The AI Act and its impact on product safety, contracts and liability

Graaf, T.J. de; Veldt, G.M.

European Review of Private Law 5-2022 [803–834]

The AI Act and Its Impact on Product Safety, Contracts and Liability

Tycho DE GRAAF* & Gitta VELDT**

Abstract: On 21 April 2021, the European Commission presented a proposal for an Artificial Intelligence (AI) Act. The proposal's aim is to address the risks associated with the placement and putting into service of an AI system on the EU market. In this contribution the Draft Regulation, its relationship to existing product safety law and its consequences for the private law liability of providers and users are assessed. More in particular, the proposed risk-based approach is explained, high-risk AI systems are discussed in more detail and what the implications of this public law instrument are for the private law contractual relationships and liability of the provider and user of an AI system.

Zusammenfassung: Am 21. April 2021 hat die Europäische Kommission einen Vorschlag für ein Gesetz über künstliche Intelligenz (KI) vorgelegt. Ziel des Vorschlags ist es, die mit dem Inverkehrbringen und der Inbetriebnahme eines KI-Systems auf dem EU-Markt verbundenen Risiken zu behandeln. In diesem Beitrag werden der Verordnungsentwurf, sein Verhältnis zum bestehenden Produktsicherheitsrecht und seine Folgen für die privatrechtliche Haftung von Anbietern und Nutzern bewertet. Insbesondere wird der vorgeschlagene risikobasierte Ansatz erläutert, es wird näher auf KI-Systeme mit hohem Risiko eingegangen und es wird dargelegt, welche Auswirkungen dieses öffentlich-rechtliche Instrument auf die privatrechtlichen Vertragsbeziehungen und die Haftung von Anbietern und Nutzern eines KI-Systems hat.

Résumé: Le 21 avril 2021, la Commission européenne a présenté une proposition de règlement sur l'intelligence artificielle (loi IA), visant à traiter les risques associés à la mise à disposition et en service d'un système d'IA sur le marché de l'UE. Cet article évalue le projet de règlement, sa relation avec la législation existante sur la sécurité des produits et les conséquences pour la responsabilité civile des fournisseurs et des utilisateurs. Plus particulièrement, il explique l'approche développée dans la proposition fondée sur les risques, élabore en détails les systèmes d'IA à haut risque, discute des implications de cet instrument de droit public pour les relations contractuelles de droit privé ainsi que la responsabilité du fournisseur et de l'utilisateur d'un système d'IA.

* Professor of Technology and Private Law at Leiden University. For his contribution, we used our Dutch language article 'Productveiligheid en aansprakelijkheid voor AI', *NJB* 2021(43) , pp 3534-3544 as a basis, to the translation of which we added more sources and a far more extensive discussion on liability. De Graaf's research was funded by means of Leiden University's SAILS-project. The authors thank Sandra Dixon for editing large parts of this contribution. The final version of this contribution was submitted on 20 July 2022.
Email: T.J.deGraaf@law.leidenuniv.nl.

** Assistant Professor of Private Law and Empirical Legal Studies at Leiden University.
E-mail: g.m.veldt@law.leidenuniv.nl.

1. Introduction

1. On 21 April 2021, the European Commission presented a proposal for an Artificial Intelligence (AI) Act (hereinafter the 'Draft Regulation').[1] Because it is a regulation, it will apply directly in all EU Member States when, in its final form, it enters into force (Art. 288 TFEU). The proposal's aim is to address the risks associated with the placement and putting into service of an AI system on the EU market. The Draft Regulation is of a public law nature, uses the same layered approach as other product safety legislation and aims at preventing the materialization of risks not only to health and safety but also to fundamental rights.[2] It is primarily addressed at providers. In short, these are manufacturers/developers that place AI systems on the market. Other actors in the value chain, such as importers, distributors and users, are also covered. In particular, the Draft Regulation seeks to ensure that all products placed and put into service on the EU market by these actors are in conformity with the product standards set out in or adopted pursuant to the Draft Regulation. In this contribution we critically assess the Draft Regulation, its relationship to existing product safety law and the consequences of this public law instrument for the private law contractual relationships and liability of parties concerned.

Especially the two latter topics have received minor attention in the academic debate on the Draft Regulation, in our view somewhat unjustly. Discussing these topics is important because of three reasons. First of all, the influence of the Draft Regulation on private law contractual relationships and liability will contribute to the effectiveness of this public law instrument and thus be of interest to legislators and stakeholders. Secondly, commercial parties need to understand their public law obligations pursuant to the Draft Regulation and make sure that their commercial contacts are concluded/amended in such a way that any obligations for the fulfilment of which they are dependent on other parties are passed onto these other parties on a back-to-back basis and risks are allocated accordingly. Thirdly, an in-depth analysis of the private law implications is relevant because the European Commission announced a possible revision of the product liability directive in light of AI (s. 5) and such implications and revision together determine the total liability exposure of parties concerned.[3]

---

1 Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, 21 Apr. 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

2 Product safety law focuses on preventing the risk of death, injury and property damage, the more familiar product liability law on compensating that damage if those risks materialize.

3 Although the Draft Regulation applies to both governmental bodies and businesses, for the sake of brevity we focus exclusively on businesses and in particular on providers and users, and importers, agents and distributors are largely disregarded.

In this contribution, we first discuss the Draft Regulation's objectives, scope and relationship to existing product safety law (s. 2) as a basis for our private law analysis. We then explain the proposed risk-based approach and why high-risk AI systems deserve special attention (s. 3). We then focus in section 4 on high-risk AI system.[4] Although it is not the main aim of our article, we touch upon some inconsistencies and irregularities that deserve to be resolved before this proposal becomes law. In section 5 we address the liability implications and how to deal with them and regulatory risks in contracts between the provider and the user. Section 6 contains our conclusions.

2. Objectives, Scope and Relationship to Existing Product Safety Law

2. The Commission's aims under the Draft Regulation are, among others, (1) to ensure that AI systems placed and used on the EU market are safe and respect fundamental rights and EU values, (2) to provide legal certainty to facilitate investment and innovation and (3) to facilitate the development of a single market for legitimate, safe and trustworthy AI systems and prevent market fragmentation (Ch. 1.1 of the explanatory memorandum to the Draft Regulation). The Draft Regulation defines AI systems as 'software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with' (Art. 3(1)). Unfortunately, the techniques and approaches listed in Annex I are rather broad (e.g., 'logic and knowledge-based approaches' and 'statistical approaches'). As a result, the Commission's definition covers many algorithms[5] that have little to do with AI. The Draft Regulation therefore applies to many more systems than its title seems to suggest and regulates more than is strictly necessary.[6] It would have been

4 For non-high-risk AI systems as well as perspectives and critiques covered to a lesser extent in this article, see BEUC, Regulating AI to protect the consumer. Position Paper on the AI Act, BEUC-x-2021-088 – 07 Oct. 2021; EESC opinion on the Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, INT/940-EESC-2021-02482-00-00-AC-TRA; EPRS, Regulatory divergences in the draft AI act. Differences in public and private sector obligations, PE 729.507 – May 2022; and Michael Veale & Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach', *Computer Law Review International (CRi)* 2021(4), p 110.

5 According to Wikipedia, an algorithm is a 'finite sequence of well-defined instructions, typically used to solve a class of specific problems or to perform a computation', https://en.wikipedia.org/wiki/Algorithm.

6 See also Martin Ebers et al., 'The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)', *J Multidisciplinary Scientific Journal* 2021, p 590 and P.G. van der Putt, 'Het voorstel voor de

preferable to follow the definition formulated by the High Level Expert Group on AI because it better expresses two common features of AI: self-learning and/or autonomous behaviour.[7] If the definition of AI is not limited to these features, a high-risk AI system could include, for example, an HR appraisal system that averages partial scores. The provider of such a system would then have to comply with all kinds of additional requirements. In our opinion, there is less of a need to regulate these types of systems because the risks created by self-learning and/or autonomous behaviour will not materialize. The Council has already suggested to adjust this definition in its first partial compromise of 29 November 2021 so that regular software is excluded.[8] Nevertheless, Annex I has remained unchanged and still includes several less potentially harmful techniques, and therefore still needs to be amended.

3. The scope of the Draft Regulation is more interesting. In product safety law we are traditionally accustomed to regulating products that are placed on the market (cf. Art. 1 of the Model Decision[9]) or put into service in the EU by market participants (cf. Art. 4 (1) in conjunction with 2 (h) and (k) of the Machinery Directive 2006/42[10]). The Draft Regulation has a broader and also extraterritorial scope: it regulates not only AI systems falling within the scope of traditional product safety law but also AI systems located outside the EU where the output produced by the system is used in the EU (Arts 1(a) and 2(1)) or – as proposed by

---

"Artificial Intelligence Act"; waar is de betrokkene?', *Tijdschrift voor Internetrecht* 2021(4), p 46, who hopes that the Draft Regulation can lead to a broader anchoring, also outside AI, of transparency obligations, accountability obligations and extra scrutiny of decisions adversely affecting individuals.

7 Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *A Definition of AI: Main Capabilities and Disciplines Definition developed for the purpose of the AI HLEG's deliverables* (8 Apr. 2019), p 6, https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines: 'Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions'.

8 Council of Europe, Interinstitutional File 2021/106 (COD), 29 Nov. 2021 (14278/21), p 3, point 2(a) and Art. 3(1).

9 Decision No 768/2008/EC of the European Parliament and of the Council of 9 Jul. 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, OJ L 218, 13 Aug. 2008, pp 82–128 (Model Decision).

