for AI-related harm. The main approach appears to remain that actions of autonomous machines can be attributed to individuals or groups of humans.[99] However, machine-learning techniques allow AI-driven devices to make decisions on their own without humans playing any role in decision-making.[100] The more autonomous machines become, the more difficult will be attribution of their decisions to humans. Where humans' ability to genuinely supervise the actions of AI lessens, the classic elements of damages liability considerations such as the obligation to live up to the standard of care may seem void.[101] Nonetheless, the Parliamentary Resolution and the EP JURI Study submit that there will always be a human in the value chain who can be expected to bear responsibility.[102] However, in some situations the responsible parties might not always be obvious on the basis of facts alone.

---

[95] Niklas Vainio, Valpuri Tarkka and Tanja Jaatinen, 'Assessment memorandum on the need to regulate automated decision-making within public administration in general legislation' (Finnish Ministry of Justice 2020) VN/3071/20208 50.
[96] Siim Sikkut et al, 'Report of Estonia's AI Taskforce' (Ministry of Economic Affairs and Communications 2019) 39.
[97] Ibid 39, 40.
[98] See eg ibid 17, 22, 29, 38.
[99] Eg Mark Chinen, 'The Co-Evolution of Autonomous Machines and Legal Responsibility' (2016) 20 *Virginia Journal of Law & Technology* 339, 342.
[100] See also eg Woodrow Barfield, 'Liability for autonomous and artificially intelligent robots' (2018) 9 *Paladyn, Journal of Behavioral Robotics* 193.
[101] See eg Yavar Bathaee, 'The Artificial Intelligence Black Box and The Failure of Intent and Causation' (2018) 31(2) *Harvard Journal of Law & Technology* 889, 891; Chinen (n 99) 343.
[102] Resolution on Civil Liability (n 9) para 7. See also EP JURI Study (n 29) 37. Additionally, the Commission notes that the behaviour of AI applications is in any event determined by (human) developers programming them. See White Paper (n 6) 16.

(i) Liable parties

As AI systems are characterised by complex value chains involving multiple stakeholders, a central question is: Who in the value chain incurs liability and under what circumstances?

It should be briefly noted here that one measure proposed in terms of regulating private liability for AI-related harm is assigning legal personhood to AI or robots and legislating on their 'independent liability', thus 'simplifying' considerations regarding who should bear the costs of accidents.[103] However, this is not a reasonable manner of resolving the question of allocation of liability and is clearly not easily feasible. Legal personhood would require significant legislative steps, and intricate legal and practical questions would need to be addressed in terms, for instance, of funds 'governed' and 'owned' by an AI application or a robot. A similar solution that has emerged is utilising a corporation-like legal-fiction tool to group together the potentially liable humans and organisations behind an AI application.[104] Nonetheless, nothing in AI applications inherently requires any kind of artificial construction such as this, or legal personhood for AI, even as a 'shorthand' for attributing liability. There is no liability gap as such.[105] All that is needed are clear and easily administrable rules on whether the operator of AI, the manufacturer or someone else bears the costs in the event of an accident. Laudably, in its 2020 Resolution on Civil Liability, the EP does not see any necessity to provide AI systems with any form of legal personality.[106]

Regulatory choices dictate which actors are liable for AI-related harm. Under a risk-management approach, the liable party would always be the one best suited to minimise risks.[107] The opaqueness and unpredictability of AI applications as well as the rapidly evolving technological reality might, in some instances, make it difficult to correctly identify this party. In any event, the EU legislators, for example, appear to assume that the identification is usually possible.[108]

Liability of the 'producer' or 'manufacturer' refers to holding the producer of an AI application accountable for accidents.[109] Especially when combined with strict liability, this is a powerful incentive – or disincentive – and as a legislative solution should therefore only be utilised with care. Notably, this kind of liability has been traditionally employed in contexts where the producer or the manufacturer is well-placed in terms of preventing accidents and taking precautions. In the case of AI applications this might not be so due to inherent inability to foresee some accidents.[110] Additionally, severe producer liability can deter innovation because, in order to avoid accidents, the producer might want to ensure that the AI application is not modified or combined with other instruments.

---

[103] See for discussion eg EP JURI Study (n 29) 33–39; Mark Chinen, *Law and Autonomous Machines* (Elgar Publishing 2019) 194–222; Wagner (n 1) 53–62.
[104] See eg EP JURI Study (n 29) 39.
[105] See also Wagner (n 1) 53–62; EP JURI Study (n 29) 33–39.
[106] Resolution on Civil Liability (n 9) para 7.
[107] See also eg Omri Rachum-Twaig, 'Whose Robot is it Anyway? Liability for Artificial Intelligence-Based Robots' (SSRN 2019) 16–20, 24–27, 39–40 <https://ssrn.com/abstract=3339230> ; Caroline Cauffman, 'Robo-liability: The European Union in search of the best way to deal with liability for damage caused by artificial intelligence' (2018) 25 *Maastricht Journal of European and Comparative Law* 527, 528.
[108] See eg White Paper (n 6) 22. See also EP JURI Study (n 29) 33.
[109] See also eg Staff Working Document (n 5) 8–9, 12–14.
[110] See also eg Rachum-Twaig (n 107) 3–4, 11–19, 24–27.

Due to the complexity of the value chain, it can be challenging to identify 'a correct producer'. For example, the party that provided data or 'trained' an AI application may have alone committed an error which was the cause of an accident. Liability on the basis of extra-contractual damages liability is in principle possible in such situations,[111] but it might be nearly impossible to actually obtain reparation.[112] Especially if the person harmed is an end-user or an outsider, it would be difficult for them to prove that the cause of the damage was in fact the data that was used to train the AI application. What is more, as information asymmetry often exists between the harm-sufferer and the potential defendants, the former might be unable to point out the precise actor in the value chain that caused the damage. In all, although national laws likely allow claiming damages from the provider of data or the like, under national fault-based liability rules the burden of proof rests with the claimant and establishing liability is difficult.[113]

Liability of the operator or user signifies that the operator or the user of an AI application bears the costs of accidents that have occurred due to utilisation of AI.[114] Private users of robots or other AI devices may be held liable for negligent behaviour under general law on damages liability, for instance if they neglect safety measures or use devices like robots without reading the user manuals.[115] Users may also be liable when the cause of damage is software they installed after purchasing the product, or for modifications they made to original software.[116]

In any event, consumer-users and professional users may be considered to have different obligations, and what can be required from a consumer-user is generally less than in the case of a professional. Consumers are more likely to 'blindly' rely on the safety of a device that is sold to them.[117] However, consumers should not be exempt from the obligation to act with due care, for instance undertaking basic safety measures such as reading user manuals and installing security updates. Here, the question of whether a consumer should bear the cost of AI-related harm caused to themselves can be straightforward enough, but it may be more challenging to evaluate who bears the responsibility if, for example, family members or passers-by are harmed by an AI application operated by an allegedly negligent consumer.

The liability of professional operators can be justified by the argument that professionals should only use tools they can consider themselves responsible for. Here the inability to foresee some of the actions and decisions of AI might be seen as undermining that justification. Nonetheless, it could be submitted that the correct bearer of the risk of AI causing an accident is the professional operator who decided to utilise AI.

