The EU Commission's Proposals for Regulation of Artificial Intelligence – Product safety and liability, A General Overview

Gerald Spindler

The EU Commission's new proposal for a regulation on artificial intelligence is the world's first attempt to get a legislative grip on the phenomenon of AI. The draft uses classic regulatory structures of product safety law to get the risks of AI under control using technical standards, certifications, risk, and quality management systems, which the Commission locates primarily in threats to fundamental rights. The article provides a first overview and assessment of the draft.

The second part is dedicated to the new proposals of the EU Commission regarding product liability and liability for AI-systems.

A. Part I: The Proposal for a Regulation of Artificial Intelligence (AI-Act-P)

I. Introduction

Artificial intelligence (AI) has emerged as one of the most important components of digitalization in recent years, alongside the platform economy and blockchain technology. However, the use of AI can have beneficial effects as well as evoke considerable risks and dangers: Well-known examples include the use of AI in the area of social scoring to filter out disliked minorities, or the creation of movement

DOI: https://doi.org/10.17875/gup2023-2494

profiles with the help of telemetric facial recognition[1], or in the area of opinion-forming platforms that evaluate and sort certain content and then present it to the user in an appropriately "prepared" form (so-called "content curation"), resulting in the well-known phenomenon of "echo chambers" arises[2]. The risks to the exercise of fundamental online rights are therefore manifold, ranging from data protection and freedom of expression to possible discrimination, for example through biased training data.

It is therefore not surprising that numerous expert panels and commissions were soon convened at the legal policy level to address the ethical and legal principles of AI and to make corresponding proposals. The current proposal of the *EU Commission*[3] results from the consultations on the Commission's White Paper[4] and explicitly incorporates the proposals of the European Parliament on ethical principles for AI[5], as well as the proposals of the Council of 21.10.2020[6] and the *High-Level Expert Group on AI*[7].

With the proposal for an AI Regulation, the *EU Commission* is pursuing a *risk-based horizontal approach* in the area of product safety law that relates to the use of AI in general and does not proceed on a sector-specific basis (as for example in the

[1] For basic information on face recognition see Andreas Kulick, "„Höchstpersönliches Merkmal" – Verfassungsrechtliche Maßstäbe der Gesichtserkennung," *NVwZ,* (2020): 1622; Jan Mysegades, "Keine staatliche Gesichtserkennung ohne Spezial-Rechtsgrundlage," *NVwZ,* (2020): 852; Amélie P. Heldt, "Gesichtserkennung: Schlüssel oder Spitzel? Einsatz intelligenter Gesichtserfassungssysteme im öffentlichen Raum," *MMR,* (2019): 285.

[2] For basic information on "echo chambers" see Boris P. Paal, Moritz Hennemann, "Meinungsbildung im digitalen Zeitalter Regulierungsinstrumente für einen gefährdungsadäquaten Rechtsrahmen," *JZ,* (2017): 641; instructive on their emergence: Josef Drexl, "Economic Efficiency Versus Democracy: On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Post-Truth Politics" *Max Planck Institute for Innovation and Competition Research Paper,* No. 16-16 5, (2016), accessed October 31, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881191; in detail on the connected harm for the plurarity of opinions: Josef Drexl, "Bedrohung der Meinungsvielfalt durch Algorithmen," *ZUM,* (2017): 529.

[3] Commission, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts", COM (2021) 206 final, April 21, 2021, accessed October 31, 2022, https://ec.europa.eu/newsroom/dae/redirection/document/75788, cited as AI-Act-P.

[4] Commission, "White Paper on Artificial Intelligence - A European approach to excellence and Trust", COM (2020) 65 final, 19 February 2020.

[5] Commission, "European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL)", [2021] OJ C 404/63.

[6] Council of the European Union, "Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change", [2020] OJ C 202, 11481/20.

[7] High-Level Expert Group (HLEG), "Ethics Guidelines for Trustworthy AI" (2019); HLEG, "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment" (2020).

product safety law regulations or directives,). The AI Regulation proposal is intended to be explicitly open to the future and able to consider new developments[8].

Regarding the equally much-discussed liability law[9] the focus lies on the introduction of a type of causal liability or strict liability, as proposed by the *Expert Group on Liability and New Technologies*[10] and partially taken up by the *European Parliament* in its resolution of 5.10.2020[11]. The Commission has just recently published two new proposals on AI liability and on a reform of the Product Liability, which will be dealt separately.

The AI-Act-P, on the other hand, is limited to the obligations and prohibitions described and therefore primarily follows a product safety law approach; nevertheless, if the AI-Act-P is adopted it will also have an impact on national liability law, in Germany for example via Section 823 (2) BGB,[12] even if the proposal for the introduction of causal liability, announced for the second half of 2021, is also implemented.[13]

Since various member states, including Germany, are considering implementing an AI strategy, the *EU Commission* has explicitly chosen the instrument of a regulation to counteract fragmentation within the EU[14] – which is in line with the basic approach in the context of product safety.

---

[8] Commission, Explanatory Memorandum, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts", COM (2021) 206 final, April 21, 2021, accessed October 31, 2022, 3, https://ec.europa.eu/newsroom/dae/redirection/document/75788

[9] Gerald Spindler, «823 BGB», in *BeckOGK,* ed. Beate Gsell et al. (München: C.H. Beck, 2022) paras 739 ff.; Herbert Zech, «Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung? », in *Verhandlungen des 73. Deutschen Juristentages,* ed. Ständige Deputation des Deutschen Juristentages (München: Beck, 2020), Vol. I expert opinion, Part A 11, A 87 ff.; Gerhard Wagner, "Produkthaftung für autonome Systeme," [2017] 217 *AcP* (2017): 217, 707 ff.; Gerhard Wagner, "Verantwortlichkeit im Zeichen digitaler Techniken," *VersR* (2020): 717, 724 ff.; Gerhard Wagner, «§ 823 BGB», in *Münchener Kommentar zum Bürgerlichen Gesetzbuch,* ed. Franz Jürgen Säcker, Roland Ricecker, Hartmut Oetker, Bettina Limperg, 8th edn. (München: C.H. Beck, 2020) paras 789 ff.; Maik Thöne, *Autonome Systeme und deliktsche Haftung* (Tübingen: Mohr Siebeck, 2020), passim.

[10] Expert Group on Liability and New Technologies – New Technologies Foundation, "Liability for Artificial Intelligence and other emerging digital technologies", November 27, 2019, accessed November 01, 2022, https://op.europa.eu/de/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1.

[11] Commission, Committee on Legal Affairs, "European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))", [2020] OJ C 404/107.

[12] BGB is an abbreviation for "Bürgerliches Gesetzbuch", which is the German Civil Code.

[13] See below A. XIV.

[14] Explanatory Memorandum, (n 8), 7.

II. The Basic Approach: Risk-Based with Regulation for High-Risk AI

Among various possibilities, the *EU Commission* has come out firmly in favour of a risk-based approach,[15] which contains mandatory regulations only for high-risk AI systems, but leaves it at moderate obligations and a *code-of-conduct concept* for other AI systems.[16] In this context, the AI-Act-P explicitly extends its scope of application to providers respectively operators located outside the EU.[17] The declared goal of regulating high-risk AI is to guarantee the fundamental rights of affected users, in particular the right of freedom of expression, non-discrimination, and fundamental data protection rights.[18] The central element of monitoring the requirements for high-risk AI systems is the product safety approach of conformity assessment on *technical standards*, accompanied by a *presumption of conformity*, which, however, also allows other alternatives, whereby on the one hand the EU Commission wants to ensure necessary flexibility and on the other hand wants to prevent overloading the supervisory authorities.[19]

In order to enforce the obligations of high-risk AI, the *EU Commission* wants to create a registration obligation for so-called *stand-alone AI* and thus an EU-wide database, whereby the activities of the AI can be monitored by supervisory authorities or other third parties with regard to compliance with the obligations, in particular the protection of the fundamental rights concerned.[20] At the same time, this rejects the demand for prior authorization under public law. [21]

This approach is flanked by obligations of the AI operators to inform the monitoring authorities about serious incidents or malfunctions of the AI that endanger fundamental rights; the corresponding information from the monitoring authorities is then to be evaluated by the *EU Commission* for the purpose of market analysis and assessment.[22]

Within this framework, the AI-Act-P also wants to provide facilitations for small and medium-sized enterprises (SMEs), for example by establishing "regulatory sandboxes" or facilitating the conformity assessment of AI systems.[23]

---

[15] In this direction already Mario Martini, *Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz* (Heidelberg: Springer, 2019), 226 ff.

[16] Explanatory Memorandum, (n 8), 9.

[17] See below A. III 3.

[18] Explanatory Memorandum, (n 8), 11. The memorandum lists numerous other fundamental rights affected, up to and including environmental protection.

[19] Explanatory Memorandum, (n 8),14.

[20] Explanatory Memorandum, (n 8), 11.

[21] See for this e.g. Datenethikkommission, "Gutachten der Datenethikkommission der Bundesregierung", (2019): 195, 207 f., accessed November 01, 2022, https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.html;jsessionid=FF71C19934371EB93FE4A14E4C67E962.1_cid334?nn=11678504.

[22] Explanatory Memorandum, (n 8), 11.

[23] Explanatory Memorandum, (n 8), 10.

III. Scope of Application

1. Definition of AI

The definition of AI in Art. 3 No. 1 AI-Act-P already shows the broad scope of application that the AI-Act-P aims at. According to this definition, an AI system is software that uses techniques or approaches described in Annex I and that can produce certain results, such as recommendations, or influences its environment by making decisions, depending on human-set goals. Annex I to Art. 3 No. 1 AI-Act-P lists *machine learning* including *deep learning*, knowledge-based approaches including expert systems, as well as statistical approaches, search and optimization methods. In this way, the *EU Commission* wants to use a definition that is as technologically neutral and future-proof as possible, which is open to newer developments through possible adaptations of Annex I, for which the *EU Commission* is authorized under Art. 4, 73 of the AI-Act-P to issue delegated acts for updating Annex I. However, it is striking from the outset that characteristic elements of AI, such as the *unpredictability of its behaviour* and the *Black-Box-Effect*, are not mentioned at all, so that deterministic software and even normal expert systems are covered, i.e., a much broader area is addressed than was used in the definition of the *High Level Expert Group on AI*.[24]

The area of data essential for AI is also outlined: Art. 3 No. 29 AI-Act-P defines the term *training data* as data with which the AI system fills in the learning parameters including the emphasis within the neuronal networks, while *validation data* according to Art. 3 No. 30 AI-Act-P are data that serve to adjust (*tuning)* the non-learnable parameters and the learning process as such,[25] whereby the *validation data* can also be part of the *training data*. Finally, this is supplemented by the definition of *test data* according to Art. 3 No. 31 AI-Act-P, which is intended to enable an independent assessment of the trained and validated AI system before it is placed on the market or operated.[26]

The AI-Act-P also focuses on the definitions of biometric identification AI, e.g. in Article 3 No. 36 of the AI-Act-P, which defines a "remote biometric identification system" as any AI that aims to identify persons based on their biometric data, in particular facial recognition, by comparing them to a database, without the user

[24] Cf. The definition of the High Level Expert Group on AI (AI HLEG), *Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete. Für die Zwecke der Gruppe entwickelte Definition* (Brussels: European Commission, 2018) 6; similar Zech, (n 9), A 20.

[25] See also Annalyn Ng and Kenneth Soo, *Data Science – was ist das eigentlich?!* (Berlin: Springer, 2018), 16 ff.

[26] See to the definition of testdata also Claudia Niederée, Wofgang Nejdl, «§ 2 Technische Grundlagen der KI», in *Rechtshandbuch Künstliche Intelligenz und Robotik,* ed. Martin Ebers et al. (München: C.H. Beck, 2020) para 31.

of the AI knowing in advance whether the person in question is present and can be identified.

Rather en passant, however, the AI-Act-P makes another important distinction, namely between AI systems integrated into products (*"embedded"* AI systems) and those that function so to speak "alone" without such an integration, i.e. essentially as software or based in a cloud (*"stand-alone"* AI systems). While for the "embedded" AI systems the conformity assessment procedures are and remain relevant, the AI-Act-P for the first time subjects all software ("stand-alone" AI systems) to a CE procedure in a horizontal approach, however only based on internal controls, but combined with a registration obligation in databases.[27]

2. Regulatory addressees

The addressees of the AI-Act-P are, on the one hand, all *manufacturers* or *operators* of AI systems, including those who only market or operate an AI system under their name or trademark, irrespective of whether this is done in return for payment or free of charge, Art. 3 No. 2 AI-Act-P. It is noteworthy here that not even the disclosure of data, as provided for in Art. 3 (1) of the DID Directive, [28] is required to open the scope of application of the AI-Act-P. In this context, not only *private operators* of AI systems are covered, but also explicitly public authorities, Art. 3 No. 2 AI-Act-P. Open source systems are thus not excluded from the AI-Act-P, but are fully subject to its requirements. Both providers and operators are covered as "operators".

On the other hand, users of AI systems are also covered by the regulations if they use the AI for professional purposes, Art. 3 Nr. 3 AI-Act-P.

A distinction must be made between those affected by the AI systems, the *"AI subjects"*, who are subject to the influence of the AI systems in the form of recommendations or measures taken by the AI systems.

3. International Scope

Art. 2 (1) AI-Act-P declares all those who place AI systems on the market or put them into operation in the EU to be the addressees of the AI-Act-P, even if they are based outside the EU. Thus, the AI-Act-P partially goes beyond traditional product safety law, which in these cases subjects importers to the regulations of EU law, such as Art. 2 e) ii) of the General Product Safety Directive.[29]

Users, on the other hand, are only to be subject to the obligations under Article 2 (1) (b) AI-Act-P if they are based in the EU. However, if the result of an AI system

[27] See in detail below A VIII.3.

[28] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1.

[29] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety [2002] OJ L 11/4.

is used within the EU, not only operators but also users located outside the EU are subject to the AI-Act-P, Art. 2 (1) c) AI-Act-P.

4. Relationship with other EU Legal Acts

a) Relationship with GDPR

The GDPR shall remain unaffected regarding its regulations or be supplemented by the AI-Act-P,[30] here especially in the area of *training data*. These are one of the central problem points within technology regulation, as they form the basis of many AI applications.[31] Especially for *machine learning* techniques, the *training data* have a dominating influence on the development of the AI, so that a legislative quality control is indispensable with regard to this data.[32] Otherwise, undesirable consequences such as the development of discriminatory algorithms may occur.[33] Currently, the use of *training data* can only be controlled in a very rudimentary way by Art. 5 (1) d) GDPR, which requires a certain level of quality assurance with regard to the data used. However, since in many cases synthetic or at least anonymized *training data* is used, it often does not fall within the scope of the GDPR.[34]

In particular, the AI-Act-P also affects Art. 22 of the GDPR, which sets out requirements for *automated decision-making* based on personal data. The AI-Act-P also contains a number of breaches or mitigations of the GDPR, for example with regard to the *purpose limitation principle* for AI training or in the area of *"regulatory sandboxes"*.[35] In order to enable high-quality data sets and AI based on them, the use and processing of *sensitive data* within the meaning of the GDPR is also permitted for certain providers, see Art. 10 (5) AI-Act-P; for example, the *EU Commission* states in Recital 45 AI-Act-P that access to relevant health data for the training of AI in the health sector is to be opened up via the "European Health Data Space", although this is to be subject to institutional supervision and compliance with specific security provisions.[36] In this respect, there is a further restriction of the general prohibition of processing in Art. 9 GDPR. An exception to the strict *purpose limitation*

[30] Explanatory Memorandum, (n 8), 4.

[31] Philipp Hacker, "Europäische und nationale Regulierung von Künstlicher Intelligenz," *NJW,* (2020): 2142, 2145; Philipp Hacker, "A Legal Framework for AI Training Data," (working paper, 2020), accessed November 01, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3556598.

[32] Like this now also Commission, Explanatory Memorandum, (n 8), recital 44, which above all points out that the data used can also be a source of unintentional discrimination, so that this 1st he point to start with.

[33] Explanatory Memorandum, (n 8), recital 44.

[34] In detail to this Manon *Oostveen, "Identifiability and the applicability of data protection to big date," International Data Privacy Law,* (2016): 6, 299, 307, doi:10.1093/idpl/ipw012.

[35] See to this below A. IX.

[36] Before processing it is explicitly not necessary to anonymize the dataset if this would significantly impair the pursued purpose, cf. Art 10 (5) AI-Act-P.

principle under Art. 5 (1) b) GDPR - according to which personal data may only be collected for *specified, explicit and legitimate purposes* and may not be further processed in a manner incompatible with these purposes - is made by the AI-Act-P with regard to the (further) processing of these data in *"regulatory sandboxes"* to the effect that such processing is permitted if it serves the development and testing of innovative AI systems, cf. Art. 54 Abs. 1 (a) AI-Act-P.[37]

b) Relationship to Other Product Safety Acts, in Particular Proposal for a Machinery Regulation

Since the proposal for an AI-Act ultimately follows product safety law approaches, the question of the relationship to sector-specific regulations is obvious. The *EU Commission* wants to view the AI-Act as a horizontal supplement to all regulations based on *the New Legislative Framework (NLF)*, whereby these can provide for supplementary safety requirements with regard to the specific embedding of AI in the respective product.[38]

Accordingly, the AI-Act-P, with the exception of its Art. 84, does not apply to product safety requirements according to the *"Old Approach"*, which contains precise requirements, for example in the area of aircraft or motor vehicles.[39] Accordingly, the AI-Act-P only applies to a limited extent to the following regulations or directives: (a) Regulation (EG) 300/2008[40]; (b) Regulation (EU) 167/2013[41]; (c) Regulation (EU) 168/2013[42]; (d) Directive 2014/90/EU[43]; (e) Directive (EU) 2016/797[44];

[37] In detail to "regulatory sandboxes" see below A. IX.
[38] Explanatory Memorandum, (n 8), 4.
[39] Explanatory Memorandum, (n 8), 4.
[40] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 [2008] OJ L 97/72.
[41] Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles [2013] OJ L 60/1.
[42] Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles [2013] OJ L 60/52.
[43] Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC [2014] OJ L 257/146.
[44] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (*recast*) [2016] OJ L 138/44.

(f) Regulation (EU) 2018/858[45]; (g) Regulation (EU) 2018/1139[46]; (h) Regulation (EU) 2019/2144[47].

IV. Basic Ban on Certain AI Applications

The AI-Act-P takes a risk-based approach that distinguishes between unacceptable risks, high risks, and low or minimal risks of AI applications. Certain AI applications are subject to an unconditional ban, be-cause those AI applications are considered to create risks that are no longer acceptable:

1. Procedures for Influencing (unconscious) behaviour

A first group can be summarized according to Art. 5 (1) a), b) AI-Act-P as a prohibition of influencing the unconscious behaviour of people, which, however, according to Art. 5 (1) AI-Act-P is limited to causing physical or mental harm. Art. 5 (1) (b) AI-Act-P specifies this again regarding the exploitation of specific vulnerable groups such as persons who are physically or mentally disadvantaged due to their age. Article 5 (1) (a), (b) AI-Act-P thus specifies Article 8 and 9 of the Unfair Commercial Practice Directive.[48] of already forbidden manipulations.[49]

---

[45] 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 and (EC) No 595/2009 and repealing Directive 2007/46/EC [2018] OJ L 151/1.

[46] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 [2018] OJ L 212/1.

[47] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 [2019] OJ L 325/1.

[48] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ L 149/22.