10 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, 9 Jun. 2006, pp 24–86 (Machinery Directive).

the European Parliament – affects natural persons within the EU (Arts 1(c) and 2(1)(c a)).[11] The Draft Regulation's wider-than-usual territorial scope probably has to do with the fact that product safety legislation, as can be seen in e.g., the Model Decision and the Machinery Directive, almost always applies to movable goods. Because such goods can only be in one place at a time, it is easier to establish their location for regulation purposes. In contrast, an AI system may, for example, consist of standalone software running in the cloud (Software-as-a-Service (SaaS)) outside the EU and being used in the EU. Think, for instance, of AI applicant selection software running in the US and used via a browser in the EU.[12] An AI system can also consist of software embedded in hardware as firmware, with the AI part running outside the EU. For example, an insulin pump that communicates autonomously via the internet with AI software running in China (Internet-of-Things) and autonomously determines the amount and timing of insulin to be injected into the patient's bloodstream.

4. It is also important to note that the Draft Regulation aims at maximum harmonization, but does not harmonize private law remedies, e.g., those of consumers (see s. 5 below),[13] and does not replace but supplements the existing rules

11 Products are deemed to be placed on the market for the first time if the offer is targeted at end-users in the EU, Commission Notice on the market surveillance of products sold online (C/2017/5200, *OJ C* 250, 1 Sep. 2017, pp 1–19), para. 1.2(b) and recital 15 and Art. 6 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 Jun. 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, *OJ L* 169, 25 Jun. 2019, pp 1–44 (Market Surveillance Regulation). See W. Gregory Vos, 'AI Act: The European Union's Proposed Framework Regulation for Artificial Intelligence Governance', 25 *J. Internet L* 2021(4), p 10. Proposed amendment 50 and 51 European Parliament in European Parliament, Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and the Council on harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM2021/0206 – C9-0146/2021 – 2021/0106(COD) 20 Apr. 2022) (hereafter: the EP-report). Various EP-committees have issued further opinions, as well as national parliaments. A mandatory consultation of the European Economic and Social Committee is also expected. For an overview see the European Parliament Legislative Observatory, Procedure file 2021/0106(COD) Artificial Intelligence Act, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD (accessed 18 Jul. 2022).

12 For problems Amazon experienced using such software, see Jeffrey Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women* (11 Oct. 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

13 Incidentally, it is likely that the Draft Regulation – if it makes it to the finish line in whatever form – will be included in the annex to Directive 2020/1828, which will also make collective action possible throughout the EU in the event of a breach. This would address some of the criticisms made, e.g., by BEUC 2021, p 23. Compare also G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling (Recht en Praktijk nr. CA22)* (diss. Leiden) (Deventer: Wolters Kluwer 2020), para. 190.

relating to data protection (e.g., the GDPR 2016/679), consumer protection (e.g., the Consumer Sales Directive 2019/771 and the Digital Content and Services Directive 2019/770) and non-discrimination (e.g., the Charter of Fundamental Rights of the European Union) (s. 1.2 of the explanatory memorandum to the Draft Regulation). Likewise, the Draft Regulation is intended to supplement existing product safety legislation or at least to be integrated into it (see s. 4 below). This makes it difficult for those concerned to determine which obligations to abide by and how these different instruments relate to each other.

3. Risk-Based Approach

5. The Draft Regulation is risk-based, meaning that the obligations of providers and users (and others in the value chain) in relation to AI systems depend on the degree of risk posed by the marketing, deployment or use of those systems. Four risk categories are distinguished: (1) prohibited practices (Title II, Art. 5), (2) high risk (Title III, Chapter 1, Arts 6–7), (3) transparency risks (Title IV, Art. 52) and (4) no/minimum risk. Prohibited practices are listed exhaustively in Article 5 and include, among others, the use of AI techniques that subliminally influence the subconscious in such a way that physical or psychological harm is inflicted or is likely to be inflicted on individuals (Art. 5(1)(a)). An example could be the continuous use of AI systems in surreptitious advertising in a bar or casino that causes or is likely to cause physical harm (to the liver) or psychological harm (gambling addiction), respectively. For the two lowest risk classes (transparency risk and no/minimum risk), the Draft Regulation refers, among other things, to the possibility for Member States to encourage codes of conduct (Art. 69). Only high-risk AI systems will be addressed below.[14]

4. High-Risk AI Systems

4.1. Categories, Obligations and Obligors

6. High-risk AI systems fall into two categories: (1) AI systems which (a) are embedded in a product covered by the product safety legislation listed in Annex II and are intended to be used as a safety component[15] of that product ('embedded AI systems') or (b) are themselves covered by such legislation ('standalone AI systems') (1 (a) and (b) therefore relate to existing EU product safety legislation, see s. 4.2 below) and (2) AI systems referred to as 'area-based systems' (see s. 4.3 below).

14 For a more extensive discussion of the other categories see Michael Veale & Frederik Zuiderveen Borgesius, *CRi* 2021, pp 98–102 and 106–108.

15 The definition of safety component is very broad. It extends to a component 'the failure or malfunctioning of which endangers the health and safety of persons or property' (Art. 3(14)). Contrary to what the name suggests, it is not decisive whether the component fulfils a safety function.

Importantly, AI systems in category (1) are only regarded as high-risk systems if the product in question – whether the product in which the AI system is embedded or the standalone AI system itself – is required to undergo a third-party conformity assessment (Art. 6(1)(b)). In the case of embedded AI systems, the manufacturer of the product containing such a system is often allowed under the relevant EU product safety legislation to carry out the conformity assessment of the product itself. In that event, the AI system is not characterized as high-risk under the Draft Regulation and the manufacturer therefore does not have to comply with the regulation's obligations that apply to the providers of such systems, unless the product is subject to area-based regulation (see 4.3 below).

7. The body which carries out a third-party conformity assessment is called a conformity assessment body, or more commonly a notified body, and is often an accredited private party. The notified body assesses whether the AI system, the provider's quality management system and the technical documentation comply with the EU so-called harmonized standards (detailed product standards and technical specifications) implementing the so-called essential requirements (high-level requirements) of the Draft Regulation (Art. 43(1)(b) Draft Regulation).[16] In making this assessment, the notified body relies not only on documents furnished by the provider but also on tests and periodic audits carried out by the notified body itself (Art. 5.3 of Annex 7 of the Draft Regulation). The assessment must be performed before the AI system is placed on the market (Art. 43.3) and again whenever it is substantially modified (Art. 43.4).[17] It is unclear how well this approach would work in practice. Notified bodies will most likely not yet have all the AI expertise required. Their competences will have to be accredited (Art. 43.3 second paragraph).

8. Title III, Chapter 2 of the Draft Regulation contains the essential requirements with which high-risk AI systems must comply and which, as said, will be implemented in more detailed European harmonized standards. As there are quite a few essential requirements, we will highlight only some of them. The AI system provider (in short, a manufacturer/developer that places embedded or standalone AI systems on the EU market, Art. 3(2)) must ensure pursuant to Article 16(a) that

16 Explanatory notes on the Draft Regulation, p 7. This exemplifies what is called the 'new approach'. For an explanation of this approach, see G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling*, paras 1 and 3 and Chs 4 and 4.2. Specifically with regard to the Draft Regulation see Michael Veale & Frederik Zuiderveen Borgesius, *CRi* 2021, pp 104–106.

17 Article 3 (1) (23) definition of substantial modification, see proposed amendment 61 EP-Report, p 48: '(23) "substantial modification" means a change ***or a series of changes*** to the AI system following its placing on the market or putting into service which affects the compliance of the AI system with the requirements set out in Title III, Chapter 2 of this Regulation or results in a modification to the intended purpose for which the AI system has been assessed ***or to its performance***;'.

they are designed and developed so that events can be logged (Arts 12(1) and 16(a)) and so that operations are 'sufficiently transparent to enable users to interpret the system's output and use it appropriately' (Art. 13(1)). Many self-learning AI systems are, by their nature, '*black boxes*', i.e., it is often not clear even to the provider how the AI system learned and arrived at a particular result.[18] The unclear wording of Article 13(1), which focuses on the output and the use thereof, raises the question whether a black box AI system is sufficiently transparent to meet the requirements of that provision.[19] If not, those requirements could hamper innovation and justify removing Article 13(1) from a future version of the Draft Regulation. However, it could also be argued, and we believe more convincingly, that in certain cases the technology should be adapted so as to ensure that the requirements are met (perhaps even in such a way that the AI is explainable).[20]

9. Article 16(a) also requires the provider to ensure that the AI system is designed and developed in such a way that (1) it can be effectively overseen by a human operator with a view to preventing or minimizing risks to health, safety or fundamental rights (Art. 14, e.g., by means of the proverbial red stop button), to which the European Parliament (hereafter 'EP') suggested an addition to ensure that those overseeing 'are specifically made aware and remain aware of the risk of automation bias',[21] and (2) it achieves, throughout its life cycle, 'an appropriate level of accuracy, robustness and cyber-security' in light of its intended purpose (Art. 15(1)). Furthermore, the provider must furnish instructions for use (Art. 15(2)), draw up and update technical documentation (Arts 16(c) in conjunction with 11), have in place a quality management system (Arts 16(b) in conjunction with 9 and 17) and perform corrective maintenance as well as withdraw or recall the AI system if it believes or has reason to believe that the system is not in conformity with the regulation (Art. 21). The ease with which corrective maintenance can be performed or the AI system can be withdrawn or recalled will depend on the extent to which the system can be modified remotely: this is sometimes possible by means of an over-the-air update but sometimes physical access to the system is required. Also, if the provider uses data sets to train, validate or test the AI system, it must ensure that those sets are 'relevant, representative, free of errors and complete'

18 Martin Ebers, 'Regulierung von KI und Robotik', in Martin Ebers, Christian Heinze, Tina Krügel & Björn Steinrötter (eds), Künstliche Intelligenz und Robotik. Rechtshandbuch (München: C.H. Beck 2020), pp 90–92 and Martin Ebers, 'Regulating AI and Robotics', in Martin Ebers & Susana Navas, Algorithms and Law (Cambridge: Cambridge University Press 2020), pp 165–166.