In this context, one can also consider the ongoing academic discussions in Austria[118] and Germany,[119] as well as on an international level,[120] regarding (analogous) application of

[111] See also eg Peggy Valcke, Aleksandra Kuczerawy and Pieter-Jan Ombelet, 'Supervising automated journalists in the newsroom: liability for algorithmically produced news stories' (2016) 61 *Revue de Droit des Technologies de l'Information* 5, 9–12, 15–17.
[112] See also eg Safety and Liability Report (n 3) 14.
[113] See also Safety and Liability Report (n 3) 14.
[114] See also eg Staff Working Document (n 5) 8–9, 19–21.
[115] Eg Spindler (n 2) 132.
[116] Eg Wagner (n 1) 50.
[117] See also eg Cauffman (n 107) 530.
[118] See eg Christoph Kronthaler 'Analoge Anwendung von § 1313 a ABGB auf technische Hilfsmittel?' [2019] *Österreichische Juristen Zeitung* 946, 947.
[119] See eg Michael Denga, 'Deliktische Haftung für Künstliche Intelligenz' (2018) 2 *Computer und Recht* 69 for German law.
[120] See eg Ugo Pagallo, *The Laws of Robots* (Springer 2013) 121.

vicarious liability rules. Arguments brought forward in favour of applying vicarious liability are often based on the *respondeat superior* principle in Anglo-American jurisdictions, but also on policy goals concerning providing for adequate compensation instead of imposing liability on a party who could not pay proper remuneration. In the case of employment relationships, the financially weaker party is the employee. If employers can be held liable for wrongful autonomous acts of their employees despite neither having proper influence on their behaviour nor participating in it, the user of an AI device could be similarly held liable.[121] Another argument is that that by employing technical tools, the principal saves money or earns more money. Thus, the principal should also bear the potential additional (accident) costs that relate to deciding not to perform some tasks themselves.[122]

(ii) Causation

Law on damages liability operates with the notion of causation. Within it are actually two matters: factual causation and legal causation.[123]

Factual causation is often explained by referring to the *conditio sine qua non* test, or the 'but for' test. Under this test, any condition without which damage would not have occurred is relevant.[124] Legal causation is used to limit the relevant causes in comparison to the *conditio sine qua non* test. Here, however, divergences can exist between EU Member States. While some Member States apply the *conditio sine qua non* test as the sole test, other approaches used are the theory of adequate causation or an open and flexible approach.[125] Adequate causation means that harm must be a direct and reasonably foreseeable outcome of behaviour. Member States applying a flexible approach include policy considerations or apply flexible criteria in terms of deciding which causes and instances of damage are connected to each other in a legally relevant manner.[126]

The traditional legal concept of causation is based on the assumption that one already knows who the wrongdoer is. In addition, legal rules are generally based on human conduct which cannot be compared to the 'behaviour' of AI systems.[127] Due to the opaqueness of AI and the multiple stakeholders involved, the actual cause or source of harm may not be directly evident. Accordingly, several policy papers by EU institutions mention that it may be difficult to prove the chain of causation, which might discourage individuals from filing a claim.[128] However, it has been noted that novel technologies also offer new opportunities to record and to monitor the system in operation, which might to some extent lessen the difficulty.[129]

When it comes to the adequacy test, the question is what exactly must be foreseeable, by whom, and when.[130] If foreseeability to humans is considered necessary in terms of establishing

[121] See also Pagallo (n 120) 131; Denga (n 119) 73.
[122] Kronthaler (n 118) 947.
[123] See eg Jaap Spier and Olav A Haazen, 'Comparative Conclusions on Causation', in Jaap Spier (ed), *Unification of Tort Law: Causation* (Kluwer Law International 2000) 127, 130.
[124] See eg Cees van Dam, *European Tort Law* (Oxford 2nd edition 2013), 121–122.
[125] See eg Spier and Haazen (n 123) 127, 130.
[126] Eg ibid 133, 134.
[127] Eg Bathaee (n 101) 891.
[128] See eg Safety and Liability Report (n 3) 14; EP JURI Study (n 29) 56.
[129] See for discussion eg Wagner (n 1) 46; the EP JURI Study proposes that a 'logging by design' requirement be established: EP JURI Study (n 29) 83.
[130] Eg Miquel Martín Casals, 'Causation and Scope of Liability in the Internet of Things (IoT)' in Lohsse et al (n 1) 221.

causation, understanding the decision-making process of an AI is crucial.[131] AI-driven systems apply a decision-making process that differs from that of humans as they do not suffer from the same cognitive limitations as the human brain; their computational capacity allows them to search through an uncountable number of possible solutions in a short time.[132] As these systems can learn and change their patterns and adapt to new conditions, it becomes ever harder to attribute their actions to producers or operators.[133] Consequently, human actors may try to argue that AI-related harm was genuinely unforeseeable to them. Nonetheless, as it is generally known that AI can make individual decisions that are not foreseeable to humans, the unpredictability of AI can itself be deemed foreseeable. Therefore, harm caused by AI could be considered recoverable without requiring foreseeability of a particular harm, especially if the type and nature of harm are such that it cannot be considered highly extraordinary in the relevant situation.

(iii) Fault

Fault comprises intention and negligence. The wrongdoer is at fault if they commit an act or omission they should not have committed and can therefore be held (morally) accountable for the consequences. In practice, to establish negligence, courts tend to apply the average reasonable person or a similar notion as a reference standard.[134] With regard to AI-related cases, fault is easy to establish when damage has been caused by an event such as a cyber-attack, as this will always amount to intentional and thus faulty conduct, usually that of a third party.[135] However, where no clear intervening 'human-wrongdoer' is identifiable, the notion of fault becomes difficult to apply to cases involving AI. The impossibility of foreseeing some of the accidents caused by AI further complicates the issue, as the notion of fault can be understood as referring to a failure to prevent foreseeable harm.

The ability to trace harm back to human behaviour is generally needed to apply traditional national fault-based liability rules.[136] However, AI applications can be opaque even to their programmers. It can be impossible to tell how their decision-making process works or what exactly led the AI system to make a specific decision. A further issue is when should *absence* of fault be found when someone has relied on the use of AI;[137] that is, when does relying on an AI application exonerate a human or when does it not?

In terms of preliminary plans for future law, it can be noted that the Commission proposes establishing clear cybersecurity obligations in future legislation.[138] One could even more broadly consider technical standards to determine negligence,[139] signifying that failure to comply with an applicable standard would constitute fault. Commentators suggest a reasonable producer or developer in the same situation as a benchmark for cases of negligent harmful programming or similar actions. Moreover, if a system's self-learning is influenced by persons other than the developer or producer, then those persons could be liable.[140] A further possibility is to not take foreseeability into account, but to consider only the social and practical outcomes.

[131] Bathaee (n 101) 892.
[132] Eg Martín Casals (n 130) 222.
[133] See also eg Spindler (n 2) 126–127.
[134] See also van Dam (n 124) 225–278.
[135] See also Resolution on Civil Liability (n 9) para 9.
[136] See also Safety and Liability Report (n 3) 13.
[137] See also ibid 15.
[138] See ibid 15.
[139] Spindler (n 2) 130.
[140] Eg Cauffman (n 107) 529–530.

(iv) Further questions

When addressing liability for AI-related damage, the issue of legally protected interests and traditional approaches to compensating certain types of harm could constitute a problem. When AI is involved, the harm inflicted will often be pure economic loss or non-tangible loss such as privacy infringements. In many Member States, compensation is not easily awarded for these, or only limited compensation is available. There can also be significant divergences in terms of the amount of compensation for non-material harm.