[49] In detail to this Benjamin Raue, «§ 4a UWG», in *Münchener Kommentar zum Lauterkeitsrecht,* ed. by Peter W. Heermann and Jochen Schlingloff, 3rd edn. (München: C.H. Beck, 2020) paras 161; Horst-Peter Götting, «§ 4a UWG», in *UWG Handkommentar,* ed. by Horst-Peter Götting, Axel Nordemann,

2. Social Scoring

Another central concern of the Commission's proposal is the prohibition of *"social scoring"* under Art. 5 (1) (c) AI-Act-P, which assesses the trustworthiness of natural persons based on their social behaviour or personal characteristics.[50] The prohibition is directed only at public or governmental bodies, not at private operators. In addition, the prohibition is limited to impairments of these individuals in social contexts unrelated to those in which the data was collected, alternatively, to impairments or harm to those individuals in ways that are not justified or disproportionate to the social behaviour.

In this way, the AI-Act-P indirectly restricts the ban on *social scoring* by referring to the balancing of interests, thereby creating a considerable degree of legal uncertainty.

3. Biometric Recognition by AI

The AI-Act-P pays special attention to biometric identification systems in publicly accessible places – which has already led to corresponding criticism regarding a too open approach; the main criticism is that the current draft would enable mass surveillance in public spaces.[51] Article 5 (4) of the AI-Act-P contains an opening clause for Member States to decide on the admissibility of such systems under the conditions set out in Article 5 (1) (d), (2) and (4) of the AI-Act-P. Article 5 (1) (d) of the AI-Act-P prohibits in principle the use of such systems for law enforcement purposes, but allows their use for certain purposes which are likely to soften the prohibition, in particular for the search for possible victims of crime, for criminal prosecution and for purposes of ensuring the safety of life and limb of natural persons, including the prevention of acts of terrorism. It is true that Article 5 (2) of the AI-

3rd edn. (Baden-Baden: Nomos, 2016) paras 12 ff.; Ruth Janal, «§ 4a UWG», in *BeckOK IT-Recht,* ed. by Georg Borges and Marc Hilber, 7th edn. (München: C.H. Beck, 2022) para 6; Olaf Sosnitza, «§ 4a UWG», in *BeckOK IT-Recht,* ed. by Ansgar Ohly, Olaf Sosnitza, 7th edn. (München: Beck, 2016) paras 35 ff.

[50] See for this Niklas Maamar, "Eine europäische Perspektive auf Verbraucher-Scores zwischen Big Data und Big Brother," *CR,* (2018): 820, 821; Philipp Hacker, "Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht," *ZfPW*, (2019): 148, 155; Isabell Conrad, Dominik Hausen, «§ 36 Datenschutz im Internet», in *Handbuch IT- und Datenschutzrecht,* ed. Astrid Auer-Reinsdorff and Isabell Conrad, 3rd edn. (München: C.H. Beck, 2019), 244; Ulrich Hoffrage and Julian N. Marewski, «Social Scoring als Mensch-System-Interaktion», in *Social Credit Rating,* ed. by Oliver Everling (Wiesbaden: Springer Gabler, 2020), 305-16; Uwe Hartwig, Stefanie Ernst and Felizitas Pokora, "Social Scoring: Evaluation qualifizierender Beschäftigung,"Hans-Böckler-Foundation, *WSI-- Mitteilungen*, (2008): 267, 273; see also Datenethikkommission, (n 21), 99, 106.

[51] Like this it is mentioned on twitter by vice-president of the Parliament Nicola Beer, accessed November 02, 2022, https://twitter.com/nicolabeerfdp/status/1384910602485829633?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Etweet; sceptical also Member of the Parliament Patrick Beyer, who is worried about an extensive biometrical mass surveillance, interview from April 21, 2021, accessed November 03, 2022, https://www.tagesschau.de/wirtschaft/technologie/eu-gesetzentwurf-kuenstliche-intelligenz-ki-101.html.

Act-P attempts to strike further stakes in the balancing of interests by also taking into account the extent and likelihood of damage if such a system were not used, as well as the impairment of fundamental rights. However, it should not be overlooked that the relatively far-reaching opening clauses open the door to biometric recognition.

Furthermore, Art. 5 (2) sentence 2 AI-Act-P requires compliance with time, location and personal restrictions, including corresponding warranties (see also recitals 19, 20, 21 AI-Act-P); this refers in particular to the *purpose limitation* (Art. 5 (1) b) GDPR) and *data erasure obligations* (Art. 5 (1) e) GDPR), which already follow from the GDPR. Article 5 (3) of the AI-Act-P additionally safeguards this by requiring a prior decision by a court or an independent authority, except in urgent cases for which the decision can still be obtained retrospectively.

V. High-Risk AI Applications

1. Definition

For the definition of high-risk AI applications, the AI-Act-P uses a two-fold approach:

- On the one hand, the AI-Act-P focuses on the use of AI systems as safety-relevant elements in products subject to product safety law,[52] in particular conformity assessment procedures, and
- on the other hand for stand-alone AI systems on an extensive Annex II.[53] For both criteria, it is the intended use that matters, not just the specific function in which the AI system is used.

The first group of product safety requirements according to Art. 6 (1) b) Annex II AI-Act-P is characterized by a broad spectrum of directives and regulations, all of which are based on the *New Legislative Framework*, i.e. the conformity assessment procedures, beginning with the (also revised) Machinery Regulation[54] through the

[52] This, among other things, to ensure that only safe products circulate on the internal market; whereby this safety in the digital age should also be guaranteed with regard to all digital components such as AI, cf. recital 28 AI-Act-P.

[53] For their classification as high-risk AI, it is particularly relevant in accordance to their intended use, whether they pose a high risk to the health, safety or fundamental rights of Union citizens, taking into account both the severity of the potential harm and the likelihood of its occurrence, cf. recital 32 AI-Act-P.

[54] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery and amending Directive 95/16/EC [2006] OJ L 157/24.

Elevator-Directive[55] to the medical product regulations[56]. In addition, however, AI applications as safety components in product safety regulations that do not follow the conformity assessment procedure are also covered under Art. 6 (1) a), Annex II, Section B AI-Act-P, including above all vehicle type approval procedures.

According to Art. 6 (2), Annex III AI-Act-P, the *second group* covers *stand-alone AI systems* that may essentially affect substantially security aspects, such as use in critical infrastructures, or also fundamental rights, such as AI systems for pupil and student assessment, employee selection and promotion or the use of *scoring systems* in the area of essential private or public services, including the *credit scoring* system (Annex III No. 5 b) AI-Act-P. Annex III No. 6 of the AI-Act-P highlights as high-risk AI systems in particular those used in the field of criminal justice and the prosecution of criminal offences, such as predictive policing.[57] But so does the use of AI systems to detect crime. The same applies to AI systems in migration and asylum procedures, Annex III No. 7 AI-Act-P.

According to Art. 7 AI-Act-P, the *EU Commission* is to be empowered to supplement or modify Annex III under the conditions specified in Art. 7 AI-Act-P. These include, above all, damage or threats to fundamental rights that have already occurred because of an AI system (Art. 7 (2) (c) AI-Act-P), or an economic, social or knowledge imbalance of power vis-à-vis the user of the AI system (Art. 7 (2) (f) AI-Act-P).

2. Requirements for High-Risk AI Systems

In its risk-based approach anchored in product safety law, the AI-Act-P ultimately follows similar patterns to the recently presented draft of a Digital Service Act on particularly large online platforms or, as in the past, financial market regulations, in that risk and quality management systems as well as transparency and publicity obligations are introduced on a risk-graded basis. The product safety approach is also reflected in the presumption of conformity with accepted technical standards and

[55] Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts [2014] OJ L 96/251.

[56] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1; Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L 117/176.

[57] Regarding Predictive Policing Lucia M. Sommerer, *Personenbezogenes Predictive Policing. Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose* (Baden-Baden: Nomos, 2020); Ines Härtel, "Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren," *LKV,* (2019): 49; Tobias Singelnstein, "Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention," *NStZ,* (2018): 1.

the corresponding conformity assessment procedures, with which the *EU Commission* intends to implement a flexible approach. The requirements were essentially developed from the recommendations of the *High Level Expert Group on AI* and the Assessment List for trustworthy artificial intelligence derived from them.[58]

a) Riskmanagementsystems

According to Art. 9 AI-Act-P, all high-risk AI systems must be flanked by a risk management system, the details of which are specified in Art. 9 (2) AI-Act-P; at the same time, Art. 9 (2) p. 1 AI-Act-P requires a continuous update of the risk management system. According to Art. 9 (2) sentence 2 AI-Act-P, the elements include the known components of a risk management system, such as the identification and assessment of potential risks and the definition of measures. The risk management system should also include foreseeable misuse of the AI systems as well as data from product monitoring pursuant to Art. 61 AI-Act-P on additional risks. Regarding the required measures according to Art. 9 (2) p. 2 d) AI-Act-P, Art. 9 (4) p. 1 AI-Act-P makes clear that no 100% security is required, but that restrictions can be classified as "acceptable". This is reinforced by Article 9 (4) (3) (b) of the AI-Act-P when sufficient control options are required for risks that cannot be completely eliminated, flanked by corresponding information obligations about such risks and training for users, Article 9 (4) (3) (c) of the AI-Act-P.

Finally, Art. 9 (4) p. 4 AI-Act-P emphasizes the users' knowledge, training and experience, including the environment in which the AI is to be used, to eliminate or reduce the risks. The AI-Act-P also pays particular attention to the testing of AI systems, which according to Article 9 (7) of the AI-Act-P should be carried out at the latest prior to market launch; however, Article 9 (6) of the AI-Act-P limits the testing requirements to the intended area of use of the AI - abuses etc. accordingly do not need to be included.

b) Requirements for Data, Especially Training Data

AI systems require training on data; therefore, it is not surprising that Art. 10 AI-Act-P explicitly deals with data as a prerequisite for AI systems, in particular *"Data Governance"*. According to Article 10 (2) of the AI-Act-P, this includes, among other things, the choice of data sets, the relevant assumptions, possible presetting or alignments (biases), and the identification of possible data gaps and deficiencies. Article 10 (3) and (4) of AI-Act-P set out requirements that are actually self-evident, such as the representativeness, completeness and accuracy of the data, as well as the consideration of local or functional contexts in which the AI systems are to be used.

It is interesting to note that Art. 10 (5) AI-Act-P provides for a partial breakthrough of strict data protection, especially of sensitive data under Art. 9 GDPR,

[58] See for this AI HLEG, "The Assessment List for Trustworthy Artificial Intelligence for self-assessment (*ALTAI*)", European Commission, July 17, 2020, accessed November 02, 2022, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342.

with Art. 10 (5) AI-Act-P providing for corresponding safeguards, but without requiring full anonymization if the data is otherwise unusable.

c) Technical Documentation and Conformity Assessment Procedures

A prerequisite for the conformity assessment procedure is meaningful documentation, as required by Article 11 (2) of the AI-Act-P. However, even those systems that are "only" subject to monitoring by supervisory authorities must have documentation with the minimum content according to Annex IV of the AI-Act-P, Art. 11 (1) AI-Act-P. Only with this information can certification procedures, as well as subsequent checks by market surveillance authorities, be carried out.

A central role in the overall concept of the *EU Commission* is played by harmonized *technical standards*, which are commissioned by the *EU Commission*, but for which the operator can also demonstrate equivalent solutions in accordance with the *New Legislative Framework* in order to comply with the requirements. In this way, the *EU Commission* aims to achieve the necessary flexibility to manage the risks, which will naturally depend on whether, when and under what conditions such standards can be developed.

d) Traceability Instruments (logging devices)

It is well known that AI systems are often characterized by the so-called black-box problem[59], where the traceability of the results generated by the AI remains unclear.[60] In order to take this problem into account, Art. 12 (1) AI-Act-P requires the use of traceability mechanisms, so-called *logging devices*. In particular, the *logging devices* are intended to enable the monitoring of activities of the AI that may result in risks pursuant to Art. 65 (1) AI-Act-P; these mechanisms are also intended to facilitate the product monitoring obligations, Art. 12 (3) AI-Act-P in conjunction with Art. 61 AI-Act-P. Finally, special requirements are imposed on biometric recognition systems, Article 12 (4) of the AI-Act-P.

e) Human Supervision

Art. 14 AI-Act-P requires high-risk AI systems to be adequately supervised by humans when the AI is in use, with supervision aimed at preventing or reducing risks to health, safety, or fundamental rights, and including foreseeable misuse, Art. 14

[59] AI HLEG, *A definition of AI: Main capabilities and scientific disciplines* (Brussels: European Commission Directorate-General for Communication, 2018), 6, locates the problem like this "The notion of black-box AI refers to such scenarios, where it is not possible to trace back to the reason for certain decisions".

[60] Niederée and Nejdl, (n 26), 123; Hans Steege, "Künstliche Intelligenz und Mobilität," *SVR,* (2021): 1 (4); Herbert Zech, "Künstliche Intelligenz und Haftungsfragen," *ZfPW,* (2019): 198 (202); Zech, (n 9), A 33; Heinz-Uwe Dettling and Stefan Krüger, "Erste Schritte im Recht der Künstlichen Intelligenz," *MMR,* (2019): 211 (212); Friedemann Kainer and Lydia Förster, "Autonome Systeme im Kontext des Vertragsrechts," *ZfPW,* (2020): 275 (279); Dimitrios Linardatos, "Künstliche Intelligenz und Verantwortung," *ZIP,* (2019): 504 (504); Georg Borges, "Rechtsrahmen für autonome Systeme," *NJW,* (2018): 977 (978).

(2) AI-Act-P. To this end, the AI system must provide for appropriate measures, such as human-machine interfaces, which must either be built in by the operator from the outset or provided for users to implement. Article 13 (4) of the AI-Act-P specifies the requirements by stipulating that the human supervisor must be able to understand the capabilities and limitations of the AI system and to supervise it appropriately, in particular to respond immediately to malfunctions. Furthermore, the human supervisor must be aware that there is a risk of *"automation bias"*, i.e. blindly accepting the AI's recommendations. The human supervisor should also be enabled to put the results of the AI systems into perspective at any time, as well as to interrupt the operation of the AI (panic button).

Art. 14 (5) AI-Act-P again contains special provisions regarding the use of AI systems with biometric information; here, it is part of human supervision that no decisions or measures are taken until at least a second natural person has not verified and confirmed the identification of the data subjects.

f) Sturdiness, Accuracy and IT Security Requirements

Art. 15 AI-Act-P also requires sufficient security and accuracy of the AI systems. Regarding the sturdiness of the systems, the AI-Act-P leaves the exact requirements largely open, but points out that these can be achieved by technical measures such as back-up systems or *"fail-safe plans"*, Article 15 (3) AI-Act-P. It is noteworthy in this context that Art. 15 (3) sentence 3 AI-Act-P also covers so-called *"feedback loops"*, in which the self-learning system practically arrives at a path dependency of its assessments based on its own results; these are to be mitigated (and thus not necessarily prevented) by appropriate measures. With regard to cybersecurity, Art. 15(4) AI-Act-P requires that AI systems shall be secured against attacks by unauthorized third parties, also covering the manipulation of *training data* or the falsification of learning models; in the context of conformity assessments, the AI-Act-P also includes certifications under the Cybersecurity Act, for which a presumption of conformity then also applies according to Art. 42(2) AI-Act-P.[61]

g) Transparency and Instruction Obligations

Finally, Art. 13 AI-Act-P contains instructional obligations and first provides in Art. 13 (1) AI-Act-P that AI systems must be designed in such a way that they are sufficiently transparent to enable users to use the system correctly and to interpret the results. However, the real focus is on the instructions that an AI system must contain: In addition to a general clause in Art. 13(2) AI-Act-P, Art. 13(3) AI-Act-P contains a catalog of necessary instructions, which primarily refers to the degree of *sturdiness*, *accuracy* and *safety* for which the AI has been tested, as well as circumstances

[61] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151/15.

that may have an influence on it. Furthermore, information must be provided on risks to health, safety or impairment of fundamental rights that may occur as a result of foreseeable events within the intended purpose of the AI or from anticipated misuse; noting that Art. 13 (3) (b) (iii) AI-Act-P does not distinguish between the different fundamental rights. In addition, the required information on the *training, validation* and *test data* used for the AI is important, Art. 13 (3) b) v) AI-Act-P; only in this manner can the user assess the basis on which the AI was actually trained. Finally, information about the human monitoring measures must also be provided pursuant to Art. 14 AI-Act-P, Art. 13 (3) d) AI-Act-P.

VI. Transparency Obligations for All AI systems

For specific AI systems, the transparency obligations under Art. 52 AI-Act-P also apply, which do not have to be high-risk systems. This concerns AI systems that pose particular risks of manipulation, whether through interaction with humans, para. 1, or through emotion recognition systems or biometric categorization, para. 2, or finally through the generation or manipulation of content resembling real persons or events, in particular images or videos (so-called *"deep fakes"*), para. 3. For all groups, the AI-Act-P requires that the third parties concerned be informed that corresponding AI systems are being used, in each case with exceptions for AI systems that serve law enforcement or crime fighting purposes. In addition, Art. 52 (3) (2) AI-Act-P allows the use of *deep-fake* AI systems for necessary artistic or scientific purposes or for forming opinions, without the artificial creation of the content having to be made clear in these cases.

However, apart from informing the data subjects, Art. 52 AI-Act-P does not provide for a mandatory right for the data subjects to receive an offer or service from the operator even without the use of AI. Therefore, even with this regulation, the data subject does not (yet) have a genuine opt-out right associated with a right to contact a human being.

VII. Obligations for Operators and Users of AI systems

1. Obligations for Operators, Manufacturers and Quasi-manufacturers

Art. 16 of the AI-Act-P obliges the operators, in addition to complying with the requirements for the AI systems, to follow the (usual) components of a *conformity assessment* procedure, including the affixing of the CE mark (Art. 19 of the AI-Act-P), in particular to maintain a *quality management system* in accordance with Art. 17 of the AI-Act-P, to maintain the log files, insofar as these are under the control of the providers, or to carry out the registration in accordance with Art. 51 of the AI-Act-P. In addition to the components for the safe design and development, as well as the testing and validation of the AI systems, known from product safety, including the *risk management system* according to Art. 9 AI-Act-P, the quality management system primarily comprises comprehensive specifications relating to *data management*,

from data collection to data mining to data storage, Art. 9 (1) f) AI-Act-P. Moreover, the quality management system must include product monitoring pursuant to Art. 61 AI-Act-P as well as procedures for the notification of serious incidents pursuant to Art. 62 AI-Act-P, Art. 17 (1) h) and i) AI-Act-P. In this context, Art. 17(2) AI-Act-P also considers the size of the *operator's* organization and thus the proportionality.

Regarding the *log files* created by the AI systems pursuant to Art. 12 AI-Act-P, the *operators* will be obliged to retain them if they are under their "control", be it because of contractual agreements with the user or based on legal obligations, Art. 20 (1) AI-Act-P. The time period within the log files must be kept is limited by Art. 20 (1) (2) AI-Act-P to that which is appropriate to the purpose of the AI system and to the relevant Union and Member State regulations. Interestingly, the GDPR is neither considered nor breached here, so that the purpose of data deletion and economy, Art. 5 (1) b) and c) GDPR, must be observed.

Finally, closely interlinked with the product monitoring obligations is Article 21 of the AI-Act-P, which obliges the *operator to take corrective measures* in the event that the *operator* has indications that the AI system no longer complies with the requirements of the AI-Act-P, up to and including the obligation to recall the product. In these cases, the *dealers* involved must also be informed, as must *importers or authorized representatives*.

According to Art. 24 AI-Act-P, *manufacturers* are treated like *operators* if they fall under Annex II Section A, i.e. the *conformity assessment procedures* according to the *New Legislative Framework*, and the product is placed on the market together with the AI system under the name of the *manufacturer*. However, the operator is not released from the obligations regarding the AI system, but only with the product itself.

