9

Product Liability Law and AI

Revival or Death of Product Liability Law

Vibe Ulfbeck

I INTRODUCTION

AI devices will increasingly form part of our daily lives, whether as incorporated into physical products such as cars and vacuum cleaners or as 'standalone' applications we acquire and that can interact through Internet of Things ('IoT') devices.

It has often been pointed out that the development towards more application of AI solutions will imply that human functions will be taken over by machines, thereby reducing the need to focus on liability for human errors and increasing the need to focus on liability for malfunctioning products. This would bring product liability rules to the fore.[1] The question is, however, how these rules will work in the new context.

Product liability concerns physical damage caused by physical products. It is based on notions of control as embedded in the concept of a 'defect' and the idea of clearly distinguishable risk spheres in the value chain.[2] In contrast, AI has 'unpredictability' and 'black box' explanation problems as built in features[3] and may present itself as both 'intangible' and highly 'complex' in its interaction capabilities. Consequently, it challenges both the idea of liability based on control through a defectiveness test and the idea of product liability as concerned with a world of physical objects that are distributed in a clearly organised value chain.[4]

[1] Cerre, 'Report, 2021', <www.cerre.eu/publications/eu-liability-rules-age-of-artificial-intelligence-ai/>, 49; Taivo Liivak, 'Liability of a Manufacturer of Fully Autonomous and Connected Vehicles under the Product Liability Directive' (2018) 4 *International Comparative Jurisprudence* 178, 178–189; Vibe Ulfbeck, 'Autonomous Ships and Product Liability under the EU Directive' in Henrik Ringbom, Erik Røsæg and Trond Solvang (eds), *Autonomous Ships and the Law* (Routledge 2021).

[2] The idea of clearly distinguishable risk spheres in the value chain is reflected in the central product liability principle that the producer cannot be held liable if it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him, see PLD Article 7(b).

[3] See Communication from the Commission of 10 January 2017, Building a European data economy, COM(2017) 9 where 'complexity', the legal nature of the IoT device and the autonomous nature of the device are identified as the main challenges with regard to product liability law.

[4] The product liability regime is based on the idea that a product, once manufactured by the producer, is sold to a commercial buyer, who then passes it on to other buyers and sellers until it finally reaches the end user, for example, the consumer. This can be termed a 'clearly organised value chain'.

https://doi.org/10.1017/9781108980197.011 Published online by Cambridge University Press

The aim of this contribution is to examine the impact of AI on central product liability concepts in order to be able to evaluate whether the product liability regime must indeed be expected to 'take over' as a central liability regime in the future. It focuses in particular on the product liability regime as represented in the EU product liability directive (PLD) and makes references also to the Proposal for a new PLD.[5] It starts out by providing an in-depth analysis of the central concept of a defect in product liability law in the context of AI (Section II) and then contextualises the findings by focusing on the value chain and its related concepts as the frame within which product liability law works (Section III). Section IV concludes.

II THE CONCEPT OF THE DEFECT: STANDARDISATION AND INDIVIDUALISATION AT THE SAME TIME?

A *The Reasonable Expectations Test in the Product Liability Directive*

According to Article 6 in the PLD, a product is defective if it does not live up to 'the safety which a reasonable person is entitled to expect, taking all circumstances into account'.[6] The test is a general test that relies on the concept of the 'reasonable person'. This concept is to be understood in an objective manner.[7] The decisive question is not what the victim actually expected from the product but what would generally be expected by a reasonable person (the public at

[5] The existing product liability regulation in the EU can be found in Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (PLD). A proposal for a revision of the PLD has recently been introduced, see Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final (Proposal for a new PLD). The Proposal for a new PLD has been underway for some time, see inter alia the EU commission's staff working document entitled 'Liability for emerging digital technologies', SWD (2018) 137 final, 25 April 2018. The EU Commission also established an expert group on Liability and New Technologies – the New Technologies Formation (the Expert Group). The task of the group was to establish the extent to which liability frameworks in the EU will continue to operate effectively in relation to emerging digital technologies (including artificial intelligence, the internet of things, and distributed ledger technologies). The Expert Group published its report, 'Report on Liability for Artificial Intelligence and other Emerging Technologies (the Expert Group Report), on November 21, 2019. See in particular pages 27–28. See also EU Commission White Paper on Artificial Intelligence, COM(2020) 65 final, 19 February 2020.