In any case, one must bear in mind that if a violated interest is protected by EU law, that is, if harm has been caused by infringing EU law, there is in any event an obligation for the Member States to apply liability rules so as to ensure that even pure economic loss can be fully compensated.[141] Additionally, non-material harm is recoverable under EU law. The recoverability of non-material harm has been explicitly stated in certain pieces of secondary legislation that can be relevant for cases involving AI-related harm, such as the above-discussed GDPR.[142] It is also possible that national courts are obliged by EU law to ensure recoverability of non-material harm in EU law-related cases even in the absence of particular legislation expressly addressing recoverability of intangible losses.[143]

For these reasons, the issue of types of harm inflicted in AI-related cases is not that significant a problem in the EU as would seem at first sight. However, provisions of any novel EU legislation on AI-related harm should be formulated in a manner that reiterates and further clarifies these issues.

(v) Substantive questions: interim conclusions

The brief review above indicates that applying existing (national) liability rules to cases involving AI-related harm may be challenging for courts. From the standpoint of harm-sufferers and potential defendants, case outcomes can be unpredictable. In some situations, those harmed by AI may lack protection. These remarks apply, in particular, to cases where a human or organisation that 'caused' harm is difficult to identify and AI has acted as the 'main wrongdoer'. It seems that in many situations harm-sufferers may lack the necessary information and expertise to prove all the conditions for liability where these are for the claimant to prove (as is usually the case under general damages liability law). In terms of fault and causation in particular, it can also be ambiguous what exactly the claimant should prove in order to be awarded compensation. Discussions related to clarifying legal approaches to harm caused by AI are ongoing at both EU and national level.

B. The way forward in the EU? – Selected notes

[141] See eg Case C-470/03 *A.G.M.-COS.MET*, ECLI:EU:C:2007:213; Joined Cases C-46/93 and C-48/93 *Brasserie du Pêcheur*, ECLI:EU:C:1996:79.
[142] Art 82(1) GDPR.
[143] See for detailed discussion Katri Havu, 'Damages Liability for Non-material Harm in EU Case Law' (2019) 44(4) *European Law Review* 492.

Above, we have described preliminary plans for EU legislation and covered some developments at the Member State level. We also delved into challenges related to liability considerations in terms of AI-related harm. The question of what the European legal landscape will actually look like in the future remains to some extent open, but certain selected remarks can be made on the desirability of amendments to existing EU legislation and the adequacy of the proposals presented.

(i) Particular legislation: current issues and challenges for the future

Product liability

As we have seen above, the EU legislators have expressed willingness to revise the EU product liability framework.[144] Several remarks can be made about the shortcomings of the current PLD and as regards themes to be considered while revising product liability rules.

One important question is whether data, particularly when supplied as stand-alone software, falls within the scope of *products*. The fact that electricity is explicitly mentioned in the PLD as the only non-tangible is often used as an argument to exclude other non-tangible items.[145] Currently, the question also arises as to whether software is classified as a product or a service. While essential software components are more likely to be considered integral parts of a product, this may not necessarily be the case for stand-alone applications.[146]

The Commission proposes that the definition of product be further clarified to take into account the complexity of emerging technologies and to ensure that damage caused by products that are defective due to digital features can be compensated.[147] This would make it easier for entrepreneurs such as software developers to assess if they would be considered as producers within the meaning of product liability rules. The Commission further states that software stored on devices such as DVDs or flash drives should be considered a product.[148] Be that as it may, nowadays software is often provided as a download, thus an intangible good and not in the purview of the Directive. It has been argued, however, that one could consider the physical manifestation of a program on the host mainframe as a product, supplied when a copy is transmitted over the Internet.[149]

The EP JURI Study also criticises lack of clarity in terms of whether software is to be classified as a product as new technologies often consist of interdependent hardware and software components.[150]

Here one can note that it is hardly justifiable to treat software differently based solely on its medium of distribution or storage. In terms of the definition of 'product' for the purposes of product liability rules, this could be solved by adopting a very broad notion of 'movable',

[144] See sections II–III above.
[145] Daily Wuyts, 'The Product Liability Directive – More than two Decades of Defective Products in Europe' (2014) 5 *Journal of European Tort Law* 4–5.
[146] See also Safety and Liability Report (n 3) 14.
[147] European Commission, 'Evaluation of Council Directive 85/374/EEC' (Working document) (2020) 23–24; Safety and Liability Report (n 3) 13.
[148] Safety and Liability Report (n 3) 14.
[149] Wuyts (n 145) 6.
[150] EP JURI Study (n 29) 57.

meaning anything that is not real estate or a service. All 'movables' would constitute 'products'.[151] However, this approach might not help if software could still be classified as a service. Another option is to adopt an interpretation according to which the existing PLD provision on products does not exclude non-tangible items (although this might be slightly far-fetched).[152] One could draw the line between products and services by deciding that customised programmes produced for an individual or a limited group of persons are considered services, while broadly available mass-produced programmes are considered products.

All in all, both academics and EU institutions recognise that product liability rules could be applied to software and that applicability to software is desirable in the future. For the sake of legal certainty, applicability to software should be set out clearly in future rules.

In the case of custom-made AI solutions sold as a *service*, the current PLD is not applicable. However, this does not necessarily mean that the provider or operator will not incur liability. The operator can be held liable according to national fault-based liability rules if they acted intentionally or negligently while using the application. Additionally, pursuant to the Draft Regulation published by the EP, the operator of an AI application could incur fault-based liability to the harm-sufferer.[153] Furthermore, the producer can be liable (contractual liability) to the person who purchased the AI system. Moreover, the producer or service provider may be liable in extra-contractual liability towards harm-sufferers.

Because contractual liability and general extra-contractual liability rules in any event provide remedies to harm-sufferers and other cost-bearers, services could possibly remain excluded from the scope of EU product liability legislation. However, it must be carefully considered whether the other remedies are sufficiently efficient and whether general liability rules should in any event be modified by new EU law.

Defectiveness of AI raises many theoretical and practical questions. If a software program has incorrect code lines or is exceptionally vulnerable to cyber-attacks, it does not provide the safety that a user is entitled to expect and can be considered defective. The same would apply to problems related to insufficient information or warnings provided. However, it will not always be obvious that there is a design defect or warning defect.[154] Further, harm can occur, for example, because the conditions (environment) surrounding the AI application changed and the application did not adapt its actions to this change. Here, the question is whether the variation of the surrounding conditions should have been taken into account by the producer. If yes, the product was defective already when put into circulation.

To establish a defect in traditional products, courts often utilise indicators such as malfunction, violation of safety standards, balancing risks and benefits of a product, or comparison with similar products. In the case of AI applications, the suspected defect can be that an algorithm has been defectively designed, which leads to the question how this can be verified. Traditionally, a starting point is *res ipsa loquitur*: a product that is malfunctioning while being used reasonably and correctly is probably defective. Even so, this test is inefficient if the

[151] See also Wagner (n 1) 42.
[152] See eg Bernhard A Koch, 'Product Liability 2.0 – Mere Update or New Version?' in Lohsse et al (n 1) 105, 106; Wagner (n 1) 42.
[153] See Resolution on Civil Liability (n 9), Art 8 of the Draft Regulation.
[154] See also Jean-Sébastien Borghetti, 'How Can Artificial Intelligence be Defective?' in Lohsse et al (n 1) 66.

malfunction is not obvious.[155] Another option to determine defectiveness would be (at least in theory) to compare the outcomes of two or more algorithms applied to solve the same problem.