19 Thus, also Martin Ebers et al., *J Multidisciplinary Scientific Journal* 2021, pp 596 and 601.

20 Compare Sven J. Körner, 'Nachvollziehbarkeit von KI-basierten Entscheidungen', in Markus Kaulartz & Tom Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning (München: C.H. Beck 2020), pp 44–51.

21 Proposed amendment no. 105, Art. 16(1)(aa) EP-Report, p 66.

(Arts 16(a) in conjunction with 10(3)).[22] The last two requirements are problematic. The more data that is used, the better AI systems can learn.[23] At the same time: datasets are almost never completely error-free. And in many cases they do not have to be, because algorithms can learn to ignore outliers. Requiring that the data be error-free, or even complete, therefore seems unrealistic. In addition, before the AI system is placed on the market or put into service, the provider or its authorized representative[24] must register it in a new EU AI database (Arts 51 in conjunction with 60).

10. If the manufacturer of a product subject to EU sector-specific product safety legislation places it on the market or puts it into service together with a high-risk AI system and under the manufacturer's own name, that manufacturer has the same responsibility and obligations with respect to compliance of the AI system with the Draft Regulation as the provider (Art. 24).[25] This is not surprising. After all, a manufacturer of finished movable goods must also ensure the safety of the raw materials or physical components used in them. However, where the manufacturer of a product incorporating a high-risk AI system depends on cooperation from a third-party software developer in order to comply with the Draft Directive – e.g., in order to carry out corrective maintenance – extra measures (such as pre-existing contractual agreements) may be necessary to ensure that the manufacturer is in a position to comply with the regulation's requirements (see s. 5.2 below).

11. The user (in short, the person under whose authority the AI system is used, Art. 3(4)), has far fewer obligations. It must use the system in accordance with the operating instructions (Art. 29(1)) and, to the extent it has control over the input

22 See also proposed amendment no. 96, Art. 10 (3) EP-Report, p 62 holding: 'Training, validation and testing datasets shall be relevant, representative, up-to-date, and to the best extent possible, taking into account the state of the art, free of errors and be as complete as possible. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the datasets may be met at the level of individual **data sets** or a combination thereof'.

23 Monika Valkanova, 'Trainieren von KI-Modellen', in Markus Kaulartz & Tom Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning (München: C.H. Beck 2020), p 336.

24 A provider outside the EU must appoint an authorized representative before making the system available in the EU (Art. 25(1)), as a point of contact, information point and cooperation partner for the authorities (Art. 25(2), and proposed amendment 123 and 124 of the EP-Report). The authorized representative's position will not be discussed in detail here.

25 These rules are reminiscent of Art. 3 (3) of the Sale of Goods Directive 2019/771, http://data.europa.eu/eli/dir/2019/771/oj: if a seller sells goods that incorporate, or are inter-connected with, digital content or digital services, that directive also applies to the seller 'irrespective of whether such digital content or digital service is supplied by the seller or by a third party'. A consumer may therefore assert rights against that seller in the case of non-conformity even if the seller does not control the digital content or services and that third party has concluded a separate contract with the consumer with respect to such digital content or digital service.

data, must ensure that such data is relevant in light of the AI system's intended purpose (Art. 29(3)). To that, the EP added that users must ensure that natural persons entrusted with human oversight are 'competent, properly qualified and trained and have the necessary resources in order to ensure the effective supervision of the system'.[26] Furthermore, the user must monitor the AI system based on the operating instructions and, if it has reason to believe that use in accordance with those instructions will result in the materialization of risks to health, safety or fundamental rights, must (immediately)[27] inform the provider of this and suspend the use of the system (Art. 29(4) in conjunction with Art. 65).

12. As noted above, a third-party conformity assessment is required whenever a high-risk AI system is substantially modified (Art. 43(4)). The question of whether a substantial modification has occurred can be problematic in the case of self-learning AI systems, especially if these systems amend themselves. According to Article 43(4), changes to an AI system and its performance that are predetermined by the provider at the time of the first conformity assessment and are part of the technical documentation do not constitute substantial modifications. An important question, however, is the degree of detail and specificity with which a change must be described in the technical documentation in order to avoid being characterized as a substantial modification (see also Annex IV, Art. 2(f), which speaks of a 'detailed description'). In other words, can the provider simply set out a laundry list of possible changes to the AI system or its performance, even if they are unlikely, in order to ensure that if any of them occur no new conformity assessment is necessary? The European Commission (hereafter 'EC') would have been better of adding language to disincentive providers from doing so. The assessment of a technical file to determine whether a substantial modification has occurred will in any case require a great deal of expertise and foresight. The real discussions on substantial modifications are expected to occur only when enforcement measures are taken by authorities after incidents, or between the market participants and/or third parties concerned.

13. A user (or distributor, importer or third party) who markets or puts into use an AI system under its own name or trademark, changes its purpose or modifies the system substantially will be treated as the provider, in which case the original provider will no longer be regarded as such (Art. 28(1)(a)-(c) and (2)). When will the use be considered to have changed the AI system's purpose or modified the system substantially? Only if the user actively does so, or also if the AI systems changes or modifies itself on the user's watch or due to data being fed by the user? Further clarity on this subject would be desirable. If it applies, it marks a turning point in the risk allocation between the provider and the user, who – as the new

26 Proposed amendment 137, Art. 29 (1)(b), EP-Report, p 79.

27 Proposed amendment 141 EP-Report, p 80, adding 'immediately' to the criterion.

provider – must suddenly comply with a multitude of new obligations. In that event, an all-or-nothing approach applies. From then on, the authorities can hold the user-turned-provider accountable for all infringements, regardless of the extent to which they caused the relevant problem to arise. The question is whether it is realistic to require a user who puts into use an AI system under its own name to comply with these obligations and to have the AI system subjected to a new conformity assessment, even if the user did not design or develop the AI system and may not and often does not have the required source code,[28] data, tools, knowledge and/or experience. The European Parliament seems to think this is not the case. It proposed an amendment to Article 28(1)(a) exempting such user in case contractual arrangements provide otherwise. Although this might be beneficial to the user, it could in practice create substantial investigation and enforcement issues for authorities, especially when disputes arise between the parties and the regulatory authorities on the interpretation and magnitude of their contractual arrangements. We are of the opinion that contractual arrangements between private parties may, in principle, not determine public law obligations and enforcement thereof, and therefore suggest amending this. At the same time, the proposed amendment making the user provider in case it modifies the intended purpose of a (formally low risk) AI-system (Art. 28(1)(b a) (new)) or substantially modify an AI-system (new Art. 28(1) (c a (new)) *to such an extent that it becomes a high-risk system* may be positively welcomed.[29]

4.2. AI and Existing EU Product Safety Legislation

4.2.1. Product Safety Law: Old and New Approach

14. As regards the relationship between the Draft Regulation and EU product safety law, a distinction should be made between 'old-approach product safety legislation' and 'new-approach product safety legislation' (referred to in the Draft Regulation as the New Legislative Framework). Old-approach product safety legislation consists of regulations and directives containing detailed product standards and specifications. This is particularly evident in legislation adopted (for the first time) before 1985. Examples of such legislation are mainly found in the mobility sector, such as the Regulation on the approval and market surveillance of motor vehicles.[30] New-approach product safety legislation consists, in short, of legislation, mainly directives, adopted (for the first time) after 1985 and largely limited to

28 If requested, however, the authorities must be granted access to the source code on the basis of Art. 64 (2) of the Draft Regulation.

29 Proposed amendment 131 and 134, p 77 EP-Report.

30 Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007

essential requirements; detailed product standards and technical specifications on how to meet them are not included. The essential requirements in legislation are worked out in detail by EU standardization bodies (such as CEN, See CENELEC and ETSI) in non-binding, detailed product standards and technical specifications referred to as harmonized standards. As products manufactured in conformity with these harmonized standards are presumed to comply with the essential requirements,[31,32] many manufacturers in practice rely on the harmonized standards to satisfy their compliance obligations. Examples of new-approach product safety legislation are the Machinery Directive and the Medical Devices Regulation 2017/745 (MDR),[33] both of which were updated after the introduction of the New Legislative Framework.[34] The Draft Act is a New Approach-instrument.[35]

4.2.2. Old Approach

15. At first sight, the Draft Regulation seems to apply to products covered by either old-approach or new-approach product safety legislation. Under Article 6(1) the question whether an AI system is considered to be high-risk depends, among other things, on whether it is a safety component of a product (or is itself a product) covered by the regulations and directives set out in Annex II. Annex II includes regulations and directives applying the old approach (Annex II Part B) and ones applying the new approach (Annex II Part A), suggesting that the both old- and new-approach product safety legislation is subject to the entire Draft Regulation. Under Article 2(2) of the Draft Regulation, however, high-risk AI systems that fall within the scope of the old-approach product safety regulations and directives listed in Annex II Part B are subject only to Article 84 of the Draft Regulation (requiring

---

and (EC) No 595/2009 and repealing Directive 2007/46/EC, *OJ L* 151, 14 Jun. 2018, pp 1–218 (Regulation on the approval and market surveillance of motor vehicles).

31 CEN (which stands for Comité Européen de Normalisation) is the European Committee for Standardization. CENELEC (which stands for Comité Européen de Normalisation Electrotechnique) is the European Electrotechnical Committee for Standardization. ETSI is the European Telecommunications Standards Institute. These are the three recognized European Standardization Organizations.

32 Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards, *OJ C* 136, 4 Jun. 1985, pp 1–9 and Art. 40 of the Draft Regulation.

33 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 Apr. 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, *OJ L* 117, 5 May 2017, pp 1–175 (MDR).

34 The New Legislative Framework (NLF) consists of a package of measures introduced in 2008 in order to improve new-approach product safety legislation in line with the new Model Decision. The NLF is currently being evaluated, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12654-Industrial-products-evaluation-of-the-new-legislative-framework_en.