[6] Closely related to the concept of the defect is the concept of the risk development defence (PLD Article 7). This concept is not the focus of this chapter since it only becomes relevant as a liability exemption if a defect is proven to exist. Also not dealt with in this chapter, is fault-based product liability and other types of fault-based liability for AI systems, see in this regard Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final.

[7] See, for example, Duncan Fairgrieve and others in Piotr Machinowsky (ed), *European Product Liability – An Analysis of the State of the Art in the Era of New Technologies* (2016) 51; Vibe Ulfbeck, *Erstatningsretlige Graenseområder* (DJOEF 2021), 241.

https://doi.org/10.1017/9781108980197.011 Published online by Cambridge University Press

large). Furthermore, all circumstances must be taken into account when assessing the reasonable expectations, including the presentation of the product, the use to which it could reasonably be put and the time when the product was put into circulation. This makes the test a rather broad one.[8] The fact that the test relies, not on the actual, but on the legitimate expectations of the user, basically means that not any malfunction of the product is to be deemed a defect. Put differently, a product cannot necessarily be expected to be 100% safe.[9] For instance, cigarettes are sold on the market without liability for the producer although it is scientifically well established that smoking poses health risks. In the same way, pharmaceuticals are on the market without liability for the producer even though the products may have certain negative side effects.

Since the defectiveness test focuses on the expectations of the user and these expectations will most often not in reality be linked to the technical way in which the product has been construed, one could argue that the technological explanation for the malfunctioning of a product should be irrelevant. French and Belgium courts have taken this approach to the defectiveness assessment.[10] Carrying out the defectiveness evaluation without needing to focus on the technological explanation for a damage causing effect of the product would render the 'black box problem' related to AI products less important. However, in other court decisions, defectiveness assessments do focus on the underlying reasons for the defect when it comes to establishing proof of a defect.[11] Thus, establishing that something has gone wrong in the production process (fabrication defect) or that a product could technically have been manufactured in a way that would have eliminated the risk causing elements in the product (design defect) may be ways of establishing that a certain product is defective. In reality, therefore, product liability cases often involve the need for technical and technological expertise.

This also means that in order to be able to understand the challenges related to assessing whether an AI product is defective or not, it is necessary to understand – at least at a general level – how such a system is created and works.

[8] It has often been pointed out that the concept is without any precise content, see Duncan Fairgrieve, Geraint Howells and Marcus Pilgerstorfer 'The Product Liability Directive: Time to Get Soft?' (2013) 4 *JETL* 1–33, 5–6. The Proposal for new PLD adds further criteria, see Article 6(a)-(h), including 'the effect on the product of any ability to continue to learn after deployment, see Article 6(c) and further below under E(3).

[9] See, for example, Fairgrieve and others (n 7) 52, 53; Bernhard Koch, 'Austria' in Piotr Machinowsky (ed), *European Product Liability – An Analysis of the State of the Art in the Era of New Technologies* (2016) 125.

[10] See the European Commission's Third Report on the Product Liability Directive, COM(2006) 486 Final, 10 with references to decisions from these jurisdictions.