An additional solution that has been proposed is to establish harmonised technical standards. Deviation from these would indicate defectiveness.[156] Yet it seems hardly feasible to develop harmonised standards for algorithms as these are usually tailored to different types of products, and different manufacturers might program algorithms in different ways. These reasons make it difficult to draft any kinds of common and generally applicable 'rules'. Strict technical standards could also deter innovation.

Another issue is that under the current PLD (Article 6), a product must be defective when put into circulation, meaning that the focus is on the moment the product is placed on the market.[157] Thus, defects caused by maintenance or updates are not covered by the Directive. AI systems may be updated multiple times and undergo significant changes in the course of their life cycle. They depend, for example, on internet connectivity for proper functioning, which creates additional system risks. Moreover, the user can – knowingly or not – contribute to increasing risks by making mistakes while installing or utilising software, refusing or forgetting to install necessary security updates or, for instance, by choosing unsafe passwords.[158] Fortunately, the Commission recognises that modifications to functions of AI systems during their life cycle due to software updates or machine learning should be addressed in future legislation.[159] A first step in this direction has been taken with the Draft AI Act. With the rules on post market monitoring included in the Draft AI Act, the Commission takes a holistic approach aiming to cover the entire life cycle of an AI system.[160] To avoid future fragmentation, it will be crucial to align AI legislation and product liability as well as product safety legislation in this regard.

An additional issue is that under the current PLD, the producer is not liable if they establish that the state of scientific and technical knowledge at the time when they put the product into circulation was not such as to enable the existence of the defect to be discovered (Article 7, the so-called 'development risk defense'). In certain Member States, also stricter rules concerning this matter have been adopted, as allowed by the Directive. Also, the implementation of the exemption itself has been divergent.[161] Therefore, the availability of this defense is not uniform across the Union. When revising the product liability rules, it should be considered whether an exemption such as this – potentially highly relevant in the context of rapidly developing technologies – is desirable, and whether this question should in any event be fully harmonised.

A further matter is *the scope of legally relevant damage*. In terms of items harmed, whether damage to data falls within the scope of the PLD or whether 'items of property' only covers tangibles is currently ambiguous.[162] This is also critically discussed in the EP JURI Study in relation to the fact that privacy and cybersecurity issues are not addressed at all in the PLD.[163] Currently, it appears to be up to the Member States to decide whether data qualifies as property

[155] Ibid 67.
[156] See Cristina Amato, 'Product Liability and Product Security: Present and Future' in Lohsse et al (n 1) 93–94.
[157] See also Wuyts (n 145) 21.
[158] See also eg Spindler (n 2) 128.
[159] White Paper (n 6) 14.
[160] Recital 72, Articles 53–55 of the Draft AI Act; see also above Section II.A.iii.
[161] See the preamble of the PLD; Case C-300/95 *Commission v United Kingdom*, ECLI:EU:C:1997:255, and for discussion eg Marcus J. Pilgerstorfer, *European Product Liability, A Comparative Study of "Development Risks" in English and German Law* (University of Manchester 2019) 30–32.
[162] See eg Koch (n 152) 103.
[163] EP JURI Study (n 29) 59.

or not.[164] Additionally, the fact that Member States may currently apply additional national rules for compensating non-material harm[165] is likely to lead to different case outcomes across the EU. To ensure similar case outcomes, damage to data, and possibly even compensation for non-material harm, should be clearly addressed under a future liability framework.

Under the current Article 4 of the PLD, the consumer shoulders the *burden of proof* in regard to showing that a product is defective and the existence of a causal link between the defect and the damage. It has been pointed out that automated systems usually store data that can be relevant for claimants – the Commission specifically notes that modern systems usually have logging possibilities.[166] Whether and to what extent a harm-sufferer has access to this data largely depends on storage location. The chances for the harm-sufferer to use the information will be smaller if it is stored in a cloud or in another location controlled by the defendant. Even if harm-sufferers are in theory able to obtain some of the relevant data, their lack of expertise and the complexity of AI systems might still render showing causation and defect nearly impossible.[167]

In this context, one can ask whether and to what extent the burden of proof should be reversed or alleviated. Another option to facilitate access to information for the harm-sufferer is to oblige the producer to grant access to the relevant data. In terms of contemporary EU law, even the introduction of limited and field-specific 'discovery rules' is not unheard of.[168] It appears that AI-related harm is an area where a broad range of options should be considered for making claims less hindered by inability to access evidence.

A further issue to consider is the difference between *open and closed systems* and whether different rules should apply to different systems.[169] In closed systems, all the components come from one provider who is in control of the characteristics of the entire system and can therefore be considered responsible for any harm caused. By way of contrast, open systems – where hardware and software components are purchased from different parties – involve multiple 'producers' and make it difficult for a harm-sufferer to prove who is responsible for defects. Operators or users usually choose component providers but may lack the expertise to pinpoint the exact cause of harm if an accident occurs. This could be resolved by obliging component providers to grant access to the necessary data as well as by reversing or at least alleviating the burden of proof.[170] This issue of open and closed systems is relevant even beyond product liability.

A broader issue to note is that the effects of product liability constitute an intricate matter if one observes the effects from the standpoints of product safety and *innovativeness* of products. While greater product liability can increase product safety, it can either increase or decrease product novelty, which signifies that greater product liability may eventually decrease

[164] See Art 9 of the PLD and eg EP JURI Study (n 29) 59.
[165] See PLD, Rec 9 and Art 9.
[166] Safety and Liability Report (n 3) 3.
[167] For discussion see also eg Roeland de Bruin, 'Autonomous Intelligent Cars on the European Intersection of Liability and Privacy' (2016) *European Journal of Risk Regulation* 485, 491–492, 500.
[168] See Directive 2014/104/EU on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union [2014] OJ L 349/1.
[169] See eg Wagner (n 1) 48.
[170] See also eg Wagner (n 1) 49.

consumer welfare and total welfare.[171] This further complicates revision of product liability rules or drafting a well-functioning product liability regime. Any amendments to product liability rules should involve exercise of caution.

In addition, it should not be forgotten that liability rules do not operate in a vacuum. Some risks are better tackled by product safety law and even recommendations and self-regulation, which can prevent accidents ex ante. In particular, lesser risks, that is, damage that is not very serious, can well be addressed by ex-ante mechanisms while liability rules only provide 'a final safeguard'. Product safety law as well as soft law and self-regulation can also be central in increasing consumer trust and adoption of technologies by the general public.[172] Careful consideration must be given to assessing the optimal roles for different kinds of rules and modes of regulation in the context of AI-related risks. Hard law liability rules and the incentives they put in place can also contribute to the creation of beneficial self-regulation. This is important to bear in mind in planning novel product liability rules but applies to other liability legislation as well.