35 Standards with regard to AI are being developed as we speak but not within the framework of EU-legislation, see e.g., ISO/IEC 38507 on the use of AI.

an evaluation and review of the regulation) and not its other provisions (Chapter 1.2 of the explanatory memorandum to the Draft Regulation and recital 29 of the Draft Regulation). This should have been made clearer. When adopting any future delegated or implementing acts on the basis of these old-approach instruments, the Commission will be required to take into account, 'on the basis of the technical and regulatory specificities of each sector', the mandatory requirements for high-risk AI systems laid down in the Draft Regulation (recital 29).[36] Thus, self-driving cars are not directly covered by the Draft Regulation (other than Art. 84) but if new delegated or implementing acts are adopted on the basis of the – old-approach – Regulation on the approval and market surveillance of motor vehicles, the Commission must incorporate the Draft Regulation's mandatory requirements for high-risk AI systems in those new or implementing acts subject to 'the technical and regulatory specificities of each sector'. The AI elements of self-driving cars' autopilot will eventually be subject to many of the obligations applicable to high-risk AI systems under the Draft Regulation but only through an indirect route.

4.2.3. New Approach

16. The manufacturer of a product with embedded AI is often allowed, under new-approach EU product safety legislation, to carry out a conformity assessment of the product itself. In such cases, the embedded AI is in principle[37] not regarded as high risk under the Draft Regulation and the manufacturer is therefore not bound by the multitude of obligations relating to AI systems in that category (see s. 4.1 above). In practice, the situation is less straightforward than might at first appear. Take, for example, AI embedded in hand-fed surface planing machines for woodworking. These machines are included in Annex IV of the – new-approach – Machinery Directive. If such a machine, with the use of AI and sensors, self-learns how fast it must turn in order to plane wood as quickly and accurately as possible, then the machine is indeed dangerous; nevertheless, under the Machinery Directive it need only be subjected to a conformity assessment by a notified body if it is not manufactured in accordance with the harmonized standards issued pursuant to that directive *or* if those standards 'do not cover all the relevant essential health and safety requirements' (Art. 12 (4) Machinery Directive). Especially the latter criterion will in practice give rise to discussion: if the planer is designed and manufactured in accordance with the harmonized standards, do those standards cover all the relevant essential health and safety requirements, including requirements to prevent risks arising from the autonomous and/or self-learning nature of AI? We believe it is at

36 In order not to mislead those reading the Draft Regulation, we believe that it would have been better to list the old approach instruments in a separate annex and to incorporate Ch. 1.2 and recital 29 in an article in the Draft Regulation.

37 Exception: if the product is subject to area-based regulation, see s. 4.3 below.

least arguable that the harmonized standards issued pursuant to the Machinery Directive are insufficient, when it comes to AI, to cover all the relevant essential health and safety requirements.

It seems that the Commission has sought to nip this discussion in the bud by indicating in its proposal for revision of the Machinery Directive and its recasting as the Machinery Regulation that all high-risk machinery (listed in Annex I of the draft Machinery Regulation) using AI must always be subject to a conformity assessment by a notified body (see Recitals 19 and 45).[38] Recital 45 gives the following reasons for this: 'due to the characteristics of artificial intelligence such as data dependency, opacity, autonomy and connectivity, which might increase very much the probability and severity of harm and seriously affect the safety of the machinery product'. and 'Furthermore, the market for software ensuring safety functions of machinery products based on artificial intelligence is so far very small, which results in a lack of experience and data'.

At least until the Machinery Regulation replaces the Machinery Directive, however, the situation will remain murky. The planer manufacturer referred to above could wrongly believe, on the basis of the text of the Draft Regulation, that the multitude of requirements which that regulation imposes on the provider of a high-risk AI system do not apply to it because the planer complies with harmonized standards issued pursuant to the Machinery Directive and a third-party conformity assessment is therefore not required under that directive. In practice, however, the manufacturer could very well fail to consider the possibility that those standards do not cover all the relevant essential health and safety requirements relating to AI and, if it does consider this, could assume, based on longstanding practice, that the standards do cover those requirements. In a sense, the Commission's approach gives the planer manufacturer a false sense of security that the embedded AI system will not be categorized as high risk, whereas at the very least the question is debatable.

Given the reasons for regulating AI as stated in the proposal for a new machinery regulation, we expect that many more new-approach product safety regulations or directives listed in Annex II (A) will be amended to require a third-party conformity assessment in the case of all high-risk products incorporating AI. If this expectation turns out to be true, the question arises whether the Commission should not have chosen to follow the old-approach regime for new-approach legislation as well: i.e., to determine separately for each regulation and directive which products (with embedded AI or consisting of standalone AI) are

38 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on machinery products', COM(2021) 202 final, 21 Apr. 0202, which at the end of recital 45 provides: 'Therefore, the conformity assessment of software ensuring safety functions based on artificial intelligence should be carried out by a third party'. However, the articles of the draft Machinery Regulation are not as explicit as recital 45.

subject to which AI regime.[39] However, in that case it would take a very long time to introduce the requirements relating to high-risk AI systems in every regulated sector. It would also necessitate a discussion, every time existing product safety legislation is amended, as to whether those requirements apply or need to be modified. This in turn would lead to delays and fragmentation. For the time being, it seems that the Commission has favoured speed and uniformity over legal certainty. We think this is a good choice in view of the rapid development of technology and the often-lengthy legislative processes, although better communication with manufacturers is needed to counteract the false sense of security referred to above. Moreover, a lot of guidance is needed on which aspects are covered by essential requirements in sector specific legislation and which aspects are not, especially in areas where there is potential overlap like with medical devices.[40] At the moment such guidance is lacking, let alone that clear articles are included on how to deal with overlapping regulatory obligations. In the absence of such guidance and articles, market participants lack the legal certainty they so rightly crave in this increasingly complex area of law. And such lack of legal certainty may in turn lead to non- or less compliance, something which is not in anyone's interest.

4.3. Other High-Risk AI: AI Systems Creating a Risk to Fundamental Rights (Area-Based)

17. High-risk AI systems also include the AI systems referred to in Annex III to the Draft Regulation (Art. 6(2)). According to Chapter 5.2.3 of the explanatory memorandum, these are, in short, AI systems with 'mainly fundamental rights implications'. An example is the AI application selection software mentioned above, which runs in the US and is used in the EU via a browser (Annex III point 4 (a)). These systems are classified as high-risk irrespective of any existing product safety legislation. The application of the Draft Regulation to them is relatively straightforward: the relevant actors must comply with the requirements of the Draft Regulation and follow a conformity assessment procedure based on internal checks

39 Admittedly, the problems outlined do not arise in sectors that are more strictly regulated in the sense that almost all products (including software) in those sectors require a conformity assessment by a notified body, e.g., the MDR (see Art. 2.1). For a general proposal that high-risk standalone AI systems should always require a conformity assessment by a notified body, see Gerald Spindler, 'Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E). Ansatz, Instrumente, Qualität und Kontext', *Computer und Recht* 2021(6), p 373.

40 See extensively W. Choi, M. Van Eck, C. van der Heijden e.a., *Legal analysis European legislative proposal draft AI act and MDR/IVDR, Hooghiemstra & Partners & Axon Science Based Lawyers, January 2022. Report commissioned by the Dutch Ministry of Health, Welfare and Sport*. for problems in concurrence with the medical devices regulations.

(pursuant to Art. 43 (2) in conjunction with Annex III points 2–8).[41] In principle in principle a conformity assessment by a notified body is not required.

5. Contracts and Liability

5.1. Introduction

18. What would the Draft Regulation, if adopted in its current form, mean for contracts and liability? The Draft Regulation does not appear to actively harmonize private law remedies.[42] The European Parliament has proposed an amendment of Recital 84 in the form of a new Recital 84 b stating amongst other things that natural and legal persons, as well as groups thereof, should have the right to lodge a complaint against the providers or users of AI systems and receive compensation.[43] At the same time, the EP amendments of the core articles do not contain a harmonized right to European right to compensation or damages in horizontal relationships, making this amendment effectively useless from a legal point of view.[44] Any claim brought against the provider or user by individuals who suffer damage from AI systems must therefore still be based on existing EU and national private law. We highlight a few issues that may arise in this connection.

Firstly, obligations under the Draft Regulation will unmistakably colour the private law duties of care owed by providers and users to each other,[45] who must

41 For a criticism of this approach, see (among others) N. Smuha, E. Ahmed-Rengers, A. Harkens, W. Li, J. MacLaren, R. Piselli & K. Yeung, *How the EU can achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, LEADS Lab @University of Birmingham (5 Aug. 2021), pp 36 ff.; Michael Veale & Frederik Zuiderveen Borgesius, *CRi* 2021, p 106; EESC, nos. 1.10 and 4.25. See for exceptions: biometric identification (Art. 43(1) in conjunction with Annex III(1)) and Art. 43(2) of the Draft Regulation.

42 See also G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling*, Ch. 3 as well as G. M. Veldt, 'Proefschrift: drie stellingen: Europese productnormen en privaatrechtelijke normstelling', *WPNR* 2021(7331), pp 518–521.

43 EP-Report, Proposed amendment 46, p 42: '(84b) Natural and legal persons and groups of natural or legal persons should be entitled to access proportionate and effective remedies. They should in particular have the right to lodge a complaint against the providers or users of AI systems and receive compensation against any direct damage or loss they have with regard to their health, safety, or fundamental rights, due to an infringement of this Regulation by the provider or the user. Without prejudice to any other administrative or non-judicial remedy, natural and legal persons and groups of natural or legal persons should also have the right to an effective judicial remedy with regard to a legally binding decision of a national supervisory authority or of the Commission concerning them or, where the national supervisory authority does not handle a complaint, does not inform the complainant of the progress or preliminary outcome of the complaint lodged or does not comply with its obligation to reach a final decision, with regard to the complaint'.