[11] See COM(2006) 486 Final, 10 with references to decisions from English courts, *Richardson v LRC Products Ltd* [2000] EWHC J0202-12; *Foster v Biosil* (2000) 59 BMLR 178, but see later *Alan Peter Ide v ATB Sales Limited* [2008] EWCA Civ 424 (CA). See also Fairgrieve, Howells and Pilgerstorfer (n 8) 9.

https://doi.org/10.1017/9781108980197.011 Published online by Cambridge University Press

B *The Special Characteristics of AI Systems with Regard to the Defectiveness Assessment*

The feature of an AI system that is the most challenging to handle with regard to a defectiveness assessment is the autonomy of the system. Thus, in an AI system, an algorithm does not work solely on the basis of commands of an 'if … then' nature. Rather, the algorithm is programmed to be a 'self-learning' algorithm that can receive training and evolve on the basis of sets of data that it is exposed to.[12] The algorithm is programmed to find correlations between different phenomena, not causation. An AI system will not answer the question why there is a correlation between pictures of certain types of drivers and pictures of traffic accidents, it only identifies the correlation and 'acts' on the basis of this correlation by giving advice or by taking decisions. Before the AI system is put on the market, the algorithm is trained under the supervision of the developer. This means that the developer chooses the relevant datasets on the basis of which the training is carried out, and the developer tests the way in which the algorithm reacts to new data on the basis of its training. When the development of the AI system has been finalised, the AI system can in principle be put on the market. Some AI systems are programmed to continue learning after this stage on the basis of data received in 'real life' whereas others are 'frozen'.[13]

It has been claimed that 'authors often tend to mystify the decision-making mechanisms of algorithms as something 'unforeseeable, unpredictable or unquantifiable'.[14] Thus, from a legal perspective, it is important to understand in what sense an AI system may work in a way that is 'unpredictable, unforeseeable and unquantifiable'. At the general level, it can be argued that since the AI system is created by humans, it only does what it has been asked to do by humans. Thus, as explained above – a developer needs to create the algorithm through programming and to program the algorithm to be able to receive 'training' by being exposed to data in which it detects correlations. The developer also needs to decide on the basis of what data sets the algorithm is to be trained. The developer of course has control over the programming of the algorithm and the sets of data to which it is exposed in the 'laboratory' (an open real-world setting). Finally, the developer must test the created algorithm. However, in a number of respects, an AI system can be said to be 'unpredictable, unforeseeable and unquantifiable'. Firstly, the developer cannot know which correlations the algorithm will find and on what basis two phenomena are deemed to have a correlation. For instance, an AI system for an autonomous

[12] For a description of classical AI relying on symbolic logic and neural networks, the behaviour of which can only be described statistically, see for instance Herbert Zech, 'Liability for Autonomous Systems: Tackling Specific Risks of Modern IT" in Sebastian Lohsse, Reiner Schulze, Dirk Staudemayer (eds), *Liability for Robotics and the Internet of Things* (Nomos 2019) 187–200.

[13] Cerre (n 1) 55.

[14] Liivak (n 1) 183.

vehicle trained on the basis of a large number of photos of traffic situations may find correlations between certain types of situations and certain types of drivers, but may also find correlations between the paper quality of different photos. Secondly, making sure the data set on which the algorithm is trained does not have any flaws is in itself a challenge. Thirdly, even though the trained algorithm is thoroughly tested prior to being put on the market, it will not be possible to test how the algorithm will work (what it has learned) in all of the situations that can potentially arise. Finally, to the extent the AI system has self-learning capabilities after it has been put on the market, the developer will have no control with the data to which the system will be exposed and on the basis of which it will learn. In these respects, an AI system can be described as 'unpredictable, unforeseeable and unquantifiable'.[15]

C *Defectiveness Assessment Methods*

In practice, courts have focused on different parameters when making defectiveness assessments.

Generally, the product is compared with the description of the product and other similar products.[16] Whereas, the description of the product will also be relevant with regard to AI products, comparing the product to other products may be less meaningful, as AI systems based on the same algorithm may evolve differently depending on the data they are exposed to.[17]

In the United States, the risk/utility test plays a central role in assessing defectiveness. In Europe, it is not entirely clear to what extent this test can be used.[18] On the one hand, it has been argued that the reasonable expectations of the consumer can be and should be assessed regardless of cost/benefit considerations which may tend to introduce a fault-based liability regime through the back door. On the other hand, it could also be argued that what can reasonably be expected is exactly that the

[15] See Tiago Sergio Cabral, 'Liability and Artificial Intelligence in the EU: Assessing the Adequacy of the Current Product Liability Directive' (2020) 27 *Maastricht Journal of European Comparative Law* 615, 625: 'The developer/producer will be unable to fully understand a decision by a machine'.