Other particular legislation and the bigger picture

Existing EU level policy papers indicate that AI-related harm will be addressed by different kinds of pieces of legislation even in the future. The fields covered above evidence that AI-related harm may already be covered 'like any other harm' by field-specific rules; indeed, relying on AI as a tool does not have to change the liability of humans or organisations from the liability they would otherwise incur. In some cases, the involvement of AI might not cause additional problems in applying field-specific rules. However, applying rules to certain situations involving, for instance, highly independent and opaque AI applications, can constitute a challenge, at least until a sufficient amount of case law addressing AI-related harm is available. Difficulties in evaluating, for example, causation and fault or what counts as exonerating circumstances can be present in applying a liability rule found in particular legislation as well as in applying general law on damages liability. The Commission has correctly identified issues like these as areas where additional legislation and clarifications may be needed.[173]

It seems likely that future pieces of particular legislation will, to some extent, better take into account harm caused by AI. Some relatively recent pieces of legislation have already been drafted that carefully observe potential challenges posed by new technologies.[174]

However, even the field-specific rules currently in force rely on complementing national law in terms of details of liability. Therefore, albeit particular EU rules apply to certain situations involving AI-related harm, liability is not necessarily similar across the Union. This applies, for example, to claims related to the GDPR. If, in the future, national laws retain a significant role in areas where particular legislation is in place, enacting 'general EU level liability rules' on AI-related harm will not harmonise liability for all kinds of situations and fields.

---

[171] See eg Ping Lin and Tianle Zhang, 'Product Liability, Multidimensional RD and Innovation' MPRA Paper No. 97078 (Munich Personal RePEc Archive 2019) <https://mpra.ub.uni-muenchen.de/97078/>. See also on the implications of liability rules with a view to different policy goals concerning AI eg de Bruin (n 167) 490, 500–501.

[172] See also eg White Paper (n 6) 24.

[173] Eg White Paper (n 6) 13–15.

[174] In terms of existing, recently drafted legislation see the GDPR, Recs 6, 58. See also, in terms of product safety legislation, Safety and Liability Report (n 3) 10–11.

Whether the bigger picture of liability rules – where sector-specific pieces of EU law retain a significant role, 'general AI liability law' is potentially issued, and national rules on liability are in any event needed to complement the EU rules – will be too complex is a valid question. However, the bigger picture of law on damages liability in the EU has been somewhat intricate for a long time, and what will potentially be added soon in terms of 'general AI liability EU law' is not necessarily overtly dramatic from the standpoint of clarity of the overall legal landscape. Additionally, national courts applying EU law to cases before them should in any event request preliminary rulings from the CJEU if facing true lack of legal clarity.[175]

(ii) What role for national laws on damages liability?

The question whether national liability rules would suffice to address AI-related harm in the EU encompasses two themes: first, whether the substance of existing national liability rules is inadequate; and secondly, whether rules and case outcomes in any event should be made more uniform across the Union to avoid fragmentation within the Single Market.

From the standpoint of substantive liability questions, existing national liability rules would likely yield predictable outcomes in situations where the role of AI is minor in the events that constitute the facts of a case, and the issue of how to correctly apply, in particular, the conditions of causation and fault is not much different from situations not involving AI. Existing national damages liability laws may be sufficient, for example, in cases where a third party (neither anyone participating in the supply chain nor anyone associated with the user of an AI system) intervenes. In these cases, the characteristics of AI systems play only a minor role and the intervening third party, such as someone making a cyber-attack, is liable for any harm caused. Even in other situations where identifying persons that caused harm is not made excessively difficult by the involvement of AI, national laws would likely suffice to resolve cases. In areas like these, case outcomes might not necessarily be identical in every Member State. Nonetheless, they could, in each Member State and in any event, be sufficiently predictable and reasonable in the light of the law of the Member State in question.

It can be asked whether a 'damages liability law substance' analysis already indicates that new (EU) rules would be needed, for instance, in terms of facilitating claims against parties that are 'remote' from eventual harm, such as providers of data who did not take part in 'producing' the AI application in any other manner than providing, for example, picture material that was then utilised in training the AI to recognise a pedestrian. As also discussed above, national damages liability laws likely allow extra-contractual claims directed at, for example, a data provider.[176]

Nonetheless, the theoretical possibility of a damages claim such as this is often not enough in order to actually obtain compensation if, for example, the harm-sufferer is an outsider harmed by an intelligent bike operated by a consumer end-user. Proving the claim is nearly impossible unless the information asymmetry between the claimant and the defendant is alleviated. What is more, without information that is possessed by actors such as the data-provider and the actual manufacturer of the bike, the harm-sufferer is not likely to know whose mistake caused the harm. In considering whether new (EU) rules would be needed, it must be assessed whether a

[175] See Art 267 TFEU.

[176] See also eg Valcke, Kuczerawy and Ombelet (n 111) 9–12, 15–17 (about Belgian law); Katri Havu and Waltter Roslin, 'Tekoäly ja vahingonkorvausvastuu media- ja viestintäalalla: teoreettisia lähtökohtia ja valikoituja havaintoja' (2019) (7–8) *Lakimies* 896, 914, 923 (about Finnish law).

claim against data providers and similar 'remote' defendants is a type of claim that should be facilitated, considering aspects of fairness, efficiency or societal welfare. (Directing a claim against a different party who then could direct a regress claim towards, for example, a data provider could adequately resolve the situation as well.)

More broadly, the issue of complex ecosystems and multiple actors, and related difficulties in identifying the correct defendants and obtaining sufficient information about how the harm was actually caused, might justify alterations in the burden of proof regarding, for example, causation. Therefore, even if liability for AI-related harm would to some extent be left to be resolved under national laws, harmonising legislation that addressed the burden of proof could be justified.[177] A counterargument for alleviating the burden of proof is the risk of excessive or abusive litigation, as well as the possible outcome where claimants start addressing claims against all possible defendants who are then all using resources in litigation (whereas only one of them is the true cause of harm).

For instance the Parliamentary Resolution of 2020 discusses questions of damages liability substance and the adequacy of existing (national) laws as well as the goal of making the law more *uniform* in the EU.[178] Additionally, Commission documents illustrate the importance of both goals: addressing AI-related harm sufficiently clearly in terms of the substance of the law as well as ensuring that case outcomes are to a certain extent similar across the Member States (level playing field).[179] However, some vagueness is present in official documents in terms of exactly what harmonising measures are considered necessary. Moreover, EU bodies highlight problems such as claimants' difficulty in showing causation, which are nevertheless not fully addressed by means of proposing comprehensive rules that would exhaustively resolve these issues.[180] Therefore, the question of what kind of role national laws will play in the future remains partially open.

National rules on damages liability will in any event complement EU rules, for instance, rules of sector-specific legislation where EU law does not include rules on details of damages liability. National laws might need to be interpreted in a certain manner in EU law-related cases in order to comply with the principles of EU law and with the obligation to offer efficient and adequate judicial protection.[181] Additionally, if potential future harmonisation of more general liability rules applicable to AI is not perfect, that is, if gaps occur in harmonising EU legislation (intentionally or not), national laws play a role in filling those gaps.[182] If there are pieces of national particular legislation,[183] they will apply to AI-related harm as long as they are not in contradiction with any EU law. Due to the primacy of EU law, EU law takes precedence over conflicting national rules.