44 EP-Report, Proposed amendment 270, p 142 regarding Art. 68k.

45 G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling*, Ch. 7 and Christina Amato, 'Product Liability and Product Security: Present and Future', in Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and Internet of Things.*

take these obligations into account in their internal dealings. This is particularly important where the user is treated as the provider following a substantial modification of the AI system. This may well require amendments to existing agreements or the conclusion of new agreements between them (s. 5.2 below). Secondly, the Draft Regulation will affect the legal relationship between the provider and third parties (such as consumers[46]). It would go too far to consider all possible interactions between the Draft Regulation and private liability law in relation to the provider, the user and third parties.[47] We suffice with some remarks on tort actions based on breach of a statutory duty and product liability as both could apply in the relationship between providers, users/operators and third parties (s. 5.3 below).[48]

5.2. In the Relationship Between the Provider and User

19. As a result of its change of status from user to provider (see s. 4.1 above) in the event of a substantial modification of a high-risk AI system, the new provider becomes the sole point of contact for the authorities. In addition, the new provider is obliged to bring the AI system into line with the requirements of the Draft Regulation, resulting in new or at least increased duties of care. The question is how the old and new providers will deal with these risks. Much will depend on how the substantial modification took place. Usually, software can only be substantially modified by changing its source code. As a rule, a software supplier which has developed and holds the copyright to that code grants the customer a right to use the software's object code pursuant to a software license agreement, and in that agreement prohibits the customer from changing the software without prior written consent. If the customer nevertheless changes the software in one way or other without such consent, the software licence agreement often provides that the

---

Münster Colloquia on EU Law and the Digital Economy IV (Baden-Baden: Nomos 2019), pp 77–95.

46 Consumers are not included in the definition of user under the Draft Regulation. See Art. 3(4), in which individuals using AI systems in the course of a personal, non-professional activity are excluded.

47 For an overview of the most important principles in the various Member States with regard to liability for AI, see E. Karner, B.A. Koch & M.A. Geistfeld, *Comparative law study on civil liability for artificial intelligence* (Brussel Nov. 2020 (Published 5 May 2021)). See further for Dutch law with respect to non-contractual liability T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid voor robots en algoritmes', *NTHR* 2017(3), pp 123–132 and contractual liability T.J. de Graaf & I.S. Wuisman, 'Contractual liability for the use of AI systems under Dutch law and EU legislative proposals', in Bart Custers & Eduard Fosch-Villaronga (eds), *Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice* (Springer & T.M.C. Asser Press 2022), Ch. 14.

48 See for the inception impact assessment dated 30 Jun. 2021 and the ongoing consultation, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en. A Commission proposal is expected in Q3, 2022.

customer's right to contractual indemnification by the supplier based on the infringement of third parties' intellectual property rights lapses, as does any obligation of the supplier to repair defects in the software. This seems quite reasonable.

However, changes to AI systems are more complex. This is because these changes can occur not only through human actions (by the supplier's or customer's software developers) but also because the AI system self-learns and adapts based on what it has learned. Whether it is reasonable for a supplier to be freed from the obligation to indemnify or repair seems at first sight to depend on the cause of the relevant change. If the change originates in the software developed by the supplier, that result does not seem reasonable. If the cause is incorrect training data provided by the customer, it may seem reasonable. However, there are many shades of grey in between, and it is very questionable whether, if it is reasonable from a civil law perspective, it is also reasonable from a product safety perspective. After all, if – to revert to the terminology of the Draft Regulation – the user is suddenly treated as a provider because the AI system undergoes a substantial modification, the new provider will be highly dependent on the old provider to continue to meet the requirements of the Draft Regulation. For example, if the new provider is required to perform corrective maintenance, it will usually need the old provider's cooperation because usually only the old provider has the required source code, data, tools, knowledge and/or experience. It would be advisable for the user to cover such risks contractually in advance, failing which it runs the risk of becoming trapped between the authorities and the old provider. In the case of a non-compliant AI system, the user also runs the risk of being trapped between third parties and the old provider, in which case contractual agreements on specific performance (in order to prevent or limit damage) and indemnification could be useful.[49]

20. Let us return to the risk of the new provider becoming trapped between the authorities and the old provider. In order to comply with its possibly sudden and unexpected information obligations towards the authorities, the user-turned-provider has an interest in having the old provider agree, where possible in advance, to cooperation obligations, including obligations to furnish information, documentation and code. It is also a good idea for the parties to have agreed that the new provider must be notified by the old provider of (1) changes to the AI system that may affect its operation and safety (e.g., updates) and (2) any risks and incidents involving the use of the AI system by third parties of which the old provider is or becomes aware after the product is placed on the market. The Draft Regulation does not explicitly require the old provider to notify the new provider of incidents

49 For contractual provisions intended to protect against this, see e.g., Art. 18 of the Directive on the online sale of goods (SGD) 2019/771 and Art. 20 of the Directive on the supply of digital content and digital services (DCD) 2019/770. See for a discussion of the impact of these directives on AI R. M. Gellert, 'The EU'S New Directives on Digital Contracts, and Artificial Intelligence: Really Future Proof?', *ERPL* 2021(3), pp 403–424.

(*top down*).[50] Conversely, it is questionable whether the Draft Regulation requires the new provider to inform the old provider of any risks of which the new provider has been informed by intermediaries (*bottom up*).[51]

21. The Draft Regulation requires both providers and users to keep and make available to the authorities the automatically generated logs which are under their control (Art. 20(1) and Art. 29(5), respectively).[52] Contractual arrangements on the availability and furnishing of these logs by the old provider to the new provider are indispensable, if only to ensure that they are furnished, without delay, if the old provider goes bankrupt. This is important not only when the logs are requested by the authorities (and must be turned over within 15 days) (Art. 62(1))[53] but also, in the event of an incident, to establish e.g., cause, causality and attribution for evidentiary purposes. In the absence of a harmonized right to information in the Draft Regulation,[54] a user's right to information vis-à-vis the provider must be based on national law, at least if no contractual arrangements have been made to that effect.

22. It is also important to note that the Draft Regulation – unlike general product safety law – contains an explicit harmonization of administrative fines (Art. 71(1) to (7)), which may have been inspired by the turnover-related fines that exist in some

50 For example, the notification duty imposed in Art. 21 (Corrective Action) of the Draft Regulation on providers of high-risk AI systems is limited to distributors, agents and importers (but not new providers). However, such providers do have reporting obligations towards the authorities. See Arts 16(h), 22 and 62. Article 61 obliges such providers to establish, document and maintain post-market monitoring systems. The proposed amendments of the European Parliament do require the provider to inform the users of the high-risk AI system, proposed amendment 118 regarding Art. 22(1) of the EP-Report. Users are also required to cooperate with information requests by the national competent authorities, the Board or the Commission including access to logs, proposed amendment 121 and 122 regarding Arts 23(1) and 23(1)(a) of the EP-Report.

51 Article 26(2) (importer versus provider) and Art. 29(4) (user versus provider) of the Draft Regulation.

52 According to the proposed EP-amendments the logs are required for ensuring and demonstrating compliance with this Regulation, for ex post audits of any reasonably foreseeable malfunction, incidents or misuses of the system, or for ensuring and monitoring for the proper functioning of the system throughout its lifecycle, proposed amendment 142 regarding Art. 29(5)(1) EP-Report.

53 Martin Ebers et al., *J Multidisciplinary Scientific Journal* 2021, p 598 advocate extension of this very short deadline.

54 See also P.G. van der Putt, *Tijdschrift voor Internetrecht* 2021, p 146, who argues for information and compensation rights of natural persons adversely affected by AI systems. Given the traditional focus of product safety law on manufacturers and public law oversight, we believe that the Draft Regulation may be amended to include an information right (as in the MDR) but will not be amended to include a right to damages. A right to damages will more likely appear in the liability instrument(s) yet to be published. See also our discussion above of Recital 84 b proposed by the EP.

Member States for infringements of product safety law.[55] However, the fines are significantly higher than in national law, providing an extra incentive for e.g., providers and users to enter into contractual arrangements, such as indemnification clauses, under which the liability for such a fine is borne by the party whose acts or omissions caused it to be imposed. Because the fines will from the outset be harmonized throughout the EU, the question may arise whether passing them on to another party through e.g., an indemnification clause would impermissibly thwart the purpose of the Draft Regulation and thereby be invalid. That is a question of EU law which falls largely within the jurisdiction of the EU Court of Justice and the answer to which will depend on the circumstances of the case.[56] We believe that if the user of a high-risk AI system suddenly becomes a provider due to a substantial modification and a regulator imposes a fine on the new provider, the new provider will want – and in our opinion should be able – to enforce an indemnification clause or otherwise take recourse against the old provider to the extent that the circumstance leading to the imposition of the fine originated from an act or omission by the old provider.

5.3. In the Relationship Between the Provider and a Third-Party

5.3.1 Breach of a Statutory Duty and Protective Scope

23. Since the obligations under the Draft Regulation are intended to address risks not only to health and safety but also to fundamental rights, the interests it seeks to protect and the harm that may occur if those interests are violated are more diverse than we are used to in product safety law.[57] For example, if the lack of human oversight of a self-learning AI system leads to discrimination in the job application process, it is conceivable that the applicant could commence a tort action against the provider of that system based on an infringement of Article 14 of the Draft Regulation, seeking compensation for his/her loss of income as a result of not being hired (pure financial loss). Insofar as national law imposes an actionability requirement regarding the scope of the statutory rule (as the English would call it), *Schutznorm* (as the Germans would call it) or 'relativity' requirement (as the Dutch would call it) in tort actions (in short, the rule or norm that was violated must be intended to protect the injured party against the harm that

55 See for an extensive discussion G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling*, para. 75.

56 See G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling*, para. 172 for questions regarding the nullity of contractual provisions where product safety obligations are harmonized at EU level, but sanctions and remedies are left to the Member States.