[16] See, for example, Fairgrieve and others (n 7) 57; Susana Navas, 'Producer Liability for AI-Based Technologies in the European Union' (2020) 9 *International Law Research* 77, 80.

[17] Y Berhamoud and J Ferland 'Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages' in P D'Agostino, C Piovesan and A Gaon (eds) *Leading Legal Disruption: Artificial Intelligence as a Toolkit for Lawyers and the Law* (Thomson Reuters 2020) 6: 'Moreover, it may prove useless to try to compare AI tools, as conclusions reached for one AI tool (i.e., the one that is defective) will not be transposable to a second AI tool, because the two, even when designed together, will have – over time – learned and evolved differently'.

[18] The preamble to the PLD is silent in this regard. Piotr Machnikowski, 'Conclusions', in Piotr Machnikowski (ed), *European Product Liability – An Analysis of the State of the Art in the Era of New Technologies* (2016), 695 raises doubt as to the compatibility of the test with the Directive. Thomas Verheyen, 'Modern Theories of Product Warnings and European Product Liability Law' (2019) 15(3) *Utrecht Law Review* <https://doi.org/10.36633/ulr.541>, 44–55, 51 finds that the European law maker preferred the reasonable expectation test over the risk utility test.

utility of a product outweighs its risks. For instance, with regard to pharmaceuticals, not any side effect renders a product defective, since on balance, the product may be found to have more advantages than disadvantages. In practice, the risk utility test is clearly accepted in at least some European jurisdictions as part of the defectiveness assessment.[19] It could also be relevant with regard to AI products.

Further, standards, both public and private, can be relevant. The PLD only mentions that the manufacturer is exempt from liability if the defect is caused by the observance of mandatory, public regulation.[20] However, it is widely assumed that public safety regulation and implementation standards may also play a role in assessing whether or not a product is defective. Schepel puts it this way: 'Formulated negatively, failure to comply with industry standards will almost automatically lead to liability'.[21] In the area of product liability, it has been pointed out that in case law, there are different views on this in different jurisdictions.[22] It is (even) less certain the extent to which compliance with standards can also be used as a defence against liability (the so called 'regulatory compliance defence').[23] The question was recently addressed in an English case, *A F Wilkes v DePuy International Ltd*, concerning an artificial hip, a stem of which fractured. A main question in the case was whether the product (the hip) could be regarded as defective. In this regard, Hickinbottom J emphasised the importance of standards and regulation:

> In an appropriate case, compliance with such standards will have considerable weight; because they have been set at a level which the appropriate regulatory authority has determined is appropriate for safety purposes.
>
> The same is true, as is again common ground before me, with regard to compliance or non-compliance with regulations which apply to a product.
>
> Certainly, where every aspect of the product's design, manufacture and marketing has been the subject of the substantial scrutiny, by a regulatory body comprised of individuals selected for their experience and expertise in the product including its safety, on the basis of full information, and that body has assessed that the level of safety is acceptable, then it may be challenging for a claimant to prove that the level of safety that persons generally are entitled to expect is at a higher level.

19 For German law, see BGH, 16.6.2009, VI ZR 107/08, BGHZ 181, 253 para 18. For further references see Fairgrieve, Howells and Pilgerstorfer (n 8) 7–8, finding that '[i]t is somewhat difficult to exclude risk-utility having some role in evaluating whether a disclosed risk is socially acceptable' and that '[t]he central test remains what 'persons generally are entitled to expect.' Part of the answer to what is socially acceptable may well include elements of risk utility'.

20 PLD Article 7(d).

21 See Harm Schepel, *The Constitution of Private Governance. Product Standards in the Regulation of Integrating Markets* (Hart Publishing 2005) 349, with reference to others.