(iii) Recent proposals for EU legislation and further comments regarding harmonisation

[177] See also eg Safety and Liability Report (n 3) 14.
[178] Resolution on Civil Liability (n 9) eg lit. H, lit. I, paras 6, 9, Rec 8 of the Draft Regulation.
[179] Eg White Paper (n 6) 14; Safety and Liability Report (n 3) 5–7, 9.
[180] Eg Safety and Liability Report (n 3) 14. The Parliamentary Resolution of 2020 in particular will be further discussed in the section below.
[181] See eg Case C-432/05 *Unibet*, ECLI:EU:C:2007:163; Case 33/76 *Rewe-Zentralfinanz eG and Rewe-Zentral AG Saarland*, ECLI:EU:C:1976:188; Case 106/77 *Simmenthal*, ECLI:EU:C:1978:49 paras 17–24.
[182] This can happen even though the national courts have the possibility, and last instance courts the obligation, to request preliminary rulings from the CJEU in case of ambiguity of EU law (Art 267 TFEU).
[183] See section IV.

The Parliamentary Resolution of 2020 proposes adopting an EU regulation concerning 'liability for the operation of artificial intelligence-systems'.[184] The novel rules would be in force in parallel with particular legislation such as that on product liability.[185] The EP underlines that the new common rules for AI systems should only take the form of a regulation.[186] The choice of the form of regulation – that is, directly applied in its entirety across the Union – is wise since less divergence will occur between Member States from the outset. Nonetheless, even regulations can be interpreted incorrectly by Member State courts. Moreover, any gaps or ambiguities in the text of the final regulation might cause further divergences as national laws and traditions are used, consciously or not, to fill in said gaps. As is evident from our discussion below, the Draft Regulation presented by the EP includes both matters that are consciously left for national laws of Member States as well as (presumably) unintentional incompleteness or ambiguity in some places.

High-risk and low-risk systems

In the EP Draft Regulation, the significance of whether an application is classified as high-risk or not is notable: the classification dictates whether strict or fault-based liability applies.[187] The policy goal of safely introducing AI applications to markets and to the general public, and the aim of gaining acceptance by the general public in terms of beneficial AI innovations, are clearly the background for proposing tighter liability rules for particularly risky AI applications.[188] 'Strong' liability rules and the related perception of safety contribute to acceptance of new technologies by the general public.

In the EP draft, high-risk systems are defined as systems whose autonomous operation involves 'significant potential to cause harm to one or more persons, in a manner that is random and goes beyond what can reasonably be expected'. The sector in which the system is used and the activities undertaken must be considered when assessing risk potential. The assessment must consider the severity of the possible harm and the probability of the risk materialising.[189] The definition utilises the criteria provided in the White Paper.[190] In any event, the definition of 'high-risk' differs from the one used in the EP resolution for a framework on ethical aspects.[191] In the latter, AI applications are considered high-risk 'when their development, deployment and use entail a significant risk of causing injury or harm to individuals or society, in breach of fundamental rights and safety rules as laid down in Union law'.[192] While expressions such as 'random' or 'beyond what can reasonably be expected' are broad and will need to be interpreted by courts on a case-by-case basis, the reference to a breach of fundamental rights and safety rules appears to be the other extreme, an extremely tight frame.

---

[184] Resolution on Civil Liability (n 9) Annex to the Resolution.
[185] Ibid, see para 8; Rec 10 and Art 11 of the Draft Regulation.
[186] Ibid Introduction para 5.
[187] Ibid para 14, Art 4 of the Draft Regulation.
[188] See also eg EP, 'Parliament leads the way on first set of EU rules for artificial intelligence' (Press release, 20.10.2020) <https://www.europarl.europa.eu/news/en/press-room/20201016IPR89544/parliament-leads-the-way-on-first-set-of-eu-rules-for-artificial-intelligence>; White Paper (n 6) 9–10.
[189] Resolution on Civil Liability (n 9) para 15.
[190] White Paper (n 6) 17; see also section II.A. above.
[191] EP, 'Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies' 2020/2012 (INL) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html>.
[192] Ibid para 14, Rec 11 of the proposed regulation on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies.

If the EU institutions envision coherent legislation concerning AI, then use of consistent definitions is crucial. Presenting different definitions of the same term in different resolutions is counterproductive to the goal of avoiding fragmentation across the EU and might lead to divergences in interpretation by national courts. The need for clarity in terms of defining this central notion has been previously underlined by the Commission according to which 'the determination of what is a high-risk application should be clear and easily understandable and applicable for all parties concerned'.[193] The definition of high-risk applications presented in the Resolution on Civil Liability is rather broad, but it should be noted here that the notion must leave enough room to accommodate future technical developments so that legislation will not have to be revised very often.

Following ideas presented in previous policy papers, the EP proposes in its Resolution that high-risk AI systems and the sectors where they are used be exhaustively listed in an annex to the future regulation (Article 4(2) of the Draft Regulation). Such a list can provide producers and operators with legal certainty while also preventing diverging interpretations by Member State courts. At the same time, one may ask whether an exhaustive list is likely to jeopardise the intention of creating a future-proof piece of legislation. Although the proposed list is recommended for review at least every six months, periods of insecurity can hardly be avoided for producers and operators as to whether an assessment of high-risk or low-risk will change. Additionally, if a general definition is actually superfluous and systems considered high-risk are narrowed down to the items listed in an annex, this eliminates any flexibility. In any event, in its recent Draft AI Act, the Commission chose to include an exhaustive list of high-risk AI systems[194] instead of an 'umbrella-like' general definition. As final liability rules have not been enacted, future solutions in terms of liability and high-risk AI remain open. Nonetheless, the idea put forward by the Parliamentary Resolution, that is, using both a very general notion of high-risk systems and simultaneously an exhaustive list of such systems does not appear recommendable because such a solution would endanger both flexibility and legal certainty.

A further matter is whether it is appropriate to use the distinction between high-risk and low-risk as the only criterion in determining whether or not an operator is strictly liable for harm inflicted. High-risk systems will not be the only ones that can cause harm. A person suffering severe harm from an AI system not considered high-risk might be at a significant disadvantage in obtaining compensation compared to someone harmed by a high-risk AI application. This might not seem fair. The Commission correctly notes that identification of high-risk AI can play a central role in making sure that regulatory intervention is 'proportionate',[195] but it should be borne in mind that the distinction between high-risk and low-risk AI applications should not mean that harm caused by low-risk AI remains a significant problem from the standpoint of individuals' possibilities to obtain compensation.