Similar to other product safety regulations,[62] Art. 28 AI-Act-P also treats as *operators* all those who market the AI system under their name or brand, or who have significantly modified the AI system itself or its intended use. In the latter two cases, the AI-Act-P no longer declares the actual *operator* responsible, which seems understandable because the AI system no longer corresponds to the product that the *operator* intended to market.

2. Obligations for Importers and Distributors

Similar to other product safety regulations,[63] special obligations apply to the importer, first of all the verification that the operator has complied with the conformity assessment procedure including CE marking, but also that the importer is not

[62] Thus among other things in Art. 2 e) Directive 2001/95/EC of the European Parliament and of the Council of 03 December 2001 on general product safety [2002] OJ L 11/4.

[63] See e.g. Art. 13 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002

allowed to introduce the AI system into the market if he has indications that the system does not comply with the requirements of the, Art 26 (2) AI-Act-P. Otherwise, in addition to the notification of risks to the provider and the supervisory authorities pursuant to Art. 26 (2 Sentence 2), Art. 65 (1) AI-Act-P, the importer is primarily responsible to the supervisory authorities for providing the necessary information and documentation for compliance, but also for the log files that the operator has under its control, Art. 26 (4) AI-Act-P.

If an importer cannot be identified, the authorized representative or agent of the operator of the CI located outside the EU will step in with regard to the obligations to cooperate with the *authorities*, including the documentation on compliance and access to the *log files* in accordance with Art. 25 AI-Act-P.

On the other hand, a *distributor* is responsible under Article 27(1) of AI-Act-P for checking the CE marking, including the necessary instructions, and for ensuring that the *operator* and, if applicable, the *importer* comply with the obligations under the Draft Regulation; however, it is unclear how a *distributor* is supposed to meet the latter requirement, as this includes, among other things, compliance with the risk and quality management system, etc. The *distributor* is also required to notify the *importer* of any non-compliance with the provisions of the AI-Act-P. Similar to the *importer's* obligations, the *distributor* is also required under Article 27 (2) of the AI-Act-P not to place the AI system on the market if there are corresponding indications of non-compliance with the AI-Act-P; however, in addition to the *importer* obligations the *distributor* is also required to take corrective measures itself or through the *operator*, *importer* or any other *user*, up to and including the recall of the AI system if it does not comply with the general requirements for AI systems. Art. 27 (4), Recital 23 AI-Act-P. Risks pursuant to Art. 65 (1) AI-Act-P must be reported to the supervisory authorities without delay.

3. Obligations for Users

Roughly speaking, the (commercial) *users* of AI systems are subject to three obligations: *First*, they must use the AI systems in accordance with the instructions of the operators, Art. 29 (1) AI-Act-P, *second*, that the data used for the AI systems are relevant to the intended use of the AI, Art. 29 (3) AI-Act-P, and *thirdly*, the obligation to monitor the AI system including the notification of risks according under Art. 65 (1) AI-Act-P to the *operator* or *distributor* and the temporary suspension of the AI system, in case of serious incidents according to Art. 62 (1) AI-Act-P including the interruption of the AI system. Furthermore, *users* must retain the log files that remain under their control for the period of time outlined in Article 20 AI-Act-P.

---

and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1; Art. 8 Directive 2014/29/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of simple pressure vessels [2014] OJ L 96/45.

Remarkable here are the comparatively little detailed regulations on training the AI systems, which often take place on the user side; only the passage that the *input data* must be "relevant" can be made fruitful here.

VIII. Conformity Assessments

One of the important components of the AI-Act-P is the differentiated conformity assessment procedures, which follow the *New Legislative Framework* approach, but also include the so-called *stand-alone AI systems* in a completely new way. Apart from the accreditation and notification procedures regulated in Art. 30-39 of the AI-Act-P, which contain few surprises, Art. 40 of the AI-Act-P establishes the presumption of conformity based on compliance with harmonized technical standards accepted by the EU.

The same applies to so-called *common specifications*, which the *EU Commission* can adopt by means of implementing acts if there are no technical standards or only standards that do not cover all risks, Art. 41 AI-Act-P. For products containing AI systems, the AI-Act-P acts as an additional horizontal regulation which supplements the conformity assessment procedures under the sectoral standards.

Once again, the outstanding position of harmonized technical standards becomes clear - but so far only various development projects are available, for example in the form of the roadmap of DIN and DKE with the support of the *Federal Government*,[64] as well as some standardizations of the ISO,[65] such as the trustworthiness of AI systems. (ISO/IEC TR 24028) or the IEEE (7010-2020) about "Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-being".[66]

1. Possible Procedures

In conjunction with the respective Annexes VI and VII Article 43 of the AI-Act-P sets the central course for the choice of conformity assessment procedures. According to Annex VI, the operator can prove conformity by means of internal controls, which refer to the quality management system to be established according to Art. 17 of the AI-Act-P as well as the technical documentation and product monitoring. According to Annex VII, proof of conformity is provided by an inspection of the quality management system and the technical documentation by a certification body. Section 4.6. subsection 5 Annex VII AI-Act-P contains specific requirements in case the certificate was refused due to insufficient or inadequate *training data*; in which case the AI shall be re-trained.

---

[64] See to this the Roadmap-Recommendations of the DIN and DKE, November 2020, accessed November 03, 2022, https://www.din.de/resource/blob/772438/6b5ac6680543eff9fe372603514be3e6/normungsroadmap-ki-data.pdf.

[65] See to this the overview from iSO/IEC Joint Technical Committee JTC 1/SC 42, accessed November 03, 2022, https://www.iso.org/committee/6794475/x/catalogue/.

[66] Overview of relevant standards and related standards in roadmap of the DIN and DKE, (n 64), 152 with more references.

2. Biometrical AI-Methods

However, in the case of AI systems for biometric recognition, the *operator* can only choose between the two forms of conformity assessment if harmonized technical standards or the *"common specifications"* of the *EU Commission* are available, otherwise he is instructed to use the procedure with the help of a certification body in accordance with Annex VII, Art. 43 (1) AI-Act-P. In principle, the *operator* is free to choose the certification body, unless the AI is to be used by national authorities or EU institutions for law enforcement or in the context of migration and asylum policy; in this case the market surveillance authority must act as a certifier in accordance with Article 63 (5) and (6) of the AI-Act-P.

3. Stand-Alone-AI

All other AI systems according to Annex III are only "certified" according to Annex VI with the help of internal controls by self-declaration of the manufacturer, except for creditworthiness systems, which are subject to the procedure according to Art. 97 - 101 of Directive 2016/36/EU;[67] the involvement of a certifier is explicitly not required here. For the first time, Art. 43 (2) AI-Act-P thus introduces an independent conformity assessment procedure for *stand-alone* AI systems, which, however, is only based on internal controls by the *operator*. Also, Art. 43 (2) AI-Act-P apparently does not make the conformity assessment dependent on the existence of harmonized technical standards or *"common specifications"*, as these are not mentioned in contrast to Art. 43 (1) AI-Act-P, not even in Annex VI.

4. AI Systems as a Component of Products

On the other hand, AI systems that are part of products subject to a conformity assessment procedure according to Annex II Section A of the AI-Act-P, participate in these procedures, albeit with slight modifications, since Annex VII also applies to the examination of the technical documentation by the certifier. The *operator* or *manufacturer* of the products can use the same certifiers that are also approved for the respective product certification, provided that they also meet the requirements of Art. 33 (4) (9) (10) AI-Act-P. Even if the respective regulation provides for the possibility for the manufacturer to opt out of the certification procedure, he can only do so if he applies harmonized technical standards or the *"common specifications"* of the *EU Commission* according to Art. 41 AI-Act-P.

5. AI Changes

Art. 43 (4) subpara. 2 AI-Act-P also regulates the important case of changes to AI systems due to their characteristic of self-development; if these independent further

[67] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC [2013] OJ L 176/338.

developments remain within the framework provided for by the operator and are part of the technical documentation according to Annex IV No. 2 f) AI-Act-P, they are not to be considered as a change to the AI system and therefore do not trigger a new conformity assessment. Also, against the background that issued certificates are to be valid for 5 years according to Art. 44 AI-Act-P, this regulation should not be underestimated in its scope. In practice, it will be problematic to determine precisely whether the independent changes to the AI are still within the framework set by the operator, and according to which criteria this is to be assessed.

6. Temporary Suspension of the Conformity Assessment Procedure by the Supervisory au-thority

Art. 47 (1) AI-Act-P empowers the market surveillance authority to temporarily suspend the conformity assessment procedures or to approve the market launch of an AI system for the respective Member State if this exceptionally serves public safety or the protection of life and limb, environmental protection, but also the protection of particularly important industries or critical IT infrastructures. In this case, the market surveillance authority must check if the AI systems meet the requirements, Art. 47 (2) AI-Act-P.

7. Affixing CE Marking

In addition to the preparation of the EU declaration of conformity according to Art. 48 AI-Act-P, a typical feature of EU product safety is the affixing of the CE mark. While this should still not yet be a problem for products with AI systems, it is different for *stand-alone* AI products. Art. 49 (1) AI-Act-P therefore allows the CE marking to be affixed either on the *packaging* or in the documentation to be prepared.

8. Registration in EU Database

Finally, another cornerstone of the European Commission's regulatory approach is the obligation of *operators* (or authorized representatives) under Article 51 AI-Act-P to register high-risk AI systems in the database operated by the *European Commission* under Article 60 AI-Act-P before they are launched or put into operation. Although this does not imply a reservation of approval, it facilitates ex-post control by the market surveillance authorities and the *EU Commission*.

IX. Creation of "Regulatory Sandboxes" and Facilitation of SMEs

A tool especially associated with new technologies such as blockchain and cryptocurrencies [68] which the *EU Commission* also wants to apply to AI systems, are the so-

[68] See to this also the overview regarding "Regulatory Sandboxes" in the financial sector of the ESMA/EBA/EIOPA, "FinTech: Regulatory Sandboxes and innovation hubs" 2019, accessed November 03, 2022, https://www.esma.europa.eu/sites/default/files/library/jc_2018_74_joint_report_on_regulatory_sandboxes_and_innovation_hubs.pdf ; see also Baker & McKenzie, "A Guide

called *regulatory sandboxes*.[69] However, this *"regulatory sandbox"* does not turn out to be an incubator for innovative AI systems that are not subject to regulation for a while, but is intended to represent a controlled test environment for the development and testing of AI systems under the direct supervision of the competent authorities of the Member States or the *European Data Protection Supervisor* in accordance with a test plan agreed with the supervisory authorities, Art. 53 (1) AI-Act-P. As far as personal data are involved, Art. 53 (2) AI-Act-P also explicitly requires the involvement of the *data protection supervisory authorities* of the respective Member States. However, Art. 53 (3) AI-Act-P can again be interpreted in such a way that the supervisory authorities have a certain leeway in applying the *"regulatory sandbox"*, in that only in the event of significant risks to health, safety or fundamental rights should an obligation to take immediate remedial action and - if this should last longer - to interrupt the development and testing process intervene. Finally, the fact that the *"regulatory sandbox"* does not represent a fundamental "grace period" for the operators of the AI systems is shown by Article 53 (4) of the AI-Act-P, which subjects all participants in the *"regulatory sandbox"* to liability in accordance with the applicable provisions of the EU and the Member States for damage caused to third parties as a result of the experiments in the *"regulatory sandbox"*; since the participants also include the supervisory authorities, state liability also applies. However, most of the provisions on the details of the *regulatory sandboxes*, including the rights and obligations of their participants, are left to delegated acts by the *EU Commission* under Article 53(6) in conjunction with Article 74(2) of the AI-Act-P.

In this context, Art. 54 AI-Act-P pays special attention to the data protection implications of the *regulatory sandboxes*, whereby the *principle of strict purpose limitation* according to Art. 5 (1) b) GDPR is opened under certain conditions. This is only permissible for "innovative" AI systems that serve either law enforcement, the fight against crime, the safeguarding of public security or public health, in particular the fight against diseases, or the improvement of environmental protection, Art. 54 (1) a) i) - iii) AI-Act-P. Furthermore, Art. 54 (1) b) AI-Act-P requires that the objectives of the development and testing of AI systems cannot be achieved with synthetic or anonymized data. Finally, Art. 54 (1) c) - h) AI-Act-P impose numerous other conditions, all of which serve to minimize the risks to data protection, such as the requirement that data be deleted after the "*sandbox*" has ended or that processing only take place in an isolated and protected space.

---

to regulatory FinTech sandboxes internationally" 2020, accessed November 03, 2022, https://www.bakermckenzie.com/-/media/files/insight/publications/2020/05/a_guide_to_regulatory_fintech_sandboxes_internationally_8734.pdf?la=en; Energiesektor in Bundesamt für Energie/Frontier Economics, "Regulatory Sandboxes – best practices für die Schweiz, Freiräume für neue Ansätze und digitale Innovation in der Stromversorgung" 2020, accessed November 03, 2022, https://pubdb.bfe.admin.ch/de/publication/download/10074 .

[69] Comprehensive on the administrative law problems of these "regulatory sandboxes", see Christoph Krönke, "Sandkastenspiele – "Regulatory Sandboxes" aus der Perspektive des Allgemeinen Verwaltungsrechts," *JZ*, (2021): 434 with further references.

On the other hand, the measures announced by the *European Commission* for the benefit of start-ups and SMEs are limited to the obligation of member states to ensure easier access to the "*sandboxes*" for these AI operators, otherwise to the creation of special communication channels in order to provide guidelines for the application of the AI-Act-P for these companies, according to Article 55 (1) a) of the AI-Act-P. In contrast, the obligation to consider the size of the company concerned when setting fees for the conformity assessment procedure, Art. 55 (2) AI-Act-P, is likely to be more significant.

X. Codes of Conduct

Art. 69 AI-Act-P creates the possibility for operators of non-high-risk AI systems to also apply the requirements that apply only to high-risk AI systems to other AI systems through voluntary *Codes of Conduct*. Within this framework, these *Codes of Conduct* shall be supported, especially for AI systems in the area of sustainable environmental protection or accessibility for severely disabled persons, including the participation of *stakeholders* in the design and development of the AI systems, up to diversity in the development teams, Art. 69 (2) AI-Act-P. Such *Codes of Conduct* require that users as well as all other interested *stakeholders* or their associations are involved in their development and adoption, Art. 69 (3) AI-Act-P.
Unlike Art. 40 i and Art. 28 (1), (4), 24 (3), 32 (3) GDPR, the AI-Act-P does not contain any relief for *operators* if they have joined such *a Code of Conduct*; in this respect, it remains more than doubtful what incentives should exist for operators to develop such *Codes of Conduct* or to join them.

XI. Supervisory and Monitoring Structures

1. Creation of a European Artificial Intelligence Board

Similar to the GDPR and the Digital Service Act proposed in December 2020, which provides for the creation of an *EU Digital Services Board*, the *EU Commission* also wants to provide for a *European Artificial Intelligence Board* for the regulation of AI according to Art. 56-58 AI-Act-P, which is essentially to advise the *EU Commission* and ensure coordination of enforcement and monitoring by the national supervisory authorities. The *European AI Board* should be composed of the national supervisory authorities and the *European Data Protection Supervisors* and be chaired by the *EU Commission*, Art. 57 AI-Act-P.

2. Monitoring Authorities

In addition to the usual obligations of the Member States to designate national supervisory authorities, which must cooperate with each other, Article 59 (1) (2) of the AI-Act-P provides that the supervisory authorities must be organized in such a way that they can carry out their activities impartially and objectively – but this does not mean that they must be fully independent as under the GDPR. Finally, Art. 59

(8) AI-Act-P designates the *European Data Protection Supervisor* as the supervisory authority over EU authorities or agencies that may be covered by the AI-Act-P when using AI systems.

3. EU-Wide Database as a Register

Since the AI-Act-P for the first time also covers *stand-alone AI systems* outside of products, their registration is of essential importance for effective market and product monitoring. Even though it is not a classic register for the creation of rights and obligations and the AI-Act-P does not provide for a requirement for approval in the narrower sense, registration in the EU database in accordance with Article 60 of the AI-Act-P is necessary for an *operator* to be able to introduce his high-risk AI system into the European market or put it into operation. According to Annex VIII AI-Act-P, the required information includes not only the usual information on the identity and accessibility of the operator and the EU declaration of conformity, but also information on the purpose of the AI (No. 5) or instructions for its use (No. 11), except if the AI is used for law enforcement or migration and asylum purposes.

XII. Monitoring and Reporting Obligations of AI Operators

1. Product Monitoring

In view of the unpredictable risks and developments that occur in self-learning AI systems in particular, the obligation to monitor products after a market launch or commissioning of an AI system is coming into focus – not only in product liability law[70], but also in product safety law –, here Art. 61 AI-Act-P. For this purpose, the *operator* must prepare a product monitoring and surveillance plan as part of its technical documentation, the details of which must comply with the requirements of an implementing act of the *EU Commission*, Art. 61 (3) AI-Act-P. If the AI system is part of a product that is subject to other conformity assessment procedures and thus also to the product surveillance obligation, the obligations according to Art. 61 (1), (2) AI-Act-P must be integrated into it, Art. 61 (4) AI-Act-P.

2. Reporting Requirements

Similar to the obligations under the GDPR in the event of data breaches (*notification of data breach*), Art. 33 GDPR, Art. 62 (1) AI-Act-P also standardizes a reporting obligation for *operators* of high-risk AI systems to the market surveillance authorities

[70] On product monitoring obligations for AI systems see Spindler, (n 9), 761 ff.; Alexander Schmid, "Pflicht zur "integrierten Produktbeobachtung" für automatisierte und vernetzte Systeme," *CR,* (2019): 141, 142; Gerald Spindler, «§ 11», in *IT-Sicherheitsrecht,* ed. by Gerrit Hornung, Martin Schallbruch, (München: C.H. Beck, 2020) para 31; Michael Denga, "Deliktische Haftung für künstliche Intelligenz," *CR,* (2018): 69, 74; Franz Hofmann, "Der Einfluss von Digitalisierung und künstlicher Intelligenz auf das Haftungsrecht," *CR,* (2020): 282, 285 f.; Wagner, (n 9), 707, 750.

in case of a serious incident or malfunctioning in the Member State where the incident or malfunctioning occurred, but only if these obligations under EU law are intended to protect fundamental rights. Thus, Art. 62 (1) AI-Act-P establishes a *general notification obligation* beyond the regulation of AI, which can affect all EU regulations that come into consideration. In this context, it is noteworthy that Article 62 of the AI-Act-P only refers to *incidents relevant to fundamental rights*, but not to the other risks to public security mentioned in the AI-Act-P.

Operators must notify without delay if they have reason to believe that the AI system is likely to be the cause of the incident or malfunction; in any case, the operator must notify within 15 days after becoming aware of the significant incident or malfunctioning, Art. 62 (1) (2) AI-Act-P.

3. Enforcement and Monitoring

The monitoring of the markets is the responsibility of the authorities under Regulation (EC) No. EU/2019/1020, whereby the term *"operator"* refers to all obligated parties under Art. 16 et seq. AI-Act-P, i.e. both *providers and distributors and users*, and also *stand-alone AI systems* as products, Article 63 (1) AI-Act-P. For products subject to the conformity assessments of the sector-specific product safety regulations and directives, the respective authorities continue to be responsible, for credit institutions the corresponding supervisory authority, for biometric systems used in the context of law enforcement or migration and asylum, the national data protection supervisory authorities, Art. 63 (3) - (5) AI-Act-P, for systems in the area of the EU institutions the *European Data Protection Supervisor*, Art. 63 (6) AI-Act-P.