22 Duncan Fairgrieve and Geraint Howells, 'Rethinking Product Liability: A Missing Element in the European Commission's Third Review of the European Product Liability Directive' (2007) 70 *MLR* 962–78. In the Proposal for a new PLD, 'product safety requirements' are specifically mentioned as a criterion that is relevant for the defectiveness assessment, see Article 6(1)f.

23 Fairgrieve and Howells (n 22) 972–973.

> The challenge is compounded where, as here, the standards for the product are set on a European-wide basis, such that CE marking hallmarks a product as one which has satisfied the relevant standards (including safety standards) so that it can be marketed throughout Europe.[24]

This reasoning is in accordance with Schepel noting: 'it is hard to see how a publicly accepted mode of production, in compliance with standards and customary in the sector concerned, could fall short of legitimate safety expectations'.[25]

Despite the controversial nature of the view, it could be argued that because of the technological and complex nature of AI products it might be presumed that regulatory regimes and standards will come to play a particularly important role in this field.[26] In spring 2021, a proposal for an AI Regulation was presented.[27] It is the purpose of the regulation to create harmonised rules on AI and it establishes a system for ensuring the quality of AI systems through standardisation and certification. The AI Regulation distinguishes between 'high risk' AI products and other AI products, establishing mandatory requirements for high risk products and a voluntary system based on codes of conduct for other AI systems. The proposed AI regulation follows the 'New Legislative Framework Approach' meaning that the requirements set out in the regulation are objectives at the general level which are then detailed at the technical level in the so-called 'harmonised standards'.[28] At the moment, several technical AI standards have been developed and more are under development.[29] A product that complies with the technical, harmonized standards is presumed to live up to requirements in the underlying regulatory framework. In Section E later, examples are given to illustrate how the AI Regulation could be relevant for the defectiveness assessment under the PLD.

[24] *A F Wilkes v DePuy International Ltd* [2016] EWHC 3096 (QB), [2018] QB 627, [98]–[100].

[25] Schepel (n 21) 378.

[26] This has also been noted by the EU commission, see Liability for Emerging Technologies, SWD (2018)137 final 18, 5 where it is observed that safety regulation and standards must be taken into consideration in dealing with liability issues concerning the safety for the product. Also Christina Amato 'Product Liability and Product Security: Present and Future' in Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds), *Liability for Robotics and the Internet of Things* (Nomos 2018) 94, arguing in favour of standards since leaving a 'discretion of judgements … are not sustainable in the new era of high technology'. Cp. Jean-Sebastian Borghetti, 'Civil Liability for Artificial Intelligence. What Should Its Basis Be?' (2019) 17 *Revue des Jurists de Science Po* 196 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3541597> 97 voicing the concern that standards in a fast-moving field will not always be up to date. Similarly, Gerald Spindler, 'User Liability and Strict Liability in the Internet of Things and for Robots' in Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds), *Liability for Robotics and the Internet of Things* (Nomos 2018) 125–143, 136–137.

[27] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM(2021)206 final.

[28] 'AI Watch: AI Standardisation Landscape – State of Play and Link to the EC Proposal for an AI Regulatory Framework' (2021) 7. See also Amato (n 26) 84–89 for a recent description of the 'the New Approach' and the 'New Legislative Framework'.

[29] 'AI Watch' (n 28).

Finally, instructions and warnings accompanying the product are relevant for the defectiveness assessment. With regard to AI products, it has been pointed out that the importance of these will increase due to the complexity of the products.[30]

In practice, it has been common to distinguish between three types of defects: fabrication defects, design defects and instruction defects. The parameters above enter into the assessment with different weight in the three different categories and there are different opinions as to how the defectiveness assessment should be made with regard to products containing AI components.