57 See Art. R4 (2), second paragraph Annex 1, Decision No. 768/2008/EC (Model Decision), as discussed by, among others, G.M. Veldt *in Europese productnormen en privaatrechtelijke normstelling*, para. 63.

in fact occurred), it is up to the national courts to adjudicate whether that requirement has been met in a particular case.[58] In the example given, the interest protected is the fundamental right to non-discrimination in employment and the loss of income is the harm that may occur from a violation of that right. Since Article 14 refers explicitly to the protection of fundamental rights, we believe a good case can be made that the relatively requirement is met. Of course, this says nothing about whether a causal connection can be established. The Draft Regulation can thus contribute to the enforcement of anti-discrimination rules.

5.3.2. Product liability

24. There is still much uncertainty about the applicability of the current Product Liability Directive to AI. As the public law arm of AI regulation, the Draft Regulation can help shape the product liability rules applicable to AI and the elements of a claim thereunder, but it also raises alignment issues between product liability and product safety. We will explain several bottlenecks in the EU product liability regime as applied to AI, after which we will discuss what the introduction of the Draft Regulation in its current form could mean for product liability claims. We will also address some alignment issues in view of the announced revision of EU product liability law with respect to AI. In our view, good alignment of the Draft Regulation and any new product liability initiatives is crucial for providing a clear, consistent and effective regulatory framework.

25. Under the current Product Liability Directive, product liability is, in short, limited to damage to property (other than the product itself) and damage resulting from death or personal injury caused by a defect in the product. In any case, liability for pure economic loss is left to national law. **Product** is defined, in short, as movables and electricity (Arts 1, 2 and 9). The persons who can be held liable are also strictly demarcated. In order for the directive to apply to standalone AI, a very broad interpretation of the term 'product' is required, because software is not tangible. This broad interpretation is currently uncertain.[59] For embedded AI as referred to in the Draft Regulation, a narrower interpretation of 'product' suffices since embedded AI is integrated into a movable.[60] Insofar as AI is subject to the Product Liability Directive, the evidentiary thresholds for proving a product

58 See G.M. Veldt, *WPNR* 2021, pp 518-521 on the relativity requirement under Dutch law.

59 P. Machnikowsi et al., *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies* (Cambridge – Antwerpen – Portland: Intersentia 2016), p 693 and the underlying country reports.

60 See P. Reusch, 'Produkthaftung nach dem europäisch harmonisierter Produkthaftungsgesetz', in Markus Kaulartz & Tom Braegelmann (eds), Rechtshandbuch Artificial Intelligence und Machine Learning, p 114. See for further examples: Tiago Sergio Cabral, 'Liability and artificial intelligence in the EU: Assessing the adequacy of the current Product Liability Directive', *Maastricht Journal of European and Comparative Law* 2020(5), pp 619-620.

liability claim are lower than those applicable in regular tort actions because far-reaching evidentiary presumptions relating to the existence of a defect are used in various Members States and accepted by the EU Court of Justice.[61] The essential requirements set out in and harmonized standards issued pursuant to the Draft Regulation could in such cases be used to help establish whether an AI system is defective. Violation of the essential requirements or harmonized standards could, for example, justify a presumption that an AI system is defective or perhaps bring about a reversal of the burden of proof on causality.[62] As Koch e.a. have pointed out, a clear and tight regulatory scheme ex ante might improve the victims' chances of success in liability proceedings ex post. At the same time these new techniques might make proof of defectiveness for example more difficult.[63] For medical devices, the MDR enables patients to ask the enforcement authority, in the case of incidents, for information and documentation provided by the manufacturer to the authority, which information the authority will provide to the patient if the authority believes or has reason to believe that the device caused damage (Art. 10(14) MDR). For AI this far-reaching information obligation is (for the time being) missing in the Draft Regulation (see below on the anticipated review of the Product Liability Directive).[64] Such information may be beneficial for the victim to substantiate his claim, violation of statutory duties and/or other duty of care, as well as causation.

26. The concept of damage in the Product Liability Directive is also an important limitation in relation to AI. At least for now, pure economic loss (for example as a result of data leaks or loss of data) – i.e., without personal injury or damage to property – are, on the face of it, not eligible for compensation under that directive.

---

61 ECJ EU 21 Jun. 2017, C-621/15, ECLI:EU:C:2017:484, *W. c.s./Sanofi Pasteur MSD SNC, Caisse primaire d'assurance maladie des Hauts-de-Seine, Carpimko*, and the annotation thereon by G.M. Veldt & A.E.C. Wissink, *NTBR* 2017, pp 253-263.

62 See G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling*, paras 180-188 and 253-255. See critically on presumptions of causation S. Wojtczak & P. Księżak, 'Causation in Civil Law and the Problems of Transparency in AI', *European Review of Private Law* 2021(4), pp 561-582.

63 B.A. Koch et al, *ELI Response of the ELI on the European Commission's Public Consultation on Civil Liability. Adapting Liability Rules to the Digital Age and Artificial Intelligence* (Wien: ELI 2022), p 8. Followed up by B.A. Koch et al, 'Response of the European Law Institute to the Public Consultation on Civil Liability – Adapting Liability Rules to the Digital Age and Artificial Intelligence', 13. *JETL* 2022(1), pp 25-63. We only refer to the original report hereafter.

64 Article 17 of the Market Surveillance Regulation 2019/1020 requires market surveillance authorities to make available to the public any information they deem relevant for the protection of end users. However, the obligation is vague and, according to the second sentence, 'Market surveillance authorities shall respect the principles of confidentiality and of professional and commercial secrecy and shall protect personal data in accordance with Union and national law'.

For these categories of damage, injured parties must still rely on fault-based liability under national law or strict liability interpreted broadly under national law.[65]

27. In this context, it is relevant that on 30 June 2021 the European Commission published an *inception impact assessment* announcing the release of a proposed revision of the Product Liability Directive in the third quarter of 2022. The purpose of the revision is to take into account the challenges that AI poses to product liability.[66] In the run-up to the release of this proposal, several policy papers, expert reports and scientific contributions have been published, from which the following main points for the regulation of AI can be distilled.[67] For each point, we will indicate to what extent there is a connection with the Draft Regulation as the (more) public law counterpart. Although product safety and product liability serve different purposes that may sometimes justify divergence between the two systems, legal experts have long argued for more coherence between the two systems.[68]

---

65 See e.g., for non-contractual liability pursuant to Dutch law T.F.E. Tjong Tjin Tai, *NTHR* 2017, pp 123–132, who considers Dutch law to be very flexible thanks to 'the relatively open standard of care and the absence of limitations as to the types of damage to be compensated' (p 132) and for contractual liability T.J. de Graaf & I.S. Wuisman, in *Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice*, Ch. 14 (forthcoming). For the right to compensation in the event of a breach of the GDPR see further, e.g., T.F. Walree, *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens* (diss. Nijmegen) (Deventer: Wolters Kluwer 2021).

66 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en.

67 The Product Liability Directive has recently been reviewed (COM(2018)246). The review resulted in the establishment of two *expert groups* on 'liability and new technologies'. The New Technologies Formation described this in a 27 Nov. 2019 report titled: 'Expert Group on Liability and New Technologies, New Technologies Formation, Liability for Artificial Intelligence and other emerging digital technologies' (hereinafter the 'Expert Group Report'). Another important document is the White Paper on Artificial Intelligence – A European approach based on excellence and trust (COM(2020) 65. Brussel, 19 Feb. 2021) (hereinafter the 'White Paper') and accompanying Report on the safety and liability implications of artificial intelligence, the Internet of Things and robotics (COM(2020) 64. Brussel, 19 Feb. 2021) (hereinafter the 'EC-Report'). See also the proposal for an AI liability regulation in the European Parliament Resolution of 20 Oct. 2020 with recommendations to the Commission on the civil liability regime for artificial intelligence (2020/2014(INL)), P9_TA(2020)0276 (hereinafter the 'EP Resolution'). For a further discussion of these developments, see the European Law Institute (ELI) Pilot Innovation Paper prepared by Twigg-Flesner containing Guiding Principles for Updating the Product Liability Directive for the Digital Age) (hereinafter the 'ELI Position Paper') and P. Machnikowsi et al., *Product Liability* and Koch e.a. 2022.

68 F. Cafaggi, 'Product safety, private standard-setting and information networks', in F. Cafaggi & H. Muir Watt, *The Regulatory Function of European Private Law* (Cheltenham: Edward Elgar 2009), p 229. See also Principle 2 and 6 ELI Position Paper and, with respect to Belgian law, D. Verhoeven, *Productveiligheid en productaansprakelijkheid* (diss. Antwerpen) (Antwerpen 2017), p 581. See also D. Fairgrieve et al., 'Product Liability Directive', in Machnikowsi et al, *Product Liability*, p 103.

From the point of view of legal certainty, better harmonization and alignment of the two seems to us to be highly desirable wherever possible.