On the one hand, the powers of the supervisory authorities include full *access* to the entire *training and test datasets* of the AI systems, which must also be possible through technical interfaces for remote monitoring, Art. 64 (1) AI-Act-P; on the other hand, even *access to the source code* may be requested by the supervisory authorities in order to assess compliance with the provisions for high-risk AI systems, Art. 64 (2) AI-Act-P. Other national supervisory authorities responsible for enforcing Union law relevant to fundamental rights, are also authorized to monitor, but limited to requesting the relevant documents and documentation or, if these are insufficient, may make a corresponding request to the market surveillance authority to organize tests of the AI systems, Art. 64 (3) (5) AI-Act-P.

The AI-Act-P pays particular attention to the procedure for carrying out inspections of AI systems (apparently without restriction to high-risk AI systems, which are then generally considered to be high-risk) with regard to compliance with the obligations if risks to health, safety or fundamental rights become apparent, Art. 65 (1) (2) AI-Act-P. In the event of non-compliance with the obligations under the AI-Act-P, the market surveillance authority may order all necessary measures against the operator, up to and including the obligation to recall the AI system or product, Art. 65 (3) AI-Act-P, and, in the event that the *operator* does not comply with the order, may itself initiate the product recall, in addition to other necessary measures, Art. 65 (5) AI-Act-P.

However, even if the market surveillance authority determines compliance with the requirements of the AI-Act-P in the course of the review, it remains authorized to require the *operator* to take appropriate measures, up to and including product recall, within a period of time commensurate with the risks, provided that the AI system still presents risks to the health or safety of persons or with regard to compliance with obligations under Union law with relevance to fundamental rights or – in contrast to other powers, for example – also to the protection of other public interests, Article 67 (1) AI-Act-P. The *operators* must eliminate or reduce the risks that have arisen within the period of time to be determined by the market surveillance authority, Art. 67 (2) AI-Act-P.

XIII. Sanctions, in Particular Fines

Following the example of the GDPR (cf. Art. 83 (1) and (4-6) GDPR) and other (proposed) EU legislation such as the Digital Services Act, Art. 71[71] AI-Act-P provides for drastic fines for non-compliance with the respective provisions of the AI-Act-P: Thus, violations of the prohibitions of Art. 5 AI-Act-P, which apply to every AI system, as well as of Art. 10 AI-Act-P - the requirements for *data governance* - are to be fined for companies as *operators* with up to 6% of their worldwide annual turnover, Art. 71 (3) AI-Act-P; for other violations, Art. 74 (4) AI-Act-P then "only" estimates 4% of the worldwide annual turnover. In contrast to the GDPR (cf. recital 150 and Art. 83 (4) and (5) GDPR), the AI-Act-P does not contain a group-related regulation, so that so far only the respective *operator* of the AI system, but not the group, can be used as the basis for turnover. However, all "offenders" according to Art. 71 AI-Act-P can be considered as infringers or addressees of fines, i.e. not only *operators*, but also *users* and *operators*, if they have violated the obligations incumbent on them.

XIV. Critical Evaluation

Overall, it is difficult to evaluate the AI-Act-P: The *EU Commission* can be credited with having made a courageous attempt to introduce one of the world's first regulations of AI systems. The AI-Act-P contains numerous sensible approaches, especially regarding the principle of a *risk-based approach*, since the chances of broad-based supervision are likely to be rather slim, especially in view of the possibilities of supervisory authorities to supervise the rapidly changing AI. Likewise, the broad international scope of application, which does not take into account the location of AI *operators*, is to be welcomed - although the general definition of AI systems seems somewhat eclectic and too broad, as it would also include expert systems without the characteristic properties of AI systems, such as the *"black box effect"*.

[71] Commission, "Art. 59 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", December 15, 2020, COM (2020) 825 final 2020/0361(COD).

- Risk: Insofar it concerns high-risk AI systems the *risk-based approach* in particular tends to be devalued if only registration of the AI system in an EU database is required and the prior checks are limited to internal controls to be carried out by the operator itself, at least for so-called stand-alone AI systems. It is true that the Commission points out that there is hardly any experience with auditing and certification for stand-alone systems and that the AI sector is highly innovative and subject to constant change;[72] but it seems questionable why this should be assessed differently for *embedded AI systems* in products that are subject to a certification procedure, in other words: why certification involving certification or auditing bodies should not also be required for high-risk *stand-alone AI systems*. Despite the fundamentally correct approach of relying on technical standards and their certification, the *EU Commission* continues to distinguish between *stand-alone* and *embedded AI systems*, which ultimately seems rather arbitrary in the light of cloud-based control. After all, control by an AI detached from a product and supported or located in the cloud would be such a *stand-alone* system.
- Horizon: However, the *horizontal approach* that overcomes the sectoral boundaries of product security, is to be welcomed - and should also be made fruitful for the Cybersecurity Act in the same way as a product security element. The approach that applies in principle to product safety is also correct, i.e. to resort to *harmonized technical standards*, combined with a *presumption* that the requirements will then be met; only in this way it will be possible for the developers and operators of AI systems to present alternative, equivalent solutions beyond technical standards, so that the necessary flexibility is maintained.
- Standards: However, the definition of technical standards or *common specifications* by the *EU Commission* remains problematic: If fundamental risks are to include impairments of fundamental rights, numerous undefined factors must be included, making it difficult to define *"benchmarks"* for the avoidance of such risks. This does not change the fact that the AI Regulation contains numerous reasonable requirements, such as requiring human supervision, the prevention of *bias* or the focus on proper *data governance* with regard to interpreting the training of data-based AI, as well as the prevention of *"feedback loops"* in order to avoid path dependency of the AI and self-reinforcing assessments. In addition, detailed points of criticism remain, for example with regard to the numerous exemptions for biometric identification procedures, which remain generally permissible for private *operator* and are allowed for government authorities for law enforcement and law enforcement purposes under certain conditions. Similarly, transparency obligations for certain non-high-risk AI systems are well-intentioned, but do not give those affected by the AI systems' decisions or recommendations a proper right to opt-out or contact a human. Regulatory *sandboxes* are also very rudimentary, leaving much to the delegated acts of the *EU Commission*. Finally, the scope

[72] Explanatory Memorandum, (n 8), 14.

of market surveillance raises questions, as it remains unclear what should be considered as EU acts relevant to fundamental rights, since in principle any regulation can affect fundamental rights in some way. Overall, the proposal for an AI Regulation is therefore to be welcomed, even though it still contains numerous open flanks - the further political fate of this ambitious draft remains to be seen.

B. Part 2: Proposals on Product Liability and Liability for AI systems

I. Introduction

The issues of artificial intelligence have been occupying lawyers all over the world for several years. For example, there are also reports from expert groups at the EU Commission on artificial intelligence, which take a detailed position on the various ethical and legal issues,[73] which, among other things, takes a position on the various legal issues raised. The *German Jurists' Conference* has also taken up the topic, for which *Zech* has prepared a detailed expert opinion on the associated liability issues.[74] In essence, the discussion revolves around the possibilities that already exist in the current non-contractual (tort) liability law to deal with the specific issues of autonomous systems, as well as legal policy desiderata as to whether and how existing gaps should be filled. The legal policy discussion at the national level has now been caught up with at the European level: [75]After the *EU Parliament* had already submitted a formulated proposal on liability,[76] the *EU Commission is* now submitting a directive on the formulation of liability for AI systems (AI Liability Directive-E)[77] including a reform of the Product Liability Directive (ProdHaft Directive-E) following the proposal on the regulation of AI in terms of product safety law (AI

[73] AI HLEG, "Ethical Guidelines for Trustworthy AI", European Commission, April 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60425; European Commission, Directorate-General for Justice and Consumers, "Liability for artificial intelligence and other emerging digital technologies", Publications Office, 2019, https://data.europa.eu/doi/10.2838/573689.

[74] *Zech*, (n 9).

[75] Commission, "Proposal of the EU Commission for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain acts of the Union (AI-Reg-E)", April 21, 2021, COM (2021) 206 final, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=EN; on this in detail Gerald Spindler, "Der Vorschlag einer Regulierung der Künstlichen Intelligenz" *CR* (2021): 361 et seq. .

[76] Zech, (n 9), (cited as *Zech*, Supplement, 2022); Gerhard Wagner, "Haftung für Künstliche Intelligenz – Eine Gesetzesinitiative des Europäischen Parlaments Aufsatz," *ZEuP,* (2021): 545 et seq.

[77] Commission, "Proposal of the EU Commission for a Directive of the European Parliament and of the Council adapting the rules on non-contractual civil liability in artificial intelligence (AI Liability-E)", September 28, 2022, COM (2022) 496 final 2022/0303 (COD).

Regulation-E).[78] Almost at the same time, the *EU Commission* has published a proposal for a new horizontal regulation on the cyberresilience of IT products, which considerably expands the product safety regulations – which cannot be dealt with here in extenso, but will also have an impact on liability. [79]

To sum it up briefly: It is not so much the proposal for the AI Liability Directive as the proposed innovations in the Product Liability Directive that make us sit up and take notice. The proposal of the Product-Liability-D-P provides for nothing less than the equalization of software and even connected services with the concept of product, which is tantamount to a small revolution and also corresponds to the proposal of the CRA-E. In contrast, the AI Liability Directive-E refrains from adopting the proposals of the *EU Parliament* for the introduction of strict liability[80], in that the AI Liability Directive-E essentially restricts itself to remedying the information asymmetries in favour of the injured party.

II. Reform of the Product Liability Directive

The proposal of the Product-Liability-D-P aims above all at the synchronization with the reforms in product safety according to the Decision and the definitions in Decision 768/2008/EC[81] , but also at the inclusion of IT products or software including AI systems and connected services up to the extension of the protected legal interests to include data. The Product-Liability-D-P also introduces considerable simplifications of proof and the extension of the responsible parties or liability addresses.

1. The redefinition of the concept of product

a) Software as a product

One of the long overdue reforms of the Product-Liability-D-P concerns the inclusion of software as a *product* - in contrast to the previous law, regardless of whether

[78] Commission, "Proposal of the EU Commission for a Directive of the European Parliament and of the Council on Liability for Defective Products (Product-Liabiltiy-D-P)", September 28, 2022, COM (2022) 495 final 2022/0302 (COD).

[79] Commission, "Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU)", September 15, 2022, 2019/1020 COM (2022) 454 final, hereafter cited as CRA-E.

[80] Resolution of the European Parliament of 20 October 2020 with recommendations to the Commission on the regulation of civil liability in the use of artificial intelligence (2020/2014(INL)); Regulation of civil liability in the use of artificial intelligence, P9_TA (2020)0276; see Wagner, (n 76), 545 ff.; Zech, (n 9), supplement to the DJT Opinion, 2022, 4, 9.

[81] Decision No. 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products and repealing Council Decision 93/465/EEC, [2008] OJ L 218/82 .

the software is embodied ("embedded") in another *product* or not.[82] This is more than clearly expressed in Recital 12 of the Product-Liability-D-P, in which the *EU Commission* points out that software can also control cloud-based *products*, and is also reflected in the definition of the *product in* Art. 4 No. 1 of the Product-Liability-D-P.[83] The proposal even goes one step further and includes "digital manufacturing files" under the term "*product",* Art. 4(2)(1) Product-Liability-D-P, which primarily (but not exclusively, Recital 14 Product-Liability-D-P) means 3D data files for the manufacture of *products* in 3D printers, as Art. 4(2) Product-Liability-D-P states ("digital template of a movable").[84]

On the other hand, the *EU Commission* does not want to include pure source code in the definition of product, as this only represents information, recital 12 p. 3 of the Draft Directive on Product Liability; the Draft Directive on Product Liability thus assumes that the definition of software only includes machine-executable coding and, interestingly, deviates from Art. 1 (1) and (2) as well as recital 7 p. 2 of the Software Directive[85] in copyright law.[86] Further details, however, are not to be found in the Product-Liability-D-P, for example on the treatment of program libraries, which themselves do not have a direct controlling effect, but can be important components of a code; if one keeps in mind the goal of the *EU Commission* that controlling software should be covered, one will also have to understand such parts of a code as a *product.*

Consequently, Recital 12, Sentence 4 of the Draft Directive on Product Liability then regards the developers or producers of software, including the *operators of* AI systems, as *manufacturers within the* meaning of the Draft Directive on Product Liability.

---

[82] Herbert Zech, "Haftung für Trainingsdaten Künstlicher Intelligenz," *NJW,* (2022): 502 (505); Wagner, (n 9), 707 (716 et seq.); for copyright equivalence see ECJ Judgment of 03 July 2012 - C-128/11, ECLI:EU:C:2012:407, 47- *Used Soft = CR,* (2012): 498.

[83] Similarly, the proposal for a Cyber Resilience Act also covers software as a stand-alone "product", see Art. 3 No. 1 CRA-E.

[84] Gerhard Wagner, «§ 2 ProdHaftG», in *MüKo BGB*, ed. Franz Jürgen Säcker et al. 8th edn. (München: C.H. Beck, 2020), marginal no. 28 2020; Anne-Kathrin Müller and Martin S. Haase, "Haftungsrechtliche Aspekte des 3D-Drucks (additive Fertigung) – Teil 2," *InTer,* (2017): 124 (127); Jürgen Oechsler, "Produkthaftung beim 3D-Druck," *NJW,* (2018): 1569 (1570); in this direction also Graf von Westphalen, «§ 47 marginal no. 44.», in *Produkthaftungshandubuch,* ed. Ulrich Foerste and Friedrich Graf von Westphalen 3rd edn. (München: C.H. Beck, 2012); in general on product liability with 3D printers s. Oechsler.

[85] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, [2009] OJ L 111/17.

[86] On the protection of the source code by the Software Directive ECJ Judt. 22 December 2010 - C-393/09, ECLI:EU:C:2010:816 marginal no. 34 f. - *BSA/Ministry of Culture = CR,* (2011): 221; Gerald Spindler, «§ 69a UrhG», in *Urheberrecht*, ed. by Gerhard Schricker and Ulrich Loewenheim 6th edn. (München: C.H.Beck 2020) marginal no. 5; Andreas Wiebe, «§ 69 a UrhG», *Recht der elektronischen Medien*, ed. Gerald Spindler and Fabian Schuster, 4th edn. (München: C.H.Beck, 2019) marginal no. 4.

b) Extension to data and services

The implicit extension of liability to "components" and, above all, *services* contained in Art. 4(3) and (4) of the Draft Directive on Product Liability, for which it is sufficient that they are connected to the *product in* some way, seems almost revolutionary. According to Art. 4 No. 4 Draft Directive on Product Liability, what matters is that the *product* cannot fulfil one or more of its functions without these services. Recital 15 p. 1, 2 of the Draft Directive on Product Liability clarifies that services are not generally covered by the strict liability of the Draft Directive on Product Liability, but *services that are* essential for the function of the *product,* such as traffic data for navigation systems. However, only those *services* (and thus also data) are covered that are relevant for the safety of the *product*, including cyber security, recital 15 p. 2 of the Draft Directive on Product Liability - which is particularly important with regard to the demarcation from the interest in equivalence covered by the Digital Content Directive, which, as is well known, does not contain any statements on liability for damages.[87]

According to Recital 15, Sentence 3 of the Draft Directive on Product Liability, it is not even necessary that the *manufacturer* itself provides these *services*; rather, it shall be sufficient that the *manufacturer* merely recommends the use of such *services* or otherwise "influences" their provision by third parties. However, recital 15 p. 3 of the Draft Directive on Product Liability thus deviates from the definition of "control by the *manufacturer*" according to Art. 4 No. 5 of the Draft Directive on Product Liability, which refers to the authorization of the *services of* a third party by the *manufacturer* (including updates or upgrades). A mere recommendation may contain an authorization, but this also raises the question of the point in time to be taken into account, e.g. in the case of a modification of the *services by a* third party: Does the authorization cease to apply, for example, if the *manufacturer* only "recommends" a specific version of a *service?* Or, in the case of a general "recommendation", does it apply to all future versions of the *service* by a third party?

With this extension, the Product-Liability-D-P also covers the area of *training data,* which is so important for AI software[88] , which could already be taken into account under the fault-based producer liability according to section 823 (1) BGB in the context of supplier liability, but for which the manufacturer of the AI system

[87] Gerald Spindler and Karin Sein, "Die Richtlinie über Verträge über digitale Inhalte Aufsatz," *MMR,* (2019): 488 (491); Reiner Schulze, "Die Digitale-Inhalte-Richtlinie – Innovation und Kontinuität im europäischen Vertragsrecht;" *ZEuP,* (2019): 695 (720 f.); Lena Mischau, "Daten als „Gegenleistung" im neuen Verbrauchervertragsrecht," *ZEuP,* (2020): 335 (352).

[88] Spindler, "Neue Haftungsregelungen für autonome Systeme?," *JZ,* (2022): 793 (797); Philipp Hacker, "Ein Rechtsrahmen für KI-Trainingsdaten," *ZGE,* (2020): 239 (250); Zech, (n 82), 502 (505); *id.* Gutachten A zum 73. Deutschen Juristentag, 2020, A 68.

could exculpate himself by providing appropriate proof of due diligence.[89] In practice, such liability will also encounter problems of proof.[90] With the extension to the necessary *services,* the strict liability of the Product-Liability-D-P is now extended to the necessary data sets for an AI system - without the need to comply with Art. 10 AI-Reg-E, which further reduces the scope of application of the AI-Liability-RL-E.

c) Exception for open source software

In order not to hinder innovation and research, according to recital 13, sentences 1 and 2, open source software that is developed or made available outside of commercial "activities" is not to be covered by the concept of product under the Product-Liability-D-P. If, on the other hand, the open source software is made available in return for payment or the disclosure of personal data, the Product-Liability-D-P should apply, unless the data is used exclusively to improve security, compatibility or interoperability, recital 13 p. 3 Product-Liability-D-P. The Product-Liability-D-P thus follows the path already taken in Art. 3 (5) f) of the Digital Content Directive[91] to exempt open source software from regulation.[92]

However, here too the devil is in the detail: Open source software is often combined in distribution with proprietary software in addition to the free offer ("dual licensing"[93]). For example, *Oracle* offers its MySQL database system under the GPL v2 on the one hand and under a commercial license on the other.[94] In addition, open source software is often only offered as part of a bundled service package that

[89] Zech, (n 82), 502 (507); Grützmacher, "Die zivilrechtliche Haftung für KI nach dem Entwurf der geplanten KI-VO," *CR,* (2021): 433 marginal no. 18; Spindler, (n 88), 793 (796 f.); Gerald Spindler «§ 823 BGB», in *BeckOGK,* ed. Beate Gsell et al., (München: C.H. Beck, status July 01, 2022), marginal no. 662.

[90] Zech, (n 82), 502 (507); *ibid.* (n 87) A 58.

[91] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contract law relating to the provision of digital content and digital services, [2019] OJL 136/1.

[92] Dirk Staudenmayer, «Directive (EU) 2019/770», in *EU Digital Law*, ed. Reiner Schulze and Dirk Staudenmayer, 1st edn. (Baden-Baden: Nomos, 2020), Art. 3 Scope Rn. 106 et seq.; Spindler and Sein, (n 87), 415 (418); Mischau, (n 87), 335 (342).

[93] Carsten Gerlach, "Praxisprobleme der Open-Source-Lizenzierung," *CR,* (2006): 649 (651); Till Jaeger and Axel Metzger, «2nd chapter», in *Open Source Software*, 5th edn. (München: C.H. Beck, 2020), marginal no. 144; Astrid Auer-Reinsdorff and Christian R. Kast, «§ 9 Open Source and Open Content», in *Handbuch IT- und Datenschutzrecht,* ed. by Astrid Auer-Reinsdorff and Isabell Conrad, 3rd edn. (München: Beck, 2019), marginal no. 26.