D *Fabrication Defects*

Fabrication defects are defects that occur in one or a few products in a series of products because something has gone wrong in the production process. A product that has a fabrication defect differs from the other products in the same series and will not live up to the producer's description of the quality and safety product or to general, industry safety standards. It is broadly accepted that there should (always) be liability for fabrication errors, since the user of the product will have a reasonable expectation that there are no errors in the production process.[31] Consequently, fabrication defects are regarded as a simple category of defects. Fabrication defects can also occur with regard to AI products. For instance, the AI system may have been installed in an incomplete way with the customer.[32] These types of situations can be labelled 'easy' cases, where the product is clearly defective. However, fabrication defects must be expected to be less common with regard to AI products where the problem will rather relate to the design of the product.[33]

E *Design Defects*

1 The Concept of a Design Defect

Design defects are more difficult to deal with. Design defects are defined as defects that occur in all of the products in the same series because the product has been 'thought out' (designed) in a wrong way. The defect is in the very design of the product. An AI product design can be defective in various ways. There can be flaws in the programming of the algorithm that is done before the training of the algorithm and the dataset on which the algorithm has been trained may be incomplete or in other ways unsuitable. However, even though no flaws with respect to programming or data sets can be detected, the AI system may still produce results

30 Navas (n 16) 81.

31 See for example, Gerhard Wagner, 'Robot Liability' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer, *Liability for Robotics and the Internet of Things* (Nomos 2018) 27–62, 43.

32 Wagner (n 31) 43; Navas (n 16) 161680.

33 Navas (n 16) 168; Cerre (n 1) 248.

https://doi.org/10.1017/9781108980197.011 Published online by Cambridge University Press

that are ‘unwanted’, raising the question whether products also in this situation could be categorised as ‘defective’.[34]

2 Programming, Dataset, and Testing Errors

With regard to programming errors, it has been argued that if an error in code line causes the AI system to cause damage then the AI system must be regarded as defective.[35]

However, at the same time it has been pointed out that no programming is 100% flawless.[36] If this is generally known and accepted in society and AI products are put on the market with this knowledge then the mere fact that a product series suffers from a flaw in coding will not necessarily render these products defective. The question then becomes which types of flaws in coding should be regarded a defect.

Parallel problems arise with regard to the data sets on the basis of which the algorithm is trained. It may be possible to detect flaws in the data set but at the same time it must probably be accepted as a fact that samples may not ever be completely flawless and that even investigating the extent to which a data set contains flaws may be impossible in practice.[37]

Despite this, Article 10(3) of the proposed AI regulation requires data sets to be ‘relevant, representative, free of errors and complete’.

As has been noted in legal literature:

> …verifying the representativeness, completeness and correctness of the used datasets would be practically impossible since they usually count billions of tokens spanning across hundreds of languages. Thus, one wonders how such models – which are nowadays used also in products – will be trained in the future.[38]

As explained above, part of the answer to this question, presumably lies in standardisation. Thus, if an AI product has been certified and labelled with the relevant E-mark, it will be presumed that the underlying dataset has been ‘relevant, representative, free of errors and complete’ for the purpose of the regulation.

It must be presumed that to the extent a product does not live up to technical (safety) standards with regard to coding, training, and testing, this will often be a strong indication that the product is defective.[39] More difficult is the question of

[34] Also with regard to design defects there are some easy cases. For example, if a brake in a vehicle does not function at all due to an AI system, the brake will be regarded defective and so will the vehicle in which it is incorporated regardless of whether the defect is caused by AI or not, Borghetti (n 26).

[35] Borghetti (n 26) 196; Liivak (n 1) 183.

[36] Wagner (n 31) 43.

[37] Sebastian Felix Schwemer, Letizia Tomada and Tommaso Pasini, ‘Legal AI Systems in the EU’s proposed AI Regulation’ (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3871099>.

[38] Ibid. (n 37) 6.

[39] Fairgrieve and Howells (n 22) 962–978 points out that courts in different European jurisdictions have come to different results with regard to this question. See also Lenze (22) 21.

https://doi.org/10.1017/9781108980197.011 Published online by Cambridge University Press

whether an AI product that is in compliance with all standards can still be regarded as defective if it causes damage (the so-called regulatory compliance defence). It has been argued that at least in some situations, standard compliance should relieve the producer of liability.[40] The question will be dealt with in Section 3 with regard to autonomous decision making.