28. Most stakeholders and experts advocate extending the **definition of product** to include AI, which could be done by extending the definition of product to software.[69] An important question is whether in that event a definition of AI would be included in the product liability instrument and whether the definitions in product liability law and product safety law will remain similar or diverge. Revision of the **definition of defect** is also a point of attention, in particular because digital products or product components are not static but are or should be updatable and therefore cannot be judged as to safety only when they are put into circulation.[70] In this context, the producer's defence that the defect did not exist at the time the product was put into circulation also requires further refinement and clarification (Art. 7(b) of the Directive).[71]

29. The desirability of alleviating the **burden of proof** for injured parties is another widely shared view.[72] Such parties often lack sufficient evidence to substantiate their claims. It is expected that this evidence gap will only increase where AI is used, because the technology is often opaque ('*black box effect*').[73] The Expert Group on Liability and New Technologies refers to the situation in which the allegedly liable party refuses to share data with the injured party or has not registered relevant data, to which a presumption of fault or causation could be linked.[74] In our opinion, it would be helpful if changes to the Product Liability Directive on this point are consistent with the recording and logging obligations in

---

69 To include digital elements and digital products, see principle 4 ELI position paper and Koch e.a. 2022, pp 10-14. See also Tiago Sergio Cabral, *Maastricht Journal of European and Comparative Law* 2020, p 621, who pleads for a link with the Consumer Sales Directive.

70 White Paper, pp 15 and 17; the EC-Report, pp 17-18; Principle 6, ELI position paper; Expert Group Report, p 3; Jean-Sébastien Borghetti, 'How can Artificial Intelligence be Defective?', in Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and Internet of Things*, pp 63-76.

71 Tiago Sergio Cabral, *Maastricht Journal of European and Comparative Law* 2020, pp 624-625. See also Marta Santos Silva et al., 'Relevance of Risk-benefit for Assessing Defectiveness of a Product: A Comparative Study of Thirteen European Legal Systems', *ERPL* 2021(1), pp 91-131, para. 99 arguing that 'the gap between common expectations about the safety of devices and their actual safety is growing ... may indicate that there are expectations in society of 100% safety of digital technologies, which any expert would consider unrealistic'. See also Koch e.a. 2022, p 17.

72 See also the inception impact assessment, pp 4-5 and the influence that the logging obligation, among others, has on civil liability under German law Malte Grützmacher, 'Die zivilrechtliche Haftung für KI nach dem Entwurf der geplanten KI-VO Potentielle zivilrechtliche Auswirkungen des geplanten KI-Sicherheitsrechts: ein neues Schutzgesetz i.S.v. § 823 Abs. 2 BGB am Horizont', *Computer und* Recht 2021(7), p 443.

73 White Paper, p 15 and the EC-Report, p 18. Principle 8 ELI position paper. Expert Group Report, p 6, point 15.

74 Expert Group Report, p 7, para. 22 as cited in the EC-Report, pp 17 and 19.

the Draft Regulation and with the currently somewhat unclear requirement in the Draft Regulation that high-risk AI systems be designed and developed in such a way to ensure that 'their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately' (Art. 13(1)), so that injured parties are better able to determine whether the AI system in question was defective. The Expert Group argues for reversing the injured party's burden of proof if logging does not occur or logged data is not shared with the injured party.[75] The Expert Group also argues for reversing the burden of proof on causation, fault or the existence of a defect if certain safety standards designed to protect against harm to the injured party are violated, especially safety standards set out in or adopted pursuant to the Draft Regulation.[76] The Expert Group's position is to some extent in line with existing national evidentiary presumptions and burdens of proof.[77] However, if harmonized evidentiary presumptions or burden of proof reversals are introduced at EU level, greater specificity will be required as to (1) the prerequisites for their application and their precise legal consequences, e.g., what the injured party will still, at a minimum, need to allege and, if necessary, prove,[78] and (2) whether the evidentiary presumptions will be binding on courts and/or rebuttable. Fortunately, there is no support for relaxing the producers' regulatory compliance defence to an extent that compliance with the applicable legislation releases them from liability,[79] since it is precisely in the case of rapidly developing technology that there is a considerable chance that regulation may fall short or lag behind the state of the art.[80] As said, the mirror image of regulatory compliance – liability for violation of product safety law – is left to the Member States. Koch e.a. argue in favour of investigating whether this liability should be further harmonized to

75 Expert Group Report, p 4.

76 Expert Group Report, p 7, paras 24, 26 and 27. Under 26 the Expert Group gives further points of view for the assumption of a presumption of causation in AI. See critically S. Wojtczak & P. Księżak, *ERPL* 2021, pp 577-579 with further suggestions pp 581 et seq.

77 Expert Group Report, pp 21 and 22, and 29 and 30. See also G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling*, paras 182, 328 and 329 and 251 et seq.

78 See Expert Group Report, p 8, para. 25.

79 At present, Art. 7(d) of the Directive contains a limited *regulatory compliance defence*, in the sense that the producer is only released from product liability if compliance with a mandatory government regulation causes the defect. See extensively G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling*, para. 178.

80 G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling*, para. 184; Jan Eichelberger, 'Zivilrechtliche Haftung für KI und smarte Robotik', in Martin Ebers, Christian Heinze, Tina Krügel & Björn Steinrötter (eds), Künstliche Intelligenz und Robotik. Rechtshandbuch, Rn. 18-20. See also Expert Group Report, p 51. An option that combines strict liability with a safe haven in case certain AI-technology was tested in a regulatory sandbox with the aim of fostering innovation, was proposed by J. Truby et al., 'A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications', *EJRR* 2021, pp 1-29. For regulatory sandbox, please see Art. 53 of the Draft AI regulation.

create a level playing field in the EU and we agree this should be done.[81] A right to information from the provider directly or via the authorities (cf. the MDR referred to above) could be incorporated into product liability law, although it should be borne in mind that the injured party would still have to interpret the technical data and would often need the assistance of an expert to do so.

30. It is also argued that the **producer** concept should be adapted to include new actors.[82] In this regard, choices must be made regarding the definitions of those actors and between adherence to strict liability (product liability), fault-based liability (general contractual or non-contractual liability) or vicarious liability. A distinction could also be made based on the degree of risk associated with the product, as under the Draft Regulation. Moreover, it is important to consider whether the introduction of new type of liability, like operator liability for AI, should be placed in a revised product liability instrument or require a separate regime that functions in addition to a revised product liability instrument for situations that are not covered by the latter.[83] We will address the various options that have been considered hereafter.

For example, in its proposal for a separate AI liability regulation in the European Parliament Resolution of 20 October 2020 (hereinafter the 'EP Resolution'), the European Parliament seems to opt for the introduction of strict liability for operators of high-risk AI systems (in short, parties with some form of control over AI).[84] Interestingly, Article 4.3 of the EP Resolution also states that operators are not liable in the event of force majeure which appear somewhat contradictory. For operators of AI systems that do not fall into the high-risk category, the EP Resolution advocates fault-based liability with a reversal of the burden of proof. This would mean that the operator is, in principle, liable for any damage caused by physical or virtual activities, devices or processes driven by the

81 Koch e.a. 2022, p 22.

82 White paper, p 17; Principle 5 ELI position paper.

83 Compare Koch e.a. 2022 who separate revision of the Product Liability Directive from other liability issues in relation to AI.

84 The EP Resolution contains the following definitions in Art. 3, insofar as relevant: '(d) '"operator" means both the front-end operator and the back-end operator, as long as the latter's liability is not already covered by Directive 85/374/EEC; (e) 'front -end operator' means any natural or legal person who exercises a degree of control connected with the operation and functioning of the AI system and benefits from its operation; (f) '"back -end operator" means any natural or legal person who, on a continuous basis, defines the features of the technology and provides data and an essential back-end support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI system.' 'Control' is defined in Art. 3(f). The Expert Group deliberately chooses to leave the term 'operator' rather open, p 41. For a summary of the EP Resolution, see Philipp Etzkorn, 'Die Initiative des EU-Parlaments für eine EU-Verordnung zur zivilrechtlichen Haftung beim Einsatz von KI. Wie sich das EU-Parlament die unionsrechtliche Regelung der zivilrechtlichen Haftung beim Einsatz von KI vorstellt', *Computer & Recht* 2020(11), pp 764–768.

AI system, while subsequently being allowed several defined defences in discharge of liability.[85] A distinction between high- and low-risk AI systems in product liability law would invite discussions that may not be in the injured party's best interest. If this distinction makes it into a product liability proposal, the question will be whether the risk categories in the Draft Regulation and under that proposal are or are not consistent. Koch e.a. argue that an AI-system in practice might be so complex that a fault liability regime might leave certain victims without compensation at all, despite being worthy of protection.[86] Therefore, according to them, for some inherently dangerous categories a strict liability regime should be envisaged. At the same time, high-risk AI systems under Article 3 of the Draft Regulation do not per se qualify as 'inherently dangerous' justifying a strict liability regime.[87] Moreover, as we already pointed out, the protected interests under the Draft Regulation (which include privacy and protection against loss of data) and its product liability counterpart differ. As long as this is the case, the future risk categories and content thereof under both regimes will differ as well. Although there is a clear difference in function between the Draft Regulation (prevention) and product liability legislation (providing compensation), further alignment of both EU-regimes is necessary to achieve legal certainty and an effective application of both regimes in our opinion. It is unfortunate that an EC proposal regarding AI-liability and/or product liability has not been presented yet, which makes it harder to make adjustments at an early stage in the Draft Regulation regarding desirable parallels or explicit deviations between both.

The choice of an open concept such as operator in the Expert Group's Report and the EP Resolution in relation to strict liability is based partly on a desire to be aligned with the Member States' national strict liability rules, which focus on the liable party's control over the risk and enjoyment of the benefits.[88] Koch e.a. plea for a presumed breach of a duty of care in all other cases than inherently dangerous AI, because it provides an incentive to develop safeguards as to the potential harms, and to implement systems which may explain the processes that led to a given loss. Moreover, providers are in a better position to prevent the risks from materializing, which makes them superior risk bearers from a law and economics perspective. And such a regime is sufficiently dynamic to be adapted to the evolution of technology.[89] If there is more than one operator, the Expert Group

85 Article 8 (1) and (2) of the EP Resolution. See also White Paper, pp 18 ff. cf. Expert Group Report, p 42.

86 Koch e.a. 2022, p 28.

87 Koch e.a. 2022, p 28.

88 Expert Group Report, p 41. See also E. Karner, B.A. Koch & M.A. Geistfeld, *Comparative law study on civil liability for artificial intelligence* for an overview of the currently applicable law on liability for AI in the various Member States.