[94] Cf. Q3 "Commercial License for OEMs, ISVs and VARs", July 2010, accessed October 10, 2023, https://www.mysql.com/about/legal/licensing/oem/.

also includes support services or software maintenance.[95] If, for example, an open source software that is in itself freely available is linked to a *product* and at the same time "maintained" for a fee, the question arises for the injured party as to how he should be able to assess the character of the software, since he often lacks the necessary information. Finally, in these cases it is questionable whether it is still *non-commercially* distributed or developed open source software, especially since the Product-Liability-D-P does not focus on the license conditions. This is all the more true if one takes into account that the Product-Liability-D-P also wants to cover linked *services*.

2. Protected legal interests extended to data loss or corruption

The legal interests protected by strict product liability are also extended. First of all, the Draft Directive on Product Liability specifies for the integrity of life and limb in Art. 4 No. 6 a) Draft Directive on Product Liability that medically recognized damage to mental health is also covered.[96] In addition, injuries to the property of consumers are also covered if it is used for both private and commercial purposes, recital 19, p. 2. 2 Product-Liability-D-P; only the exclusively professional use is not covered by the Product-Liability-D-P, Art. 4 No. 6 b) iii).[97]

The most important innovation, however, is the extension of the protected legal interests to include the *loss* or *corruption of data*, unless the data was used exclusively for professional purposes, Art. 4 No. 6 c) Product-Liability-D-P. According to recital 16, sentence 1 of the Draft Directive on Product Liability, the costs of restoring the data are to be included in the damage. It apparently does not matter whether or where the data is stored, so that data in the cloud also falls under the protection of the Product-Liability-D-P. The Product-Liability-D-P would thus put an end to a

[95] Gerald Spindler*, Rechtsfragen der Open Source Software*, (München: Verband der Softwareindustrie Deutschlands e.V., 2003), 84; Jaeger, Metzger, «1st chapter», in *Open Source Software*, 5th edn., (München: Beck, 2020), marginal no. 23; specifically for the Mozilla Public Licence cf. Jaeger and Metzger, (n 93), marginal no. 100.

[96] The understanding of the protected legal interests runs parallel to the understanding known from Gerhard Wagner, «§ 823 (1) BGB», in *MüKo BGB*, ed. Franz Jürgen Säcker, 8th edn. ProdHaftG, (München: C.H. Beck, 2020) § 1 marginal no. 4; Mark Seibel, «§ 1 ProdHaftG», in *BeckOGK*, ed. Beate Gsell et al. October ProdHaftG, (München: Beck, 2020 status October 01, 2022) marginal no. 27; according to this, the concept of injury to health also covers mental illnesses and damages that are medically ascertainable and go beyond the general (life) risk, cf. Gerald Spindler, «§ 823 BGB», in *BeckOGK*, ed. Beate Gsell et al. July 01 (München: C.H. Beck, 2022 status July 01, 2022), marginal no. 108; Gerhard Wagner, «§ 823 (1) BGB», in *MüKo BGB*, ed. Franz Jürgen Säcker, 8th edn. (München: C.H. Beck, 2020), marginal no. 205 et seq.

[97] Not so for the old ProdHaft-RL Wagner, (n 96), § 1 marginal no. 13: decisive whether only private, occasional professional use causes damage; less restrictive Seibel, (n 95), § 1 marginal nos. 49, 54: even a not insignificant professional or commercial use does not harm; Ehring, «§ 1 ProdHaftG», in *Produkthaftungs- und Produktsicherheitsrecht*, ed. by Philipp Ehring and Jürgen Taeger, 1st edn. (Baden-Baden: Nomos, 2022), marginal no. 31: majority intended use in the private sphere sufficient.

long debate[98] also within the framework of section 823 (1) BGB about the quality of data as *other rights in* favour of their recognition; for it would be more than questionable why only consumers should enjoy the benefit of liability for data loss or corruption, while other data "owners" do not, without having to recognize data ownership.
Compensation for damages for the violation of data protection regulations according to Art. 82 of the GDPR[99] or the ePrivacy Directive[100] , on the other hand, shall not be affected by the Product-Liability-D-P, recital 16 p. 3 of the Product-Liability-D-P. 3 Product-Liability-D-P. The concrete calculation of damages is still to be left to the member states, as are claims for *immaterial damages* (section 253 BGB), Recital 18 Product-Liability-D-P. Here, however, it will be very important that a loss of data is not to be equated with pecuniary loss; at least for the area of damages due to loss of profit, their reimbursement will depend on the injured party being able to specifically demonstrate and prove the *liability-filling causality* between the loss of data and the loss of income.

3. Error concept or safety expectations

Another essential adjusting screw in product liability for IT products concerns the concept of error, especially in evolving and learning AI systems, but also with regard to the connection of the IT product or software with its digital environment and with connected other services, up to cybersecurity requirements.

a) Principles

The principles for determining the defectiveness of IT products remain in principle the same as in the previous Product Liability Directive, namely the *general market expectations with* regard to the safety of the *product*, Art. 6(1) Product-Liability-D-P, which is also intended to cover the intended use of the *product,* Recital 22 p. 4. 4 Product-Liability-D-P. In this context, the Draft Directive on Product Liability differentiates according to the risks of the products for the respective legal interests

[98] Spindler, (n 96), § 823 Rn. 137; Wagner, (n 96), § 823 Rn. 332; Simon Adam, "Daten als Rechtsobjekte," *NJW,* (2020): 2063 (2067); Thomas Riehm, "Rechte an Daten – Die Perspektive des Haftungsrechts," *VersR,* (2019): 714 (724); Andreas Wehlau and Klaus Meier, "Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung," *NJW,* (1998): 1585 (1588); always referring to embodiment by data carrier: BGH 14 July 1993 - VIII ZR 147/92 = *CR,* (1993): 681 (682); rejecting Andreas Spickhoff, «Der Schutz von Daten durch das Deliktsrecht», in *Unkörperliche Güter im Zivilrecht,* ed. Stefan Leible, Matthias Lehmannand, Herbert Zech (Tübingen: Mohr Siebeck, 2011), 233 (244).
[99] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.
[100] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2002] OJ L 201/37.

concerned, so that very high requirements can be imposed for medical devices, for example, Recital 22 p. 5 Draft Directive on Product Liability. As before, technical standards will therefore play a role in the lack of safety of a *product that should* not be underestimated. The presentation of the *product*, the installation and use instructions and the entertainment also play a major role, Art. 6 (1) a) Draft Directive on Product Liability, as does the reasonably foreseeable misuse of a *product,* Art. 6 (1) b) Draft Directive on Product Liability - here, however, defects that occur later, especially in IT products, will have considerable significance.

It is also important to clarify in Art. 6(2), Recital 25, Sentence 2 of the Draft Directive on Product Liability that newer updates or upgrades do not *per se* lead to the assumption that the previous version was defective, likewise in the case of newer or better later *products*. However, this is not entirely comprehensible, especially for security updates, since if a defect in an IT product is subsequently discovered and "fixed" by such an update, the conclusion that the previous version was defective is obvious; for security updates, therefore, Recital 25, Sentence 2 of the Product Liability Directive-E should not be applied.

Already at this point, the Draft Directive on Product Liability in recital 22 p. 5 hints at a simplification of the burden of proof for the injured party, in that it should be sufficient for courts to no longer have to establish the defectiveness of the specific product if the defectiveness of an entire *product category* is proven, provided that it belongs to the same category. The Product-Liability-D-P thus takes up the principle developed by the ECJ in the *Bosten Scientific Medizintechnik case*[101] and explicitly regulates it. While the ECJ decision still referred specifically to pacemakers and implantable cardioverted defibrillators and was thus issued against the background of the particular health and life risk associated with this *product category*, recital 22 p. 5 of the Product-Liability-D-P now extends the scope of application to all *products* or *product categories*.[102] Nevertheless, also under the Draft Directive on Product Liability, it will be necessary to adhere to the requirement that at least a risk threshold to be determined normatively must be exceeded and that "the mere possibility of a failure of the [...] implanted pacemakers [...] cannot constitute a defect"[103].[104]

However, the fundamental innovations of the Product-Liability-D-P result much more from the additionally listed factors that the courts are to consider when determining faultiness:

[101] ECJ Judgment of 05 May 2015 - C-503/13, C-504/13, ECLI:EU:C:2015: 148, 41 et seq. - *Boston Scientific Medizintechnik GmbH/AOK Sachsen-Anhalt et al = CR,* (2015): 716 (Ls.).
[102] Critical of a generalisation of this case law, Wagner, (n 96), § 3 Rn. 56; *ibid.,* Gerhard Wagner, "Der Fehlerverdacht als Produktfehler," *JZ,* (2016): 292.
[103] This is still the case in the Opinion of Advocate General *Bot* of 21 October 2014 - C-503/13, C-504/13, ECLI:EU:C:2014:2306, 31 - *Boston Scientific GmbH/AOK Sachsen-Anhalt et al.*
[104] In general on this requirement Wagner, (n 96), § 3 marginal no. 56; *ibid.,* (n 102), 292 (296).

b) Self-learning (AI) systems

An important factor for the relevant road safety expectations, especially for AI systems in the field of *machine learning, is* their possible autonomous further development after being placed on the market or put into operation. This effect, which has so far prevented liability for problems occurring after placing on the market that were not foreseeable at that time, at least for legal systems that excluded development errors (such as in Germany), is now taken into account by Art. 6 (1) c) Draft Directive on Product Liability, at least to some extent, in that special safety expectations are to be taken into account here.[105] Accordingly, learning AI systems must also be designed in such a way that they prevent dangerous behaviour of the *product* or AI system; the Draft Directive on Product Liability does not focus on a "reasonable" test, recital 23 p. 2 Draft Directive on Product Liability.

In this context, the further innovation in Art. 6(1)(e) Product-Liability-D-P on the relevant point in time for defectiveness also plays an important role for IT products that are still under the control of the *manufacturer,* which is likely to be the case for numerous connected IT products, especially AI systems; here, the Product-Liability-D-P correctly focuses on the point in time when the *manufacturer* relinquishes control over the IT product or the AI system. Especially when AI systems are continuously monitored with regard to their data sets and their use by the AI system manufacturer, which they may even be obliged to do under the AI Regulation-E ("post market monitoring", Art. 61 AI Regulation-E), they are under the "control of the *manufacturer*", so that the *manufacturer* must continuously ensure the road safety of the IT products or the AI system. Here, too, the Product-Liability-D-P goes beyond the AI Liability-RL-E, which regulates the requirements for data governance (Art. 10 AI-VO-E) only with regard to the burden of presentation and proof with regard to fault-based liability facts.

c) Interaction with other components

Art. 6 (1) d) Draft Directive on Product Liability contains quasi "explosives" for IT products, which, in the context of road safety expectations, requires that the *reasonably to be* expected effects on other *products be* taken into account, especially with regard to interconnected *products* ("inter-connected", recital 23 p. 1 Draft Directive on Product Liability). However, since IT products almost necessarily interact with each other, difficult questions arise here, such as whether the *developer of* an operating system should always take into account the effects of other IT products or software on his own *product.* Since we are dealing here with a multitude of software products that can hardly be surveyed, the criterion of the "*reasonably*" expected effects will be of particular importance. In this respect, it will probably be possible to fall back on the principles developed under the previous legal situation regarding obligations to instruct and observe products: The greater the danger posed by the *product* and its misuse, the more intensive and insistent the instruction and product monitoring

[105] Hofmann, (n 69) 282 (284); Wagner, (n 9) 707 (749); Wagner, (n 96), § 1 Rn. 61.

must be for the buyer - also with regard to such dangers that only arise through the combination of the *product* with other *products* or accessories.[106]

However, with regard to software, it must be pointed out that the standard to be applied to the catalogue of obligations is to be handled *more restrictively* due to the fast pace of development of operating systems and the abundance of combination possibilities with other software and hardware.[107] Consequently, liability for accessories can only be considered if the *manufacturer* himself provides interfaces for other programs or if the programs are in general use and the *manufacturer* must expect them from the outset.[108]

d) Cybersecurity and product safety

Last but not least, Art. 6 (1) f), Recital 24 of the Product-Liability-D-P closes a gap with regard to cyber security for *products,* which, however, only refers to requirements under product security law and has so far only been implemented in rudimentary form throughout the EU; in particular, the Cybersecurity Act[109] does not contain any mandatory schemes for *manufacturers of* IT products, but only their voluntary compliance. With regard to AI systems, however, Art. 15 of the AI-Reg-E explicitly requires "robustness, integrity and cybersecurity", so that the relevant security expectations of traffic in the sense of the Product-Liability-D-P are also defined in this regard. The new proposal for a Cyber Resilience Act (CRA-E), which explicitly provides for security requirements for *products, will also* bring significant improvements here, which are obviously already interlinked with the Product-Liability-D-P and even more so with the KI-VO-E.

e) Development errors

Somewhat hidden in Art. 10 (1) (e), the Draft Directive on Product Liability still excludes the so-called design defect from the liability of the *manufacturer*; according to this, the *manufacturer* can invoke the fact that, according to the objective state of

---

[106] BGH 16 June 2009 - VI ZR 107/08 marginal no. 24 = BGHZ 181, 253; BGH 24 January 1989 - VI ZR 112/88 = BGHZ 106, 273; BGH 16 December 2008 - VI ZR 170/07 = BGHZ 179, 157; Spindler, (n 96), § 823 marginal no. 654; Thomas M. J. Möllers, "Nationale Produzentenhaftung oder Europäische Produkthaftung? Zur Bindung der Rechtsprechung im Rahmen der deliktsrechtlichen Generalklausel an die Vorgaben des ProdHaftG und des ProdSG," *VersR,* (2000): 1177 (1181).

[107] Johannes Droste, "Produktbeobachtungspflichten der Automobilhersteller bei Software in Zeiten vernetzten Fahrens," *CCZ,* (2015): 105 (107); similarly BGH 09 December 1986 - VI ZR 65/86 = BGHZ 99, 167.

[108] Gerald Spindler, *Responsibilities of IT manufacturers, users and intermediaries*, study commissioned by the BSI, (Baden-Baden: Nomos, 2007), 62 with further references.

[109] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Cyber Security Agency) and on cyber security certification of information and communication technology and repealing Regulation (EU) No 526/2013 (Cyber Security Legislative Act), [2019] OJ L 151/15.

science and technology, a product defect was not recognizable at the time of placing the *product* on the market or at the time when the product was under the control of the *manufacturer*. *In* contrast to the previous Product Liability Directive, which also provided for the design defect exception as an option for the Member States[110] , this exception is now *mandatory in* nature and must therefore be implemented by all Member States. The *state of the art in science and technology*[111] will therefore be decisive, although this does not necessarily run parallel to the German understanding. This is not to be underestimated for AI systems that learn themselves, as their further development after market launch can lead to the acceptance of development errors.[112] However, AI systems in particular will usually remain under the control of the manufacturers long after their market launch, so that the exception will not apply here.

f) Updates and upgrades, machine learning

A distinction must be made between the development defect, in which the defect was already present when the *product was* placed on the market but could not be discovered, and the case where the defect in the product only occurred subsequently, i.e. after the product was placed on the market. In principle, Art. 10(1)(c) Draft Directive on Product Liability also provides for an exemption from liability of all parties involved, which is, however, considerably - and rightly - relativised by Art. 10(2) Draft Directive on Product Liability: According to this, the exemption from liability does not apply if, during the *manufacturer*'s control over the *product*, the defectiveness is caused by a *connected service*, by software including updates or upgrades or by their absence, provided that the safety of the *product is at* issue. Recital 37 S. 3 Product-Liability-D-P also includes machine learning, as long as the AI product or system is under the control of the *manufacturer*.

---

110 Cf. The implementation of Art. 7 lit. e ProdHaft-RL in § 1 para. 2 no. 5 ProdHaftG, without making use of the opening clause in Art. 15 para. 1 lit. b ProdHaft-RL; on the German implementation see Wagner, (n 96), § 1 Rn. 51; Ehring, (n 97), § 1 Rn. 97; Christian Förster, «§ 1 ProdHaftG », in *BeckOK BGB*, ed. Wolfgang Hau et al. 63rd ed. (München, C.H. Beck, 2022), Rn. 53 ff.

111 Cf. On the relevant differentiation in German law in particular BVerfG decision of August 08, 1978 - 2 BvL 8/77 = BVerfGE 49, 89 = *NJW,* (1979): 359 (362) - Kalkar; BGH of 5 February 2013 - VI ZR 1/12 marginal no. 13 = *NJW,* (2013): 1302; BGH of June 16, 2009 - VI ZR 107/08 Rn. 15 = BGHZ 181, 253 with further references; Spindler, (n 96), § 823 Rn. 633; Wagner, (n 96), § 823 Rn. 953, Thomas Klindt and Boris Handorn, "Haftung eines Herstellers für Konstruktions- und Instruktionsfehler," *NJW,* (2010): 1105; Peter Marburger, *Die Regeln der Technik im Recht*, (Köln: Heymann, 1979), 429.

112 Friedrich Graf Von Westphalen, "Haftungsfragen beim Einsatz Künstlicher Intelligenz in Ergänzung der Produkthaftungs-RL 85/374/EWG," *ZIP,* (2019): 889 (892); but much narrower Malte Grützmacher, "Die deliktische Haftung für autonome Systeme – Industrie 4.0 als Herausforderung für das bestehende Recht?," *CR,* (2016): 695 (696); see also Herbert Zech, "Künstliche Intelligenz und Haftungsfragen," *ZfPW,* (2019): 198 (213); *id.,* (n 87) A 71.

Implicitly, the Product-Liability-D-P thus introduces a non-contractual duty for updates for security, as otherwise the IT product must be considered defective. However, much depends on whether the IT product is still under the control of the *manufacturer* - because only then does the re-exception apply. This means that a *manufacturer is still* free not to opt for permanent support or updates. On the other hand, ErwGr 38 S. 3 Product-Liability-D-P explicitly refers to the Medical Devices Regulation, here Annex I Chapter I No. 3 (EU) 2017/745[113] and requires *manufacturers to* provide security updates, especially with regard to cybersecurity risks - however, the Medical Devices Regulation is not particularly clear in this respect, as it only requires reliability of the electronic components including software, which can also include security updates.[114] In contrast, the proposal for a Cyber Resilience Act apparently assumes an obligation under product safety law for lifelong updates, Annex I No. 1 k) in conjunction with Art. 5 of the proposal, which is, however, considerably relativised by the limitation to a five-year obligation to verify compliance with the requirements by the *manufacturers, Art.* 10 Para. 6, 12, Art. 23 Para. 2 CRA E.[115]

In contrast, Section 327f of the BGB provides for traders' update obligations in implementation of Art. 8(2) of the Digital Content Directive[116] . This obligation can then exist independently of the obligation under the Product-Liability-D-P. This may well result in overlaps, as the Product-Liability-D-P also covers dealers in any case, provided the actual manufacturer is not "tangible". On the other hand, unlike under the Product-Liability-D-P, the contractual obligation of the trader applies regardless of whether the trader himself still has control over the product.

Recital 38 p. 4 Product-Liability-D-P, however, establishes the – self-evident – principle that liability must be excluded if the IT product user or owner does not install the update. However, how to deal with cases in which the user is not aware of updates that have been made available remains open, as does how the *manufacturer should be* able to prove this. This, too, would tend to argue in favour of limiting liability for updates to cases in which the *manufacturer* still exercises control over the IT product.

4. Liability addressees

The Product-Liability-D-P also contains some interesting innovations with regard to the addressees of liability: In addition to the traditional concept of manufacturer

---

[113] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 concerning medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, [2017] OJ L 117/1.

[114] Gerhard Wiebe, "Produktsicherheitsrechtliche Pflicht zur Bereitstellung sicherheitsrelevanter Software-Updates," *NJW,* (2019): 625 (626).