<u>High-risk applications and strict operator liability</u>

The Draft Regulation presented by the EP would make the *operators* of high-risk AI strictly liable for any resulting harm.[196] This choice of operator liability as opposed to 'manufacturer' or 'producer' liability has the benefit of usually easy identification of the relevant person. The

[193] White Paper (n 6) 17.
[194] Draft AI Act (n 10), Article 6 and Annex III to the draft regulation.
[195] White Paper (n 6) 17–18.
[196] Resolution on Civil Liability (n 9) Draft Regulation, Art 4.

operator is more easily visible to outsiders or, for example, to those who purchase a service performed utilising AI in the process. Additionally, severe operator liability as opposed to severe manufacturer liability is a reasonable choice because, as we have noted above, manufacturer liability for AI-related harm could be criticised for placing the liability burden on an actor that might not be well-placed to prevent accidents or take precautions.[197]

Nonetheless, strict liability is always a powerful incentive or disincentive,[198] and even strict operator liability could deter adoption of new technologies that would ultimately be beneficial for society as a whole. Notably, when AI is safer than a human in a given task, it is beneficial that humans are replaced by AI. In terms of whether future legislation manages to strike a suitable balance, much depends on how the definition of high-risk applications is worded in the final rules and whether the term high-risk will be interpreted broadly or narrowly. Where AI is truly high-risk, that is, objectively dangerous and accident-prone, strict operator liability would in any event be in line with how European legal orders have traditionally utilised strict liability: in contexts where an activity is inherently remarkably dangerous, (the interests likely harmed are human life and health,) and the person or organisation carrying out the activity has a good deal of information on how best to avoid accidents and has a good chance of preventing accidents.[199]

Other operator liability

Under the Draft Regulation presented by the EP, operators of other than high-risk AI would face fault-based liability for harm caused.[200] In this context, the operator is defined as the person exercising a degree of control over a risk connected with the operation and functioning of an AI system.[201] Frontend and backend operators are distinguished from each other. A frontend operator is defined as the person exercising a degree of control over risk related to the operating and functioning of an AI system and benefiting from its operation. A backend operator is a person defining the features of the technology, providing data and support and also exercising a certain degree of control.[202] Both are potentially liable.

The operator as the liable party – as opposed, for example, to the 'manufacturer' of the AI application – can be considered a reasonable choice in the context of this fault-based liability as well. In general, fault-based liability for harm caused by AI could signify that claims were successful in some cases only, due partly to information asymmetries. According to the legislative proposal, the operator is not liable if they prove that they were not at fault, provided the system was operated without their knowledge despite their having taken all necessary measures to avoid this or that they observed all due diligence in selecting, monitoring, operating and maintaining the system (Article 8(2) of the Draft Regulation). This is to be understood as a reversed burden of proof, which is appropriate to address the information asymmetry existing between the operator and the harm-sufferer. To avoid confusion and diverging interpretations by national courts it would be desirable to mention explicitly in the final legislative text that a reversed burden of proof is envisioned.

[197] See section V.A(i) above.
[198] See also eg Robert Cooter and Thomas S Ulen, *Law And Economics* (6th ed, Pearson 2016) 201–217;
Richard Posner and William Landes, 'The Positive Economic Theory of Tort Law' (1980) 15 *Georgia Law Review* 851.
[199] See eg Walter Van Gerven, Jeremy Lever and Pierre Larouche, *Cases, Materials and Text on National, Supranational and International Tort Law* (Hart Publishing 2000) 537–598.
[200] Resolution on Civil Liability (n 9) Draft Regulation, Art 8.
[201] Ibid, see Rec 10 of the Draft Regulation.
[202] Ibid para 12.

Furthermore, it should be noted that national courts might apply the proposed legislation so that case outcomes are divergent if it is not clearly indicated in the final legislative text what exactly amounts to proving not being at fault. If the final legislation does not set out criteria for establishing matters such as this, the possibility of fragmentation remains. This kind of risk, namely of varying case outcomes because of differences in standards of proof or assessing evidence, is not uncommon under existing EU law such as the PLD, either. However, it is also true that absolute harmonisation is highly challenging to achieve, and some variation in applying the law must just be accepted.

Coherence with product liability and product safety law

The coherence of any future liability regulation with EU product safety and product liability law must also be carefully considered. Notably, existing law on product safety places the responsibility for final product safety on the *producer*.[203] If the product does not provide the safety the user is entitled to expect, the producer will be liable under the PLD or national damages liability law. In essence, existing product safety and product liability regimes emphasise the responsibility and private law liability of the producer, while the text of the Draft Regulation on AI-related harm places the operator of an AI application as the main responsible party. To some extent, the text of the Draft Regulation leaves coordination with EU product safety legislation open, and it appears that without further attention to this issue the entirety of the applicable law could be rather complex.

In any event, Recital 23 of the Draft Regulation underlines the importance of close coordination between the new instrument and future product liability rules. The Parliamentary Resolution also recommends that in the future EU product liability rules should include backend operators in the concept of 'producers'.[204] It is important to clearly determine when a backend operator is to be treated as a producer and when they are to be considered an operator. Not only will this decide which framework is applicable, but it will also determine whether they will be subject to strict liability or to fault liability (in the case of low-risk items).

Relevant harm

According to the Draft Regulation presented by the EP, strict liability of the operator would cover 'any harm or damage that was caused by a physical or virtual activity, device or process driven by the AI system in question' (Article 4(1)). Additionally, the proposed text sets out some maximum amounts of compensation and further details concerning, for example, compensation for death or injury.[205] Interestingly, the Draft Regulation also includes a passage stating that the operator of high-risk AI would also compensate 'up to a maximum amount of EUR one million in the event of significant immaterial harm that results in a verifiable economic loss' (Article 5(1)(b)). The relationship between this statement and the more general clause on recoverable harm in Article 4 is not entirely clear. If liability is meant to cover any type of harm, what does it mean that immaterial harm must result in 'a verifiable economic loss'?

[203] See in detail Safety and Liability Report (n 3) 10–11.
[204] Resolution on Civil Liability (n 9) para 8.
[205] Ibid, see Arts 5–6.

In the process leading to the Parliamentary Resolution, EU bodies have highlighted the danger that AI could present for significant immaterial interests such as human dignity and European values, and that utilisation of AI systems may increase discrimination.[206] Against this background, to only grant compensation when the harm-sufferer can prove actual economic loss appears contra-intuitive, to say the least. Notably, under existing EU law, compensation for immaterial or non-material harm is not understood as compensation for economic losses but for non-material harm 'itself'.[207] Non-material harm includes, for instance, different types of mental suffering, or, in the case of legal entities, a state of uncertainty. The 'borderline' between non-material harm and economic harm under EU law is not as clear as it maybe should be,[208] but the text of the Draft Regulation appears particularly problematic. It is challenging to deduce what exactly is recoverable immaterial harm under the rules proposed by the EP.[209]

The notions of harm and causation

From a broader perspective, it should be noted that how the notions of harm and causation are understood and applied to facts is strongly decisive in terms of case outcomes. In many contexts, EU law only provides relatively vague – if any – definitions of these conditions for liability, thereby leaving national courts, in practice, a good deal of room for manoeuvre when deciding cases.[210] This is something that is visible, for instance, in the context of Member State liability[211] and even in areas where secondary legislation is in force.[212] The issue is that, if what is needed in order to establish causation and harm, or to show the quantum of the harm, is ambiguous in light of EU law, then there is no level playing field – or even predictable law on damages liability.