89 Since it allows the defendant to prove that it had done everything that could be reasonably expected given the current status of knowledge and scientific evolution in the field at the time, Koch e.a.

makes a distinction between the liability of front-end and back-end operators based on their respective degrees of control over the risk. In contrast, the EP Resolution provides that they are to be jointly and several liable, whereby their respective degrees of control are only relevant for recourse claims against each other.[90] Here again, the technical documentation, the logs and the required transparency will provide crucial information on the degrees of control.[91]

All in all, operator liability at EU-level is a new concept that deviates from the original principles underlying personal scope of the product liability directive. Therefore, it might be wise to separate operator liability from any proposal revising the Product Liability Directive.[92] A separation of both instruments would allow for a more risk-based approach with regard to operator liability for AI, as has been done in the Draft Regulation, and the use of a general regime for 'regular' product liability. Moreover, the liability for AI being a sensitive topic, separation of both could prevent a necessary revision of the product liability directive getting stuck in the legislative process because of controversies regarding the AI-regime.

31. Koch e.a. point also at the option put forward in the Expert Report, of introducing vicarious liability in addition to the already existing vicarious liability regimes in the various Member States. Where the use of a human auxiliary would give rise to the liability of a principal, the use of a digital technology tool instead should not allow the principal to avoid liability but should give rise to such liability in the same way. We believe this is questionable seeing that liability for the use of digital technology can, at least in a contractual setting, just as well (if not better) be equated with vicarious liability for using an unsuitable object in the performance of contractual obligations.[93] However, as Koch e.a. rightly contend, a 'one size fits all' solution is not suitable for 'AI technology' as such because its applications and risks are so diverse. [94]

32. Another point of debate is amplifying the notion of '**damage**' and the question whether it should include pure economic loss. The European Law Institute (ELI) argues for a more modest extension, limited to damage to digital elements and data. The European Parliament – which favoured a separate AI liability

---

2022, pp 28 and 29. See with regard to a further law & economic analysis also M. Kovac, 'Autonomous Artificial Intelligence and Uncontemplated Hazards: Towards the Optimal Regulatory Framework', 13. *EJRR* 2022, pp. 94–113.

90 Expert Group Report, pp 6, 41 and 42 and Koch e.a. 2022, p 18. See also recitals 12 and 13 of the EP Resolution and recitals 9 and 10 as well as Art. 11 of the Annex thereto.

91 Article 10.2 of the Annex to the EP Resolution even makes it explicit that log data can be used for this purpose.

92 Compare Koch 2022.

93 T.J. de Graaf & I.S. Wuisman, in *Law and Artificial Intelligence. Regulating AI and Applying AI in Legal* Practice, Ch. 14.

94 Koch 2022, p 29 with reference to the Expert Group Report, pp 45–46.

regulation in addition to the Product Liability Directive – advocates an extension applicable only to operators of high-risk AI systems, which may be liable 'up to a maximum amount of EUR one million in the event of significant immaterial harm that results in a verifiable economic loss or of damage caused to property, including when several items of property of an affected person were damaged as a result of a single operation of a single high-risk AI-system'.[95] Here too, the question is whether the interests protected by the public law Draft Regulation will also be protected at EU level in a private law counterpart such as an amended or new product liability directive or new product liability regulation, or whether it will remain necessary to rely on national law for private law protection.

33. Those who advocate an extension of the concept of producer also argue for the harmonization of their **rights of recourse,** enabling liable parties to take recourse under mandatory or non-mandatory EU or national law against the actor who actually caused or was responsible for the damage,[96] and also against insurance companies or compensation funds.[97] It seems to us that a new product liability directive or regulation is indeed the right place to introduce, for example, a duty to provide adequate recourse or security, and not product safety law, as was previously the case under the MDR.[98] In our view, some guidance as to the applicable amounts and types of security is necessary. Moreover, if a differentiation in risk categories – resembling the Draft Regulation – would also make it to the product liability proposal(s), a corresponding differentiation between types of recourse and amounts would in our opinion be obvious. Again, clear alignment of the public law and private law counter parts in that is necessary.

---

95 Principle 7 ELI position paper and EP Resolution, Annex 1(B), recital 16 and Art. 5(1)(b). For traditional personal injury cases the European Parliament proposes a cap of EUR 2 million, Art. 5.1 (a).

96 Principle 10, ELI position paper. See also the comments under principle 5, concerning the addition of new liable parties and under principle 2, concerning transactional losses. See also Expert Group Report, pp 57 and 58, which advocates the introduction of harmonized rules on alternative causation and joint and several liability in relation to third parties, but leaves the issue of recourse among the liable parties to national law.

97 Georg Borges, 'New Liability Concepts: the Potential of Insurance and Compensation Funds', in Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and Internet of Things*, pp 145–163.

98 Principle 3, ELI position paper. See also the duty to provide sufficient financial coverage for their potential liability under the Product Liability Directive, which currently already applies to producers of medical devices under Art. 10(16) of Regulation (EU) 2017/745 (Medical Devices), as discussed in G.M. Veldt, *Europese productnormen en privaatrechtelijke normstelling*, para. 52. Incidentally, this does not affect the discussions on the introduction of compulsory (additional) first or third party insurances, the degree of regulation of their coverage and the various costs involved, see further Expert Group Report, p 30 and recital 25 of the EP Resolution. See for a critical view on compulsory insurance; M. Faure & S. Li, 'Artificial intelligence and (Compulsory) Insurance', 13. *JETL* 2022(1), pp 1–24.

6. Conclusion

34. The Draft Regulation in its current form has a broad and also extraterritorial scope. It contains too broad a definition of AI as a result of which it applies in many cases where it should not. With regard to high-risk AI systems, the proposal imposes a number of burdensome and seemingly unrealistic requirements on the providers of such systems with respect to the data used (which must be free of errors and complete) and the system's transparency (which might prohibit the use of black box AI systems). The Draft Regulation will supplement rather than replace existing product safety, data protection, consumer protection and non-discrimination legislation. This makes it difficult for those who need to abide to determine which obligations to abide by and how these instruments relate to each other.

35. For products in sectors subject to old-approach EU product safety legislation (e.g., self-driving cars using AI), the applicability of the Draft Regulation is confusing and should be made clearer. Only close inspection reveals that it is requirements are not directly applicable, but must be 'taken into account' when that legislation is amended or refined through delegated or implementing acts. In relation to products in sectors covered by new-approach EU product safety legislation, such as machinery and medical devices, many of the requirements of the Draft Regulation apply only to AI systems that are subject to a conformity assessment by a notified body under that legislation. In such cases the notified body will, as part of its conformity assessment, check to ensure that the essential requirements (high-level requirements) of both the Draft Regulation and the harmonized standards (detailed product standards and technical specifications) drawn up pursuant to it are met. Since a conformity assessment by a notified body is often not prescribed, the scope of the Draft Regulation is less extensive than may appear at first sight. However, as our wood planning example has shown, in practice a product which was originally not required to undergo a third-party conformity assessment (but only an internal conformity assessment) may, once AI is added, very well be subject to such assessment and therefore the requirements of the Draft Regulation. In a sense, the idea that the Draft Regulation does not apply to self-certified products gives a false sense of security because in practice the Draft Regulation may very well apply. This may lead to unintended non-compliance. In order to counter this, we expect that as time goes on, more sector-specific EU new-approach product safety legislation will be adapted to extend the scope of the Draft Regulation by requiring a third-party conformity assessment in the case of all high-risk products, as has already happened under the proposal for a machinery regulation. As a result, manufacturers which currently perform their own internal conformity assessments will ultimately be subject to a third-party conformity assessment. This may be desirable from a protection point of view, but in practice it will lead to extra complexity and costs for manufacturers.

36. It is to be expected that, even in amended form, the Draft Regulation will have far-reaching consequences for actors in the value chain. Non-predetermined substantial modifications require a new third-party conformity assessment. It is unclear when this is considered to be the case. If this is also the case if an AI system changes itself, manufacturers may try to predetermine as many possible modifications as they can think of in order to avoid future costly conformity assessments, thereby defeating the Draft Regulation's purpose. Or users whose training or use leads to substantial modifications may suddenly become responsible for compliance and a new third-party conformity assessment, something they most likely did not realize and therefore do not do, again defeating the Draft Regulation's purpose. The EP's proposed amendment to allow users to contract out of this requires further thought. Although by its nature a public law instrument, a failure to comply with the requirements in the Draft Regulation can have consequences for private law liability in tort.

37. The product safety obligations laid down in the Draft Regulation may form the basis of a claim based on violation of a statutory duty or may colour the private law duties of care resting on providers and users. Where these parties depend on the developer of the AI system to fulfil their product safety obligations and have little or no influence on damage caused by the product's use, it would be prudent for them to ensure – contractually or by law – that the developer is required (1) to cooperate in the performance of those obligations (including those on risk and incident reporting and on keeping logs) and, where appropriate, (2) to indemnify the manufacturer or user for any sanctions (in particular fines) and private law remedies imposed.

38. Moreover, we have shown that in light of the upcoming revision of the product liability directive, any alignment between this private law proposal and the Draft regulation as its public law counterpart, is necessary and requires careful consideration. Further harmonization of presumptions of proof in light of the Draft Regulation and other product safety law should be considered. Also, the suggested operator liability and differentiation in risk categories needs further overthinking and alignment. Introduction of this could require other adjustments for example regarding a duty to provide adequate security. In this contribution we have discussed the interfaces and possible alignment issues between the public-law and private-law domains. Time will tell how all the various open issues and competing standpoints will be resolved in the final version of the Draft Regulation and any proposals regarding the Product Liability Directive and/or liability for AI.