[115] See also Yannick Zirnstein, "Der Entwurf des Cyber Resilience Act," *CR,* (2022): 707.

[116] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contract law relating to the provision of digital content and digital services, [2019] OJ L 136/1.

and the liability of *importers,* the Product-Liability-D-P now expressly extends liability to so-called "*fulfilment providers*", i.e. *services that* serve to provide logistical support for a product import (without being *importers* themselves), up to the possible liability of online platforms.

a) Manufacturers, especially software developers

First of all, Art. 7(1) of the Draft Product Liability Directive refers to the *manufacturer* as the traditional addressee of liability, which is defined in more detail in Art. 4 No. 11 of the Draft Product Liability Directive. In this respect, the Product-Liability-D-P does not contain any surprises, since just as in the still valid ProdHaft-RL, developers are also covered, as are those who distribute third-party products under their own name or trademark ("quasi-manufacturers").[117]

b) Suppliers, in particular service providers

Even if at first glance nothing changes with regard to the joint and several liability of *manufacturers* and *suppliers*, Art. 7(1) sentence 2 of the Draft Directive on Product Liability, it should not be overlooked that the extension of the *concept of product* and *component* (Recital 26 of the Draft Directive on Product Liability), e.g. to *connected IT services*[118] , entails a considerable expansion of the addressees of liability. In relation to AI systems, data suppliers, for example, can easily fall under the *definition of supplier* and thus under strict no-fault liability, but also other connected services.

c) Extension of the concept of importers to fulfilment providers

Also significant is the (subsidiary) extension of the importer's liability also contained in the ProdHaft Directive-E (Art. 7(2)) to so-called "*fulfilment providers*", who take over the logistical handling of the import of a product if neither the *manufacturer* nor the *importer is* domiciled in the EU, Art. 7(3) ProdHaft Directive-E. Article 4(14) of the Draft Directive defines this term in more detail as *commercial services that* fulfil at least two of the criteria "warehousing, packaging, addressing and dispatching of a product", excluding any freight and postal services.

For example, these criteria could apply to *Amazon Marketplace if Amazon* stores third-party products and then delivers them to the end customer if the actual retailer is not located in the EU. On the one hand, the previous Product Liability Directive did not even know the term "*fulfilment provider*" and, on the other hand, the importer activity had to take place "for the purpose of sale, hire, hire-purchase or other form of distribution with an economic purpose" according to Art. 4(2) of the Product

[117] Cf. Art. 3 para. 1 ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC, § 4 para. 1 p. 2 ProdHaftG; on this Wagner, (n 96), § 4 marginal no. 33; Andreas Spickhoff, «§ 4 ProdHaftG», in *BeckOGK*, ed. Beate Gsell et al. (München: C.H. Beck, status May 01, 2021), marginal no. 26 ff.
[118] See above B. II. 1. b).

Liability Directive. Thus, the decisive factor was the control of the import and not merely its implementation.[119] With the new regulation, the *EU Commission rightly* wants to close a gap that has arisen precisely due to such business practices in which a classic *importer* cannot be found in the EU, but these service providers take over parts of their tasks without themselves being able to be qualified as *importers*. The *EU Commission uses the* parallel approach in the Market Surveillance Regulation[120] , which in its Art. 4-7 also places the "fulfilment service providers" within the meaning of Art. 3 No. 11 of Regulation (EU) 2019/1020 under the obligation. However, recital 27 of the Product-Liability-D-P only wants to make these "fulfilment service providers" liable if they cannot name a *manufacturer* or *importer* in the EU.

d) Online platforms

Art. 7(6), Recital 28 of the Draft Directive on Product Liability goes even further, which also makes online platforms that facilitate distance contracts liable, albeit in accordance with Art. 6(3) of the Digital Services Act. Accordingly, the decisive factor – in the wake of the ECJ's *Wathelet ruling*[121] – is whether the consumer perceives the platform as the actual provider or whether the *trader* or *manufacturer* is under the supervision of the platform.[122] This provision is also in line with the proposal for a general product safety regulation,[123] which provides in Art. 20(5)(a) that online marketplaces must provide "*the name, registered trade name or registered trade mark of the producer and a postal or e-mail address at which he can be contacted*". Recital 36 Product-Liability-D-P further clarifies that online marketplaces should ensure that, for product traceability purposes, traders comply with their information obligations under the DSA and the Product Safety Regulation-E and do not allow (product) listings by

[119] OGH January 26, 1995 - 6 Ob 636/94 = *JBl.*, (1995): 456 (457); Wagner, (n 96), § 4 Rn. 45; Georg Borges, «§ 4 ProdHaftG», in *BeckOK IT-Recht*, ed. Georg Borges and Marc Hilber, 7th edn. (München: C.H. Beck, 01.10.2021), Rn. 47; Friedrich Graf von Westphalen, "Das neue Produkthaftungsgesetz," *NJW,* (1990): 83 (89).

[120] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and the conformity of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, [2019] OJ L 169/1.

[121] Ec; Rupprecht Podszun and Philipp Offergeld, "Plattformregulierung im Zivilrecht zwischen Wissenschaft und Gesetzgebung: Die ELI Model Rules on Online Platforms," *ZEuP,* (2022): 244 (258).

[122] For more details see Gerald Spindler, "Der Vorschlag für ein neues Haftungsregime für Internet-Provider – der EU Digital Services Act (Teil 1)," *GRUR,* (2021): 545 (549); Busch, *EuCML,* (2021): 109 (111, 114); Rössel, *ITRB,* (2021): 35 (36); Gerald Spindler and Simon Gerdemann, "Das Gesetz über digitale Dienste (Digital Services Act) - Teil 1," *GRUR,* (2023): 3, "Das Gesetz über digitale Dienste (Digital Services Act) (Teil 2)," *GRUR,* (2023): 115.

[123] Commission, "Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council", COM (2021) 346 final June 30, 2021.

traders who do not comply with the relevant information obligations. *"However, the online marketplace should not be responsible for checking the completeness, correctness or accuracy of the information itself, as the obligation to trace the products still lies with the trader"* (recital 36 p. 5 General Product Safety Regulation-E). Liability under the Product Liability Directive remains expressly unaffected under Article 39 (2) of the Draft General Product Safety Regulation.

However, the reference to Art. 7(5) of the Draft Directive on Product Liability also requires that the injured party has unsuccessfully requested the platform operator to disclose the identity of the *manufacturer/importer,* etc. within a period of one month. On the other hand, ErwGr 28 S. 2 Product-Liability-D-P states that the liability privileges of the Digital Service Act remain applicable if they only assume an intermediary role. There are no special features for AI systems in this respect.

e) No exception for SMEs

The EU Commission explicitly excluded an exemption for SMEs in its proposal - with the correct reason that it is irrelevant for an injured party whether the damage was suffered by a larger or a small company.[124] In fact, in terms of the internalisation of external effects (i.e. damages), it does not matter what size the damaging party is.

f) Modification of products, especially recycled products

Article 7 (4) of the Draft Directive on Product Liability, which states (or clarifies)[125] that *modifications to* a *product* already placed on the market or outside the control of the *manufacturer* that have an impact on product safety must also be considered a new *product, is* aimed at a problem that at first glance seems to be outside the IT sector. In view of *modifications of* IT products or services or components in particular, which ErwGr 29 S. 2 Product-Liability-D-P states for upgrades in particular, this innovation is certainly applicable in the IT sector - even if the open source sector is explicitly excluded. Art. 10 para. 1 g), Recital 29 p. 4 of the Draft Directive on Product Liability limits the liability of the person who has modified the *product to the* corresponding modified part of the *product.*

For the liability of AI systems, this extension can be significant if the *manufacturer* itself does not control the AI system, but a third party trains or "educates" the AI system with new data sets. However, how to separate the changed from the unchanged parts of the systems seems hardly feasible in practice.

---

[124] EU Commission, "Explanatory Memorandum to the Product-Liability-D-P", COM (2022) 495 final, 10 ff.

[125] For a similar discussion under the ProdHaft-RL, Irina Rebin, «§ 2 ProdHaftG», in *BeckOGK*, ed. Beate Gsell, et al. (München: C.H. Beck, 2022 status September 01, 2022), Rn. 11: depending on individual circumstances.

5. Liability exceptions

The liability exceptions are also partly taken over from the previous ProdHaft Directive[126] , but partly modified considerably, especially with regard to the extension of the concept of product to include connected services and software.

The principle that a *manufacturer* or *importer* cannot be held liable if he proves that he did not himself place the *product on the* market remains unaffected, Art. 10(1)(a) Product-Liability-D-P.[127] The same applies to *distributors*, Art. 10(1)(b) Product-Liability-D-P. The exemption from liability in the event that the defectiveness of the *product* results from mandatory provisions of public law is also continued, Art. 10(1)(d) Product-Liability-D-P.[128]

Also known is the liability exception for *suppliers* (or "*components*") in Art. 10 (1) f) Product-Liability-D-P, if the defectiveness of the *component* results from the design of the main product or the instructions of its manufacturer.[129]

As already mentioned, the Product-Liability-D-P still provides for the exception for development defects – but now of a mandatory nature for the Member States and not as an option. The liability exceptions for updates and upgrades have also been modified (see II.3.a) above).

New, on the other hand - but in principle self-evident - is Art. 10 (1) g) Product-Liability-D-P, which limits the liability of the "new" manufacturer for *modifications of* a *product to* the modified parts.

6. Disclosure obligations and burden of presentation and proof

One of the other important adjusting screws in product liability concerns the distribution of the burden of presentation and proof, which, with regard to defectiveness

[126] Cf. The predecessor regulation in Art. 7 ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC.

[127] Cf. The predecessor regulation in Art. 7 lit. a ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC.

[128] Cf. The previous provision in Art. 7 lit. d ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC.

[129] Cf. The predecessor provision in Art. 7 lit. f ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC; on the implementation in § 1 para. 3 p. 1 ProdHaftG see Maximilian Seibl, «§ 1 ProdHaftG», in *BeckOGK*,ed. Beate Gsell et al. (München: C.H. Beck, status October 01, 2022), marginal no. 129; Wagner, (n 96), § 1 marginal no. 63. ff.

and causality, has so far been borne by the injured party in full,[130] which is a considerable obstacle for injured parties, especially for IT products and even more so for AI systems.[131]

In itself, Art. 9(1) Product-Liability-D-P adheres to the principle that the injured party must prove both the defectiveness, the infringement of the legal interest and the damage as well as the causality. However, the *EU Commission* recognises the practical problems just described of an injured party who has hardly any access to information that would allow him to prove the defectiveness of an (IT) product, as well as the causality between the defect of the *product* and the infringement of the legal interest, recital 30 p. 2, 3 Product-Liability-D-P. 2, 3 Product-Liability-D-P ("*information asymmetry*"). The *EU Commission* addresses this problem with two solutions:

a) on the one hand, an easing of the burden of proof by introducing an obligation to disclose information of the potential tortfeasor, Art. 8 Product-Liability-D-P;

b) on the other hand, through presumptions of evidence and prima facie evidence orders in Art. 9 Product-Liability-D-P.

a) Disclosure obligations

Article 8 (1) of the Draft Directive on Product Liability obliges the Member States to allow the courts to oblige a potential tortfeasor or defendant to disclose relevant facts at the request of the plaintiff, who can plausibly demonstrate that he is entitled to compensation. This is similar in approach to the US *pre-trial disclosure procedure*, but depends crucially on a pending lawsuit. The documents to be submitted do not only include the evidence already held by the defendant, but may also include new documents or reports to be created, ErwGr 31 S. 2 Product-Liability-D-P.

---

130 Art. 4, 7 ProdHaft-RL 85/374/EEC last amended by RL 1999/34/EC; on the implementation of § 1 para. 4 ProdHaftG Seibl (n 128) § 1 marginal no. 141; Wagner, (n 96), § 1 Rn. 77; Borges, (n 119), § 1 ProdHaftG Rn. 93; the injured party bears the burden of proof for the existence of the product defect, the damage, the causal connection, cf. BGH February 05, 2013 - VI ZR 1/12 marginal no. 19 = *NJW,* (2013): 1302; OLG Brandenburg, December 14, 2015 - 1 U 8/13 = *NJW-RR,* (2016): 220 (221); OLG Frankfurt a. M. June 08, 1993 - 14 U 116/92 = *NJW-RR,* (1994): 800 (801); the manufacturer bears the burden of proof for the existence of an exclusion according to § 1 para. 2, 3 ProdHaftG.

131 Gerald Spindler, "Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären", Studie im Auftrag des BSI, [*Responsibilities of IT manufacturers, users and intermediaries*, study commissioned by the BSI] 2007, 76, accessed October 1, 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2; Gerald Spindler «Haftung im IT-Bereich»*in Karlsruher Forum 2010: Haftung und Versicherung im IT-Bereich,* ed. by Egon Lorenz (Karlsruhe: Verlag Versicherungswirtschaft, 2011), 39 ff.

In order not to let the submission of facts etc. get out of hand - as is known from *pre-trial disclosure proceedings*[132] - Art. 8 (2) Product-Liability-D-P explicitly limits this duty to the *necessary* and *proportionate* facts *to* substantiate the claim.[133] In this context, Art. 8(3), (4) Product-Liability-D-P pays special attention to the observance of trade secrets and the protection of confidential information, which, however, according to Art. 8(4) Product-Liability-D-P should not be an insurmountable obstacle, as the member states are also obliged to authorise their courts to take "specific measures" to protect confidentiality if the defendant is obliged to disclose the confidential information. This is already known in Germany, for example, in patent proceedings through the "in camera" procedure, in which a third party bound to professional secrecy can inspect the documents.[134] However, recital 32 p. 2 Product-Liability-D-P goes even further, in that the *EU Commission* apparently considers a restriction of access to the secret documents to a certain group of persons to be sufficient, or in that only redacted minutes of evidentiary hearings or hearings are admitted. In any case, recital 32 p. 3 Product-Liability-D-P requires a comprehensive weighing of the interests of the plaintiff and the defendant, in particular the effects on the action as well as potential damages for the defendant or third parties affected. In contrast, a much more extensive approach is taken in US civil procedure law. In addition to third parties not involved in the proceedings who can be called upon in *pre-trial disclosure proceedings*[135] , the documents and information to be provided by the parties are subject to hardly any restrictions[136] and certainly hardly any

[132] Haimo Schack, *Einführung in das US-amerikanische Zivilprozessrecht*, 5th edn. (München: C.H.Beck 2020), 111; Hanns Prütting, *AnwBl,* (2008): 153 (154).

[133] Peter Gottwald, «Internationales Beweisrecht § 10», in *Internationales Zivilprozessrecht*, ed. Heinrich Nagel, Peter Gottwald, 8th edn. (Köln: Verlag Dr. Otto Schmidt, 2020), Rn. 10.24*;* Schack, (n 132), 48*,* DerekJ.T.Adler, «Is Discovery Necessary? Reflections on Pre-Trial Disclosure and Procedural Fairness», in *Global Wisdom on Business Transactions, International Law and Dispute Resolution, Festschrift for Gerhard Wegen* (München: C.H. Beck, 2015), 569.

[134] BGH November 16, 2009 - X ZB 37/08 = BGHZ 183, 153; see Peter Meier-Beck, "Die Rechtsprechung des Bundesgerichtshofs zum Patent- und Gebrauchsmusterrecht im Jahr 2009," *GRUR,* (2010): 1041 (1046); *ZPO*, Astrid Stadler, «§ 142», in *ZPO*, ed. by Hans-Joachim Musielak and Wolfgang Voit, 19th edn. (München: Verlag Franz Vahlen, 2022) marginal no. 7a.; Hermann Deichfuß, "Rechtsdurchsetzung unter Wahrung der Vertraulichkeit von Geschäftsgeheimnissen," *GRUR,* (2015): 436.

[135] Joachim Zekoll and Jan Bolt, *NJW,* (2002): 3129 (3133); Schack, (n 132), 111.

[136] See FRCP 26 (b) (1): "Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defence of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter".

security precautions,[137] in order to protect trade secrets, for example.[138] Criticism: As laudable as the European approach is, it tends to be too broad due to the relatively low hurdles for the protection of trade secrets; as described, an exclusive entrustment of third parties bound to secrecy would be preferable. The potential scope of Art. 8 Product-Liability-D-P also appears to be insufficiently contoured, as it does provide for the barrier of necessity and proportionality, which in practice, however, will lead to considerable legal uncertainty and will ultimately only emerge through ECJ case law, as injured parties are likely to initially make corresponding requests "out of the blue" in order to obtain corresponding information. Much depends on the requirements for a corresponding application by the plaintiff and its substantiation, e.g. whether blanket requests for surrender are sufficient or whether the application must be limited to the disclosure of the source code or the data sets. Nor has it been clarified how *ex post* disproportionate disclosure of documents could be sanctioned, in particular whether plaintiffs would have to pay damages. Nevertheless, liability is hardly conceivable in the admissible exercise of legal remedies. In the cases decided on liability for intentional immoral damage (section 826 BGB), the focus was therefore always rightly on the abuse of a formal or procedural position.[139] Particularly reprehensible circumstances must therefore be added[140].[141] Especially for producer liability for AI systems, but also for other IT products, this innovation has considerable weight, as plaintiffs may in principle demand access to the source code, as well as the surrender of training and validation data or related

[137] The courts have the instrument of protective orders at their disposal here, but they are rarely used in practice, cf. John K. Setear, "Discovery Abuse Under the Federal Rules: Causes and Cures," *92 Yale L. J.*, (1982): 352 (374).

[138] Schack, (n 132), 111.

[139] BGH July 03, 1990 - XI ZR 302/89 = BGHZ 112, 54 (57); BGH March 05, 1958 - IV ZR 307/57 = BGHZ 26, 391 (396); BSG September 26, 1986 - 2 RU 45/85 = *NJW,* (1987): 2038 (2039); regarding an arbitral award OLG Köln August 07, 2015 - 1 U 76/14 = *SchiedsVZ,* (2015): 295 (297); LAG Schleswig-Holstein August 19, 2015 - 3 Sa 90/15 = *BeckRS,* (2015): 73268 marginal no. 28; concerning the creation of a title through the dunning procedure BGH June 29, 2005 - VIII ZR 299/04 = *NJW,* (2005): 2991; BGH November 11, 2003 - VI ZR 371/02 = *NJW,* (2004): 446 (447) following BGH March 25, 2003 - VI ZR 175/02 = BGHZ 154, 269 (274).

[140] Since RG October 07, 1940 - IV 201/40 = RGZ 165, 26 (28) the RG speaks of "special circumstances", cf. on this and on the development of this term in the jurisprudence Ulrich Foerste, «Die Ausnutzung unrichtiger Urteile als sittenwidrige Schädigung», in *Gründen und Stiften : Festschrift zum 70. Geburtstag des Jenaer Gründungsdekans und Stiftungsrechtlers Olaf Werner,* ed. Ingo Saenger et al. (Baden-Baden: Nomos, 2009): 426 (427).