In the Parliamentary Resolution, the notions 'harm' and 'causation' are not defined in a clear and detailed manner. In particular, references to causation are vague.[213] In terms of harm to be covered, the Draft Regulation, for example, sets out maximum amounts for damages for different types of harm, but the proposed legislation is, as noted above, partially unclear and even contradictory as to what amounts to legally relevant harm.[214] Moreover, Article 9 expressly leaves a significant role for Member State laws in terms of the extent of harm and

[206] See eg White Paper (n 6) 10–12; Resolution on Civil Liability (n 9) Rec 3 of the Draft Regulation. See also, in terms of the concerns presented by the general public, European Commission, 'Summary Report on the open public consultation on the White Paper on Artificial Intelligence' (2020) 3.
[207] See eg Opinion of Advocate General Wahl, Case C-150/17 P *Kendrion*, ECLI:EU:C:2018:612, paras 107–110, 124–128; Case C-337/15 P *Staelen*, ECLI:EU:C:2017:256; Havu (n 143).
[208] See eg Havu (n 143) 508–513.
[209] See also Resolution on Civil Liability (n 9) para 19.
[210] Although EU law principles such as those of effectiveness and equivalence, and the obligation to ensure the full effect of EU law, delineate the national courts' room for manoeuvre, room for interpretation can be significant and therefore diverging case outcomes can occur in different Member States. For discussion see eg Katri Havu, 'Full, Adequate and Commensurate Compensation for Damages under EU Law: A Challenge for National Courts?' (2018) 43(1*) European Law Review* 24, 24–27 37–46; Isabelle C Durant, 'Causation' in Helmut Koziol and Reiner Schulze (eds), *Tort Law of the European Community* (Springer, Vienna 2008) 47–79. See also more broadly on the limits for national courts' room for discretion Anne-Marie van den Bossche, 'Private Enforcement, Procedural Autonomy and Article 19(1) TEU: Two's Company, Three's a Crowd' (2014) 33(1) *Yearbook of European Law* 41–83.
[211] See eg Joined Cases C-46/93 and C-48/93 *Brasserie* (n 141); Case C-571/16 *Kantarev*, ECLI:EU:C:2018:807.
[212] See eg Art 82 GDPR, the PLD, and Directive 2014/104/EU on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union (2014) OJ L 349/1.
[213] Resolution on Civil Liability (n 9), see in particular Arts 4, 5–6, and 8 of the Draft Regulation.
[214] Ibid, see eg Arts 5–6 and 8 of the Draft Regulation.

compensation in the case of fault-based damages liability for other than high-risk AI,[215] which signifies potentially notable divergences in case outcomes.

Failure to provide clear EU-level rules on matters such as the notion of causation and the criteria for establishing it is prone to lead to divergences that concern deeply fundamental questions. The fact that the issue of causation – or, for instance, details of establishing harm – are usually left for Member State systems should not preclude the EU institutions from adopting tailored solutions. As expounded above, traditional (national) approaches to causation might be difficult to apply to cases involving AI or give rise to legal uncertainty. Moreover, as the Commission has emphasised,[216] there might even be a need to reverse the burden of proof on causation in order to make obtaining compensation a real possibility. All these factors seem to suggest that the condition of causation should receive more attention.

Contributory negligence

Article 10(1) of the Draft Regulation sets out that if the actions of an affected person or any person whom the affected person is responsible for contributes to harm, the extent of the operator's liability should be reduced accordingly. The operator will not be liable at all if the harm-sufferer or a person they are responsible for is solely responsible for harm. According to Article 10(2) of the Draft Regulation, an operator may use data generated by an AI system, in accordance with the GDPR, in order to support their claims. An affected person may also use these data.

Provisions on contributory negligence are common in the liability laws of Member States.[217] However, due to the technical particularities of AI systems discussed above, any rules on contributory negligence must be drafted carefully. The question arises whether the proposed provision is fit for its purpose. In most cases, an information asymmetry will exist between the operator and the harm-sufferer. Stating that the latter may use data generated by the AI system does not automatically entitle the harm-sufferer to access this data. Harm-sufferers might, therefore, face difficulties in terms of addressing any claims concerning contributory negligence. The wording according to which harm-sufferers 'may use' data could also lead to interpretative divergences in this context. It should be considered whether the harm-sufferer must be granted access to the relevant data and what are the related rights and duties of the parties and the courts hearing cases. A further issue is that the threshold and the exact requirements for proving contributory negligence should probably be relatively clear on the basis of EU law alone in order to avoid divergent case outcomes.

VI. Closing remarks

This contribution has discussed damages liability for AI-related harm. EU legislators have started the project of evaluating whether and what kinds of novel EU rules are needed to address this kind of harm, but the plans and proposals presented thus far are relatively preliminary or

[215] Ibid, see Arts 8–9 of the Draft Regulation (Art 9: 'Civil liability claims brought in accordance with Article 8(1) shall be subject, in relation to ... the amounts and the extent of compensation, to the laws of the Member State in which the harm or damage occurred').
[216] Eg Safety and Liability Report (n 3) 14, 16.
[217] See eg § 254 BGB for Germany, Art 6:101 BW for the Netherlands, Ch 6 VahL for Finland; van Gerven, Lever and Larouche (n 199) 729–736.

incomplete. In the EU Member States, discussion is ongoing on different aspects related to liability for AI-related harm as well as on broader questions of regulating AI.

The Commission White Paper addressing AI sets out ambitious goals in terms of utilising AI in ways that best benefit society and the economy, while ensuring that potential moral and legal problems are adequately addressed. The Commission as well as the EP have recognised several potential shortcomings in relation to current law on damages liability and highlighted the need to amend legislation to make it more easily applicable to AI-related cases and to guarantee legal certainty. Currently, several pieces of particular EU legislation are applicable to AI-related harm, but applying the law, together with complementing national law (the role of which remains notable), can be unpredictable and lead to divergent case outcomes when done by national courts.

The 2020 Resolution on Civil Liability, the first official EU-level document to propose certain concrete rules that would be generally applicable to private liability for AI-related harm, is apparently a relatively preliminary document lacking depth and detail in many places. The guiding idea of the proposals and plans set out concerning AI-related harm is that general rules on AI-related liability would be adopted without replacing particular legislation on liability in fields where such legislation already exists. Following this plan, the applicable law in the future would consist of general AI liability rules, particular legislation, as well as national laws. A revision of the PLD is envisioned and constitutes a parallel development to drafting more general rules on AI-related harm.

The Resolution on Civil Liability for AI-related harm remains quite far from comprehensive law that would ensure similar case outcomes across the EU. It is desirable that EU bodies continue working with this theme and come up with a more detailed and thorough proposal. While the EU institutions have put forward practicable solutions such as operator liability based on the principle that whoever exercises control over a risk should be liable if this results in damage caused to another, fundamental questions linked to the particular characteristics of AI systems remain unaddressed or are only touched upon briefly by existing documents.

Substantive questions of damages liability such as causation and the burden of proof must be addressed in light of particular AI characteristics, for instance autonomy, opacity, connectivity and the complexity of the value chain. EU-level rules on AI-related harm should also clearly address questions such as damage to data, and recoverability in respect of non-material harm.

The question also arises as to what the division of labour between EU law and national laws should be in the future. This is a theme which is intricate and includes the question whether national legislation, if clear and predictable, suffices even though case outcomes were slightly different in different Member States. Nonetheless, the goal of avoiding fragmentation and legal uncertainty within the Single Market can be seen as justifying harmonisation of many aspects and details of damages liability. The same applies even to certain evidentiary matters, although EU legislation usually leaves these to be governed by the systems of Member States. In our analysis above, we have highlighted several themes regarding which diverging case outcomes are possible unless future EU legislation concerning AI-related harm is elaborate.

A further matter is that ongoing discussions and legislative plans in EU Member States are interesting and often appear to be based on a good command of problems surrounding the issue of legislating on liability for AI-related harm. National preparatory documents, studies and plans could possibly provide EU legislators with valuable additional insights. The fact that

Member State authors are active in terms of regulating AI illustrates that the threat of a legally fragmented Single Market remains real unless EU legislators are able to provide detailed legislation and adequately resolve uncertainties related to liability for AI-related harm.