[141] BGH June 29, 2005 - VIII ZR 299/04 = *NJW,* (2005): 2991 (2993 f.); BGH, September 24, 1987 - III ZR 187/86 = BGHZ 101, 380 (384); OLG Köln August 07, 2015 - 1 U 76/14OLG = *SchiedsVZ,* (2015): 295 (297); OLG Hamm August 11, 2015 - 28 U 136/14 Rn. 63 = *NJOZ,* (2016): 58; KG-November 05, 2012 - 26 U 97/11 Rn. 32 et seq.; preceding LG Berlin May 06, 2011 -22 O 122/09; Musielak, «§ 322», in *ZPO*, ed. Musielak, Voit, 19th edn. (München: Verlag Franz Vahlen, 2022), Rn. 91 mwN; Gottwald, «§ 322», in *MüKo ZPO*, 6th edn. (Baden-Baden: Nomos, 2020): Rn. 223 et seq, 228; Foerste (n. 139): 426 (428) with further references.

algorithms and documentation on the behaviour of the AI systems during training, but also later after market launch.

b) Facilitation of evidence, in particular rebuttable presumptions

Defects: The Draft Directive on Product Liability also provides for significant simplifications of proof, such as the rebuttable presumption (Art. 9(5)) of the defectiveness of the *product if* the defendant does not submit any documents in contravention of an order under Art. 8(1) Draft Directive on Product Liability, Art. 9(2)(a) Draft Directive on Product Liability. Furthermore, rebuttable presumptions of the defectiveness of the *product* shall apply if the plaintiff proves that the *product* does not comply with product safety regulations intended to protect against the damage that has occurred, Art. 9 (2) b) Draft Directive on Product Liability. This includes, for example, the lack of documentation or recording devices - for AI systems, for example, set out in Art. 11, 12 AI-Reg-E - so that the violation of these obligations leads to a presumption of defectiveness. The same should apply if the plaintiff can prove an "obvious malfunction" of the *product* during normal use, Art. 9(2)(c) DRP-E, for which Recital 33 p. 7 DRP-E mentions the case of the exploding glass bottle. This corresponds *largely* to the obligation under German law to secure findings and the reversal of the burden of proof that then applies, but only in the case of fault-based producer liability.[142]

A rebuttable presumption shall also apply to the causality between the defectiveness of the *product* and the damage that has occurred, if the defectiveness has been proven beforehand and it is a typical course of events, Art. 9 (3) Draft Directive on Product Liability. However, it is apparently not sufficient for a presumption of fault pursuant to Art. 9(2) of the Draft Directive on Product Liability to apply, as Art. 9(3) expressly speaks of proof.

This is also supported by the additional presumption rules in Art. 9(4) of the Draft Directive on Product Liability: Accordingly, a court may determine that the plaintiff or injured party is facing considerable difficulties ("excessive difficulties") with regard to proving defectiveness or causality due to *technical* or *scientific complexity*. In this case, the presumption of defectiveness as well as causality will apply if the plaintiff has shown ("sufficiently relevant evidence") that the product contributed to the damage and that it was probably defective and probably caused the damage. However, Art. 9(4) of the Draft Product Liability Directive does not contain any statement on the requirements for establishing *technical* or *scientific complexity*, in particular whether the plaintiff has the burden of proof in this respect; only Art. 9(4) sentence 2 of the Draft Product Liability Directive gives the defendant the possibility to dispute the plaintiff's excessive difficulties or the probability of the defectiveness of the *product* and *causality*. What consequence this denial triggers and how this relates to the general rebuttability of the presumption in Art. 9(5) of the Draft Directive on Product Liability remains open.

[142] BGH May 09, 1995 - VI ZR 158/94 = *BGHZ,* (1995): 129, 353 (361).

Recital 34 S. 4 Product-Liability-D-P requires a case-by-case determination of the *technical complexity*, whereby recital 34 p. 5 lists individual factors, in particular the complexity of the *product, e.g. in the case* of innovative medical devices, but also of the machine learning or data that would have to be analysed by the plaintiff. The same applies to causality, for example for a pharmaceutical product and the plaintiff's state of health or if the plaintiff would have to explain the inner workings of an AI system.

In a similar way, recital 34 p. 6 Product-Liability-D-P attempts to clarify the definition of "excessive difficulties" for the plaintiff. Accordingly, within the framework of the court's consideration of the individual case, the plaintiff is not obliged to provide evidence of the existence of these difficulties; it should be sufficient for the plaintiff to provide reasons for this. In particular, recital 34 p. 7 Product-Liability-D-P mentions the case of an AI system for which the plaintiff shall not be obliged to explain its characteristics or its mode of operation or causality for the damage that occurred.

In this context, the relationship between Art. 9(4) of the Draft Directive on Product Liability and the order for the defendant to disclose relevant information under Art. 8 of the Draft Directive on Product Liability remains largely unclear. Recital 34 S. 1 of the Draft Directive on Product Liability only states that the presumptions or the determination of *complexity* by the courts should be without prejudice to the order under Art. 8 of the Draft Directive on Product Liability. However, it remains unclear why a plaintiff should have "excessive difficulties" in proving defectiveness if at the same time he has the possibility to apply for orders under Art. 8 of the Draft Directive on Product Liability; in the sense of *proportionality,* a step-by-step relationship should be assumed here.

As explained, these are rebuttable presumptions (Art. 9 (5) of the Draft Directive on Product Liability), for which the *EU Commission* refers in recital 36 of the Draft Directive on Product Liability to the fact that the defendant can present and prove extraordinary circumstances that exclude liability, for example that the *product* was placed on the market contrary to the *manufacturer*'s intention or that the defect occurred due to compliance with mandatory provisions. However, it should not be sufficient to assume, similar to the principles of *prima facie evidence, that the* rebuttal of the presumption is already based on the invalidation of a principle of experience[143]; neither do the recitals of the Draft Product Liability Directive speak in favour of

[143] BGH December 11, 2018 - KZR 26/17 marginal no. 50 = *WRP,* (2019): 474; BGH January 19, 2010 - VI ZR 33/09 marginal no. 11; BGH May 04, 2012 - V ZR 71/11 marginal no. 13; Hanns Prütting, «ZPO § 286 ZPO», in *MüKo ZPO,* ed. Thomas Rauscher and Wolfgang Krüger 6th edn. (München: C.H. Beck, 2020), Rn. 67; Robert Nober, «§ 286 ZPO», in *ZPO*, ed. Monika Anders and Burkhard Gehle, 80th edn. (München: C.H. Beck 2020), Rn. 86; Ulrich Foerste, «ZPO § 286 ZPO», in *ZPO*, ed. Hans-Joachim Musielak and Wolfgang Voit 19th edn. (München: Verlag Franz Vahlen, 2022), Rn. 23.

this, nor is there any indication in Art. 9 Draft Product Liability Directive that the *EU Commission* "only" wanted to rely on *prima facie evidence* here.

7. Joint and several liability

Art. 11 Product-Liability-D-P maintains the old principle already according to the ProdHaft-RL (Art. 5)[144] that in the case of several possible liability addressees, they are jointly and severally liable for the entire damage. More important in the context of liability for IT products and AI systems, on the other hand, is Article 12 (1) of the Draft Directive on Product Liability, which does not waive the liability of *manufacturers* and others because a third party also contributed to the damage; this also covers cases of a faulty AI system that was also poorly trained by its *operator* (who is not covered by the Draft Directive on Product Liability). However, hacker attacks also do not exonerate the *manufacturer of* a defective IT product, which only made the attack possible through the security gap.

8. No more limitation to maximum liability amounts

Also more than remarkable is the waiver of any maximum liability amount in Art. 13 of the Product-Liability-D-P, neither of a contractual nature[145] nor through member state regulations - in contrast to Art. 16 para. 1 ProdHaft-RL, which still provided for the possibility of limiting liability to 70 million ECU or 85 million Euro (section 10 para. 1 ProdHaftG) at the intervention of Germany, but which has not yet been put into practice.[146] This principle of unlimited liability regardless of fault is hardly found in other strict liability regulations and is all the more astonishing since the question of insurability is also at issue; likewise against the background that pure *data loss* or the *corruption of data is* now also to be recognized as a legal asset.

9. Limitation

Art. 14 Product-Liability-D-P also provides for a limitation regime that is largely similar to sections 195 ff, in particular section 199 BGB. According to this, claims become time-barred within 3 years after the *injured party has become aware of* the damage, the defectiveness and the identity of the possible tortfeasors. Art. 14 Product-Liability-D-P equates this with the *"reasonably" expected knowledge of the injured party, which in* this respect deviates from the standard of section 199 para. 1 no. 2 BGB, which refers to grossly negligent ignorance of the injured party; apparently the *EU Commission* uses an objective standard here, which moreover already intervenes with

144 Wagner, (n 96), § 5 Rn. 1; Georg Schäfer, «§ 5 ProdHaftG», in *BeckOGK*, ed. Beate Gsell et al. (München: C.H. Beck, status October 01, 2022), Rn. 1; Langen, «§ 5 ProdHaftG», in *BGB-Schuldrecht,* ed. Barbara Dauner-Lieb and Werner Langen, (Baden-Baden: Nomos Verlag 2021), Rn. 2.

145 In this context, the contractual limitations of liability of open source products are not covered by the Product-Liabiltiy-D-P because of the general exception.

146 Report of the Commission, COM (2000) 893, January 31, 2001, 21; Spickhoff (n 116) § 10 Rn. 3; Wagner, (n 96), § 10 Rn. 1.

lower requirements for knowledge than section 199 para. 1 no. 2 BGB. In this context, the possibility to order the disclosure of information according to Art. 8 of the Draft Directive on Product Liability may also have an influence on the *"reasonably" expected knowledge of* the injured party. However, according to Art. 14 (1) sentence 2, the Draft Directive on Product Liability does not affect provisions of the Member States on the interruption of the limitation period.

In addition, Art. 14 (2) Product-Liability-D-P prescribes an *absolute* statute of limitations of 10 years after the *product has been* put on the market or has been *substantially modified*. Strangely enough, Art. 14(2) Product-Liability-D-P does not additionally refer to the *manufacturer*'s relinquishment of control over the *product*; this would result in sensitive liability gaps in the case of updates, since the actual IT product was placed on the market long before the update, and damage caused by the *product would become* statute-barred within 10 years after this point in time, despite updates having been made. Here, much depends on whether the *product* is to be considered substantially *modified by* the updates, so that the limitation period starts anew.

This *absolute* limitation period is extended to 15 years in cases where the injured party was not able to assert the claim due to late or long-term effects of an injury, Art. 14(3) Product-Liability-D-P, which only covers long-term health injuries.[147]

10. Relationship Product-Liability-D-P to the liability of internet intermediaries

Delicate problems are also posed by the provisions on the liability of operators of *interconnected services* on the liability privileges according to Art. 4 ff. Digital Services Act (formerly: Art. 12 et seq. E-Commerce Directive and sections 7 - 10 TMG). For as far as these *services* now also fall within the scope of liability of the Product-Liability-D-P, they inevitably come into conflict with the exemption from liability, e.g. of access providers, when it comes to the mediation of e.g. the access of *connected services to* a *product*. However, this does not apply to the *manufacturer*'s own services; likewise, the liability privileges in this area only affected liability for content, but not for cybersecurity risks.[148]

---

147 Cf. on late/long-term damage in German limitation law Gerald Spindler, «BGB § 199 BGB», in *BeckOK BGB*, ed. Georg Bamberger and Herbert Roth, 63rd edn., (München: C.H. Beck, 2022), marginal no. 36; Helmut Grothe, «BGB § 199 BGB», in *MüKoBGB*, ed. Franz Jürgen Säcker et al., 9th edn. (München: C.H. Beck, 2021), marginal no. 11; Andreas Piekenbrock, «BGB § 199 BGB», in *BeckOGK*, ed. Beate Gsell et al. (München: C.H. Beck, status August 01, 2022), marginal no. 62 ff.

148 Gerald Spindler, «TMG before § 7», ed. Gerald Spindler and Peter Schmitz, 2nd edn. (München: C.H. Beck, 2018), marginal no. 32; Andreas Sesing, «TMG § 7», in *BeckOK IT-Recht*, ed. Georg Borges and Marc Hilber, 7th edn. (München: C.H. Beck, July 01, 2022), marginal no. 29; Ulrich Sieber and Frank Michael Höfinger, *MMR-HdB*, ed. Thomas Hoeren, Ulrich Sieber and Bernd Holznagel, 58th edn. (München: C.H. Beck, work status: March 2022), part 18.1 General principles of liability marginal no. 38.

III. The AI Liability Directive Proposal

1. Overview

Characteristic for the AI Liability Directive-E and the fundamental decision of the *EU Commission not* to develop too strict liability rules in order not to slow down the development of AI within the EU[149] is the renunciation of the introduction of strict liability and the restriction to rules on the burden of proof for fault-based non-contractual liability. The AI Liability Directive-E thus falls far short of the proposals of the European Parliament, but also of the *Expert Group on Liability and New Technologies*[150] , both of which advocated the introduction of strict liability. However, the emphasis on innovation-friendliness of the AI Liability Directive-E is in remarkable contrast to the strict liability of the ProdHaft Directive-E, which is explicitly intended to cover AI systems, including *connected services* and *suppliers*, including data suppliers. The AI Liability Directive-E therefore largely applies "only" to the *operators of* the AI systems or to *non-manufacturers, so that it* seems questionable why innovations are to be expected here in particular - instead of with the *manufacturers* and the *suppliers*.

Central to the AI Liability Directive-E is the specification of rules on the burden of proof and presumptions with regard to the interlocking with the product safety law provisions of the AI Regulation-E. The *EU Commission* sees the *autonomous behaviour* and *complexity of* AI systems as the decisive cause for the problems of injured parties in asserting claims against *operators* or *users of* AI systems, Recital 4 of the AI Liability Directive. This is all the truer as the AI Regulation provides for obligations for *operators of high-risk AI systems* to document and log, but no rights of affected parties to inspect the documentation, Recital 16 AI Liability Directive. In this way, the *EU Commission* is attempting, as in the case of the Product Liability Directive-E, to establish a parallelism between product safety and product liability – which, however, is confronted with the same concerns as with the terminology of the AI Regulation-E (see b) above).

2. Scope of application

a) Definition of AI

The AI Liability Directive-E adopts the definitions of the AI Regulation-E regarding the definition of AI itself as well as the category of *high-risk AI systems* according

[149] See EU Commission, Explanatory Memorandum to the AI Liability Directive-E, COM (2022) 496 final 2022/0303 (COD), 6.

[150] European Commission, Directorate-General for Justice and Consumers, "Liability for artificial intelligence and other emerging digital technologies", Publications Office, 2019, 39 ff., 42 ff., https://data.europa.eu/doi/10.2838/573689.

to Art. 6 (1) AI Regulation-E and those of the *operators* (Art. 3 (2) AI Regulation-E) and the *users* (Art. 3 (4) AI Regulation-E).

Thus, the AI Liability Directive-E ultimately exposes itself to the same criticism as that already voiced for the AI Regulation-E, in particular the overly broad scope of application, which, as is well known, covers a multitude of algorithm-driven processes and is not limited to machine learning[151].[152] The same applies to the definition of *high-risk AI systems*.[153] In this respect, the AI Regulation-E distinguishes between the *high-risk AI systems* mentioned in Art. 6 (1) in conjunction with Annex II AI Regulation-E, which are *products* or safety components of *products*, as well as such independent systems, which are enumerated in Art. 6 (2) in conjunction with Annex III AI Regulation-E. Particularly in view of the areas of application listed in Annex III AI-Reg-E, it is questionable whether all systems to be classified as high-risk are really included here.[154] According to Article 7 (1) of the AI-Reg-E, it is possible for the *EU Commission to* expand Annex III of the AI-Reg-E by delegated act and to include new systems that are used in one of the areas listed in Annex III Nos. 1-9 of the AI-Reg-E and that pose a particular risk as defined in Article 7 (1) of the AI-Reg. Article 7(1)(b) of the AI Regulation-E.[155] However, it remains to be seen whether the *EU Commission's* annual review of the list in Annex III of the AI Regulation is sufficient in an economic environment characterized by rapid change and innovation. There are further reservations about the list in Annex III AI-Reg-E, as it covers fields of application such as the use of AI in criminal prosecution or in court, which always require a particularly sensitive handling of the civil liberties in

[151] This is the proposal by Philipp Hacker, "Europäische und nationale Regulierung von Künstlicher Intelligenz," *NJW,* (2020): 2142 (marginal no. 6).

[152] Critical of the broad scope of application: David Bomhard and Marieke Merkle, "Europäische KI-Verordnung," *RDi,* (2021): 276 (277, para. 5 ff.); Martin Ebers et al.*,* "Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf," *RDi,* (2021): 528 (529, para. 6 ff.)*;* Roos Philipp Roos and Caspar Alexander Weitz, "Hochrisiko-KI-Systeme im Kommissionsentwurf für eine KI-Verordnung," *MMR,* (2021): 844 (845); Maria Heil, "Die neue KI-Verordnung (E) - Regulatorische Herausforderungen für KI-basierte Medizinprodukte-Software," *MPR,* (2022): 1 (4); Hans Steege, "Chancen und Risiken beim Einsatz künstlicher Intelligenz in der Medizin," *GuP,* (2021): 125 (126); Jan Christopher Kalbhenn, "Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung," *ZUM,* (2021): 663 (664).

[153] Irina Orssich*,* "Das europäische Konzept für vertrauenswürdige Künstliche Intelligenz," *EuZW* (2022): 254 (258); Roos and Weitz, (n 152): 844 (845); Andreas Ebert and Indra Spiecker gen. Döhmann, "Der Kommissionsentwurf für eine KI-Verordnung der EU: Die EU als Trendsetter weltweiter KI-Regulierung," *NVwZ,* (2021): 1188 (1193).

[154] Joint Opinion 5/2021 of the EDPS and the EDPS on the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) June 18, 2021, 19, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf; Roos and Weitz, *MMR,* (n 151) 844 (851); Ebers, et al.*,* (n 152), 528 (531, para. 24) ff.

[155] Kristisch zu diesen Einschränkungen Ebers, et al., (n 152), 528 (531, para. 22 ff.).

question,[156] on the other hand only play a role for liability where state liability may be involved.[157]

The AI Liability Directive-E should also only apply where an AI system has had a direct impact on an injured party. Even the involvement of a human being who bases his or her decision on the recommendations of an AI system but makes it on *his or her own responsibility is* not to be covered by the provisions of the AI Liability Directive-E, recital 15 p. 3 ff. The AI Liability Directive thus indirectly ties in with Article 22 of the GDPR, which in a similar way only subjects AI systems to its requirements if no human evaluation is interposed - and ultimately evokes the same criticism as against Article 22 of the GDPR. Since human omission is also not covered by the presumption rules of Art. 3 f. AI Liability Directive-E, it is doubtful how this is compatible with the requirement of "*human being in the loop*", i.e. the human supervision always required according to Art. 14 AI Regulation-E. In recital 15 p. 5, the AI Liability Directive justifies this restriction by stating that the causality between the fault and the damage can always be established in the case of human intervention. Why this should be different in the direct use of AI systems because of the "black-box problem" is not really clear. AI products without an intervening human are already considered defective according to the Product-Liability-D-P - with the described effects on the question of causality.

b) Restriction to non-contractual fault-based liability

Art. 1 (2) of the draft Directive on liability of insurance undertakings explicitly refers only to fault-based liability, whereby all forms of negligence and intent as well as omission are to be included. Furthermore, state liability is also covered.[158]

Conversely, the AI Liability Directive does not limit itself to purely *tortious* liability, but generally covers all liability, insofar as they are based only on fault; however, Article 1 (2) of the AI Liability Directive explicitly excludes contractual claims. Consequently, as in private international law[159], the question arises as to how *quasi-*

---

156 Ebert and Spiecker gen. Döhmann, (n 152) 1188 (1190) ask against this background whether, in a departure from the previous understanding of procedural law, the use of lie detectors by law enforcement, border and migration authorities would also be permissible, cf. Annex III No. 6 lit. b KI-VO-E.

157 The Product-Liability-D-P would not be affected, however, as the violation of relevant legal interests is unlikely to occur here, especially as freedom is not covered.

158 EU Commission, "Explanatory Memorandum to the AI Liability Directive-E", COM (2022) 496 final 2022/0303 (COD), 11.

159 On the classification of c.i.c. as a tortious act, see the leading decision of the ECJ Judt., 17 September 2002 - C-334/00, ECLI:EU:C:2002:499 Rn. 19 ff. - *Tacconi*; Schinkels in *BeckOGK* Rom II-VO, status August 01, 2018, Art. 12 Rn. 3 ff.; Abbo Junker, in *MüKo BGB*, ed. Franz Jürgen Säcker, 8th edn. (München: C.H. Beck, 2021), Rom II-VO Art. 12, Rn. 6; Andreas Spickhoff, in *BeckOK BGB*, ed. Beate Gsell et al., 63. edn. (München: C.H. Beck, May 01, 2022), Regulation (EC)

contractual claims that are very similar to tortious liability are to be qualified, such as Section 311 BGB; here, there is much to be said for not including these under the exception of contractual liability.

c) Excluded areas

- Transport law: According to Art. 1(3)(a) of the Draft CLD, the Directive is not intended to cover EU liability provisions in the area of transport law, without specifying this in more detail.[160] However, this means that the AI Liability Directive applies to all national liability provisions in the area of transport, unless they are based on transpositions of EU law. In particular, the liability regulations on road traffic law, which are largely national law, such as sections 7 ff. of the Road Traffic Act (StVG) in Germany, would be affected by this. However, due to the minimum harmonization according to Art. 1 para. 4, Recital 14 p. 2 AI Liability Directive-E, this does not mean that strict liability or keeper liability would have to be abolished; "only" fault-based liability would have to be supplemented accordingly, which could affect e.g. the technical supervision according to sections 1d para. 3, 1f para. 2 StVG, section 14 AFGBV, which is liable via section 823 para. 1 BGB.[161]
- Product Liability Directive: Furthermore, Art. 1 (3) b) AI Liability Directive-E provides that the rights of injured parties under the Product Liability Directive remain unaffected, so that the *manufacturer's liability* - and in future also that of *service providers* and *data suppliers* - of AI systems always applies.[162] Nevertheless, a relevant scope of application remains for the AI Liability Directive-E.[163]
- Digital Services Act: Conversely, according to Art. 1 (3) c) AI Liability Directive-E, the *liability privileges of* the Digital Service Act are not to be affected by the AI Liability Directive-E, which is particularly important for intermediaries who provide services for AI systems. The strict feedback to the AI-Reg-E is also shown by the fact that even the regulations of the DSA on algorithms and the use of AI systems on platforms (Art. 12, Art. 14 para. 6, Art. 17 para. 6, Art. 23 para. 1

864/2007 Art. 12, marginal no. 8; Andreas Spickhoff, "Anspruchskonkurrenzen, Internationale Zuständigkeit und Internationales Privatrecht," *IPRax,* (2009): 128 (132); Jan von Hein, "Die culpa in contrahendo im europäischen Privatrecht: Wechselwirkungen zwischen IPR und Sachrecht," *GPR,* (2007): 54 (59); Maximilian Seibl, "Verbrauchergerichtsstände,vorprozessuale Dispositionen und Zuständigkeitsprobleme bei Ansprüchen aus c.i.c.," *IPRax,* (2011): 234 (239); Ansgar Staudinger, "Rechtsvereinheitlichung innerhalb Europas: Rom I und Rom II," *AnwBl,* (2008): 8 (12); Bartosz Sujecki, "Die Rom II-Verordnung," *EWS,* (2009): 310 (318).

160 An overview of relevant regulations in the transport sector can be found at https://eur-lex.europa.eu/browse/summaries.html, accessed October 1, 2023.

161 This is obviously the assumption of the legislator, Begr RegE BT-DruckS. 19/27439, 32; see also Paul T. Schrader, "Wohin steuert das autonome Fahrzeug – vorübergehend?," *ZRP,* (2021): 109 (111).

162 See above B. III. 1.

163 See below B. IV.

lit. c, Art. 27 para. 1 lit. a, Art. 29 para. 2 DSA) are apparently to be excluded from the AI Liability Directive-E or the evidentiary privileges, so that the respective member state regulations remain in place here.

- National law: Finally, Art. 1(3)(d) of the draft Directive explicitly states that the Member States' provisions on the *burden of proof* (cf. sections 138(3), 288, 291 of the Code of Civil Procedure), the assessment *of evidence or* the requirements as to when *evidence* can be presumed (section 286 of the Code of Civil Procedure) remain unaffected, as does the definition of *fault,* recital 10 of the draft Directive. Nor are rules on *damage*, the coverage of multiple tortfeasors or the statute of limitations covered by the AI Liability Directive, Recital 10, Sentence 2, AI Liability Directive-E. Accordingly, Art. 3-4 of the ELD are special provisions that only take precedence over the Member States' standards in these areas.

d) No restriction to certain legal interests or certain injured parties

By limiting itself only to supplementary provisions to Member State rules for *fault-based liability*, the AI Liability Directive deliberately refrains (unlike the ProdHaft Directive) from providing for liability only for certain legal interests[164] . This means that legal interests that do not fall under the protection of property can also fall within the scope of liability of the AI Liability Directive. This means that legal interests that are not subject to property protection can also fall within the scope of liability of the AI Liability Directive, such as *discrimination* or *equal treatment,* recital 2 of the AI Liability Directive. Accordingly, the AI Liability Directive-E is fully accessory to national liability provisions in terms of the facts, insofar as these refer to fault, whereby the form of fault can extend to negligence as well as intent. For German law, this means that, among other things, liability under section 823 (1) BGB as well as section 823 (2) BGB and section 826 BGB is covered, but also, according to the view expressed here, the *quasi-contractual bases of liability* such as section 311 BGB.

But also with regard to the injured parties covered by the protection of the AI Liability Directive-E, there are differences to the Product Liability Directive-E, as the AI Liability Directive-E does not provide for a limitation of the protection to *consumers,* but also covers commercially injured parties in principle in accordance with the Member States' liability rules.

e) Only minimum harmonisation

Moreover, the AI Liability Directive only provides for a minimum level of harmonisation, Art. 1(4), and leaves it up to the Member States to introduce or maintain stricter rules, irrespective of whether these relate to fault-based or strict liability, Recital 14 p. 2 of the AI Liability Directive.

[164] EU Commission, "Explanatory Memorandum to the AI Liability Directive-E", COM (2022) 496 final 2022/0303 (COD), 3.

3. Disclosure of evidence

The central concern of the AI Liability Directive-E is to improve the evidence situation for the injured plaintiff. To this end, the AI Liability Directive-E makes use of two means: (a) on the one hand, the defendant's duty to disclose evidence (disclosure of evidence), (b) on the other hand, presumption of conformity. Both complexes have a number of parallels to the provisions in the Product-Liability-D-P[165] and are based on a common approach.

a) Disclosure of information on high-risk AI systems

Article 3 (1) of the AI Liability Directive allows the court to disclose information or evidence about *high-risk AI systems to the operator* or other parties pursuant to Article 24 or Article 28 of the AI Regulation upon a credible request by the injured party, who had previously unsuccessfully requested the *operator* or other parties to disclose the information. However, Article 3 (1) of the AI Liability Directive does not solve the problem for the injured party of knowing or demonstrating that a *high-risk AI system is* involved at all. According to recital 17, p. 5 of the draft Directive on AI Liability, the mere refusal of the *operator* (or others) should not trigger the presumption of non-compliance with the obligations under the draft CI Regulation.

Such court orders may also be issued against third parties who are not parties to the litigation, in particular if they possess the necessary documentation or information due to their obligations under the CI Liability Directive-E, Recital 19 CI Liability Directive-E. However, disclosure of evidence by third parties should only take place if the evidence cannot be obtained from the defendant, Recital 20, p. 7, CI Liability Directive-E.

In order to counteract unrestrained requests for disclosure of evidence,[166] Art. 3 (2)-(4) of the AI Liability Directive-E (similar to Art. 8 (2)-(4) of the Product-Liability-D-P[167]) also provides for restrictions with regard to *proportionality*, in particular that the plaintiff has previously made sufficient attempts to obtain the relevant information, Art. 3 (2) of the AI Liability Directive-E. Regarding the protection of confidential information or trade secrets, Art. 3(4) of the Draft ECI Liability Directive again only requires the court to take specific measures to ensure confidentiality; as in Art. 8(3) of the Draft ECI Liability Directive, there is a lack of more precise requirements.[168] Only recital 20 p. 5 of the AI Liability Directive-E mentions, similarly to recital 32 p. 2 of the draft directive on the liability of illicit persons mentions restricted access to confidential documents or to relevant negotiations or hearings.

In accordance with the AI Regulation-E, the provisions on the disclosure of evidence are limited to the *operators* etc. of *high-risk AI systems that are* subject to the

[165] See above B. II. 6.
[166] See above B. II. 6. a).
[167] See above B. II. 6. a).
[168] See above B. II. 6. a).

documentation and logging obligations under Art. 18 AI Regulation-E; less risky *AI systems are* thus not subject to the disclosure of evidence, Recital 18 p. 2 AI Liability Directive-E. However, since the AI Liability Directive-E only contains a minimum harmonization, the member states can also provide for more extensive documentation obligations and corresponding disclosures for less risky AI systems.

b) Presumption of non-compliance with obligations

As a consequence of non-compliance with corresponding disclosure orders of the court, Art. 3 (5) of the draft CLD provides for a presumption of non-compliance with the obligations of the draft CLO. Even if the AI Liability Directive-E does not contain a provision on this, such a presumption must be limited to the defendant's non-compliance with the court orders; it cannot apply in the case of a third party's refusal, as the defendant has no influence on this. In any case, the defendant has the possibility to rebut the presumption.

4. Presumption of causality

In addition to the presumption of fault or non-compliance with the obligations of the AI Regulation contained in Article 3(5) of the AI Liability Directive, the AI Liability Directive is limited to presumptions regarding the causality between fault or defective conduct and the damage that has occurred. With regard to the facilitation of proof for non-compliance with obligations or faulty conduct, the AI Liability Directive-E largely refers to national regulations or Union law, recital 22 pp. 2, 3 AI Liability Directive-E, whereby the *EU Commission* is also thinking here of the rules of the DSA in the context of platforms or drones.[169] The plaintiff is therefore not exempt from proving that the AI system was faulty in the first place.

a) Basic rebuttable presumption of causality

Art. 4(1) AI Liability Directive-E contains the *basic rule* that courts should presume causality between a defendant's misconduct and the outcome of the AI system or the plaintiff's injury, provided (a) the plaintiff proves the defendant's misconduct with regard to a duty of care under national or Union law (or it is presumed under Art. 3 para. 5 AI Liability Directive-E) - which at first glance is not limited to the duties under the AI Regulation-E, but is relativised by Art. 4 (2) AI Liability Directive-E - (b) it appears probable that the misconduct "influenced" the outcome of the AI system and (c) that the plaintiff has made a prima facie case that the outcome of the AI system caused the damage. This presumption is rebuttable according to Art. 4(7) AI Liability Directive-E.

In this context, it seems important that recital 22, p. 5-7 of the draft Directive on liability in cases of criminal offences – of course – states that only those obligations can trigger the presumption of causality that serve to protect the injured party, not,

[169] EU Commission, "Explanatory Memorandum to the AI Liability Directive-E", COM (2022) 496 final 2022/0303 (COD), 13.

for example, obligations to inform authorities, which recital 25, p. 4 of the draft Directive on liability in cases of criminal offences reaffirms.

b) Presumption of causality towards operators of high-risk AI systems

Moreover, the presumption of causality only applies to *operators of high-risk AI systems* that are subject to the requirements under Chapters 2 and 3 of Title III of the AI Regulation-E or to persons with obligations under Art. 24 or 28(1) of the AI Regulation-E, Art. 4(2) of the AI Liability Directive-E. The presumption also depends on the plaintiff credibly demonstrating that the *operator* etc. has breached several of the obligations under Art. 10 et seq. AI-Reg-E have been breached. These include (*alternatively*):

- the obligations to train the AI system with data sets that meet the requirements of Art. 10 (2) - (4) AI Regulation-E,
- the transparency obligations of Art. 13 AI-Reg-E,
- the duty of human supervision according to Art. 14 AI-VO-E,
- the duty of robustness, accuracy and cybersecurity, Art. 15, 16 a) AI-Reg-E, or
- the absence of corrective or recall measures pursuant to Art. 16 g), 21 AI Regulation-E.

The AI Liability Directive-E wants to include the measures according to the risk management system according to Art. 9 of the AI Regulation-E in the consideration, although the concrete weight of the respective measures apart from the mentioned obligations remains unclear, Recital 26 p. 4 ff. 4 ff. AI Liability Directive-E. The fact that the risk management system is a comprehensive instrument under the AI Regulation does not ultimately help in assessing whether an *operator* has violated its specific obligations.

However, a court should not apply the presumption if the defendant can show that the plaintiff had sufficient access to relevant expertise to prove causation, Art. 4(4) AI Liability Directive-E. Recital 27 S. 2 of the AI Liability Directive refers to cases in which the plaintiff has access to documentation and logging tools of the AI system - ultimately cases of disclosure of evidence.[170]

c) Presumption of causality for users of high-risk AI systems

For users of AI systems, the AI Liability Directive-E restricts the presumption of causality in Art. 4(3) to cases where the plaintiff proves (and not only makes a prima facie case – "proves") that the *user did* not follow his duties to use or monitor the AI system according to the relevant instructions or interrupted the use, Art. 29 AI Regulation-E, or alternatively did not train the AI system with appropriate data (Art.

[170] So then also EU Commission, "Explanatory Memorandum to the AI Liability Directive-E", COM (2022) 496 final 2022/0303 (COD), 13.

29(3) AI Regulation-E). The AI Liability Directive-E thus considerably restricts the presumption of causality vis-à-vis the *operators of AI* systems, which, however, is in line with the obligations of the AI Regulation-E – but which, conversely, also does not exclude the qualification of such *users* as *manufacturers* under the ProdHaft Directive-E who modify the AI systems on the basis of training with data.[171]

d) Non-professional users of AI systems

A further restriction of the presumption of causality is contained in Art. 4 (6) AI Liability Directive-E for the non-professional use of AI systems. Here, the presumption of causality shall only apply if the non-professional *user* materially interfered with the conditions of the operation of the AI system ("materially interfered with the conditions of the operation of the AI system") or could have determined the conditions of use but failed to do so. Recital 29 p. 6 et seq. AI Liability Directive-E clarifies the references to the *operator*'s instructions for use once again by making it clear that the non-professional *user of* an AI system can also fall under the presumption of causality if he has disregarded these instructions.

e) Presumption of causality for non-high-risk AI systems

Last but not least, Article 4(5) of the AI Liability Directive contains a provision similar to Article 9(4) of the ProdHaft Directive for *operators* or *users of* less risky AI systems: Here, the presumption of causality only applies if the court is convinced that there are considerable difficulties for the plaintiff to prove causality. However, since ErwGr 28 S. 2 of the AI Liability Directive-E again essentially refers to the "black-box" problem of AI systems, this restriction has little effect in practice, as every plaintiff is likely to face this problem. Moreover, according to Recital 28 S. 4 of the AI Liability Directive, the plaintiff should not be forced to explain the characteristics of the AI system or how these lead to the fact that causality cannot be proven – which ultimately softens this restriction considerably.

5. Collective law enforcement

Art. 2 (6) c) AI Liability Directive-E explicitly provides for the possibility that associations or other third parties can collectively assert the rights of injured parties, for which Art. 6 supplements Annex I of Directive EU 2020/1828.[172]

---

[171] See above B. II. 4. b).

[172] Directive EU 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, [2020] OJ L 409/1.

6. Evaluation of the AI Liability RL-E

Finally, Art. 5 and Recital 31 AI Liability Directive-E explicitly provide for the evaluation of the AI Liability Directive-E as a result of the two-stage process envisaged by the *EU Commission,* for example with regard to the introduction of strict liability as proposed by the *EU Parliament.*[173] This is intended to take into account the rapid technological, but also economic development, in order not to nip innovation processes in the bud through excessive liability.[174] However, this is in contrast to the extension of liability in the Product-Liability-D-P (see above B. 0).

IV. Relationship of the AI Liability Directive-E to the Product Liability-Directive-P

The relationship between the new Product-Liability-D-P and the AI Liability Directive does not appear to be simple: Article 2 (3) c), Recital 9 of the Product-Liability-D-P states that it shall not supersede other national liability regimes of both a *contractual* and *non-contractual* nature, including the regulations implementing the AI Liability Directive, but only to the extent that this liability does not relate to the defectiveness of a *product. However*, if one considers that AI itself will generally be software that is covered by the Product-Liability-D-P, since this now also concerns stand-alone software, it is difficult to distinguish defective *AI* from violations of the AI-VO-E, on which the AI Liability Directive-E is based, because every defective training of an AI with data or the lack of *logging devices* will lead to an AI software being regarded as defective.[175] Ultimately, the scope of application of the AI Liability Directive is noticeably shifted in the direction of the ProdHaft Directive.

An original scope of application therefore remains for the AI Liability Directive-E only regarding the liability based on legal interests of the ProdHaft Directive-E, furthermore its far-reaching limitation of protection to consumers, whereas the AI Liability Directive-E also covers commercially affected persons. Furthermore, the AI Liability Directive-E can also cover violations of fundamental rights, for example, if national law provides for such protection in the area of liability, e.g. in the case of discrimination.[176] Therefore, although the two areas overlap substantially, they have different focal points in *detail.*

---

[173] See above (n 80).

[174] EU Commission, "Explanatory Memorandum to the AI Liability Directive-E", COM (2022) 496 final 2022/0303 (COD), 6 f., 14.

[175] See above B. II. 3. b).

[176] On liability due to discrimination in the context of labour law, see Monika Schlachter-Voll, «§ 15», in *Erfurter Kommentar zum Arbeitsrecht*, ed. Rudi Müller-Glöge, Ulrich Preis, Ingrid Schmidt 22nd edn. (München: C.H. Beck 2022), marginal no. 4 ff: Martina Benecke, «§ 15 AGG», in *BeckOGK*, ed. Beate Gsell et al. (München: C.H. Beck, status September 01, 2022), marginal no. 13 ff; Boris Dzida and Naemi Groh 13 et seq.; Boris Dzida and Naemi Groh, "Diskriminierung nach

V. Conclusion

The real bang for the buck in the package of directive proposals lies in the considerable extension of the Product Liability Directive to software, even if this is to be qualified as cloud-based or stand-alone – which corresponds to a desideratum[177] that has been propagated for a long time. But the inclusion of *connected services is also* noteworthy, as is the consistent extension to *data delivery services*. Furthermore, the Product-Liabiltiy-D-P explicitly emphasises the cybersecurity requirements as well as the obligation to update, which was previously difficult to justify in terms of tort law. The extension of legal protection to data is also interesting. Thus, the waiver in the AI Liability Directive-E of the introduction of strict liability for AI systems still seems justifiable, even if there would have been some arguments in favour of extending strict liability to *operators of* AI systems. However, the provisions on the duty of disclosure, which harbours considerable "blackmail potential" comparable to *pretrial discovery,* still appear problematic in both draft directives, especially with regard to the disclosure of trade secrets; here, clarification of the conditions for the protection of trade secrets as well as the requirements for the plaintiff's submission would have been desirable. It will be exciting to see how the Member States and the *EU Parliament* will react to the partly revolutionary proposals.

dem AGG beim Einsatz von Algorithmen im Bewerbungsverfahren," *NJW,* (2018): 1917 (1921 et seq.); on liability under § 823 II BGB due to discrimination on the grounds of disability, cf. Spindler, (n 96), Rn. 278 with further references.

177 Cf. for example Zech, (n 82)., A 68; Herbert Zech, "Künstliche Intelligenz und Haftungsfragen," *ZfPW* 209, 198 (212); Wagner, (n 9), 707 (718); Spindler, (n 131), 369 ff.