3 Standard Compliance – But Autonomous and Unpredictable Acts

The most difficult cases will be the ones in which no coding errors, no errors with regard to the dataset and no testing errors can be detected but the AI system still produces unexpected decisions because it behaves autonomously.[41] The Proposal for a new PLD does not give any guidance as to how the defectiveness assessment should be made in this situation. It only states in Article 6(c) that one must take into consideration 'the effect on the product of any ability to continue to learn after deployment'.

The situation in which a product lives up to all formal requirements with regard to safety specifications and yet causes damage is not unknown in product liability law. As explained above, it seems to be the general starting point that regulatory compliance does not per se relieve the producer of liability. However, in some areas regulatory compliance seems to be a strong argument against civil liability. Pharmaceuticals and medical devices could be mentioned as examples. Often it will be well known that for some people, a pharmaceutical product will have certain side effects and yet the product is not deemed defective. As mentioned earlier, in the English case *Wilkes*, concerning a hip implant, the view was expressed that it may be a challenge to argue that a product that lives up to all formal requirements with regard to safety should nevertheless be regarded as defective.

Further, AI products will have the 'side effect' of causing damage every now and then. It could be argued, however, that there is a difference between AI products on the one hand and ordinary pharmaceutical products and medical devices on the other hand in that the risks related to AI products are 'unknown' and 'unquantifiable', making it difficult to estimate to what extent the advantages of using the product outweigh its disadvantages, whereas with the pharmaceuticals and medical devices it is possible to identify and quantify the risk in advance so that it is clear to both the producer, the user and society at large what the risk when putting the product on the market is as tested against a standard. But also with regard to medical devices it may be difficult to quantify the risk in advance. In the English case of

[40] Bernhard Koch, 'Product Liability 2.0 – Mere Update or New Version?' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Liability for Robotics and the Internet of Things* (Nomos 2018) 99–116, 112, note 49 arguing that there should be no liability for damage caused by hacking if the producer has complied with all standards in this regard.

[41] Borghetti (n 26) 97 finds the difficult cases to be the ones where there is only a 'possibility or a suspicion' that the algorithm was defectively designed.

https://doi.org/10.1017/9781108980197.011 Published online by Cambridge University Press

Colin Gee v DePuy International Ltd[42] which (also) concerned a hip transplant, the material used for the implant had the inherent risk that some people might develop adverse reactions to it. Regulators and patients were informed of this risk and told that it was 'unknown and incalculable'[43] and yet the product was approved of to be put on the market and e-labelled.[44] The problem in the case was that no standard addressed the particular type of weakness of the product that the case concerned (incidence of adverse reaction to metal wear debris (ARMD)).

If all existing standards have been observed and no standards apply to the particular problem in the case, the question is how to evaluate whether the product suffers from a defect if it still causes damage.

In line with this, the AI Expert group[45] has questioned whether, when a sophisticated system with self-learning capabilities makes an unpredictable decision deviating in the path, such deviation can be treated as a 'defect'.[46]

There are different opinions as to how this question should be answered.[47]

One view is that in these types of situations the product should (always) be regarded as suffering from a defect since the product had 'the potential' to develop a defect and the 'susceptibility' to acquire unsafe characteristics.[48] The consequence of applying this rule seems to be establishing a position close to strict liability for damage caused by an AI product regardless of whether it suffers from a defect or not.

Others take a less far reaching position. Thus, it has also been stated that, sometimes, the defectiveness assessment will not give rise to difficulties since it can be made 'intuitively':

> If an autonomous vehicle runs over a pedestrian in a crosswalk, one can argue that the solution is easy. We do not really need to go very deep within the AI's thinking; an autonomous vehicle is not supposed to run over people and, in normal situations, if it worked, the damage would not have occurred.[49]

42 [2018] EWHC 1208 (QB), [2018] Med LR 347.

43 *Gee* (n 42) [487]

44 E-labelling provides web-based product information as an alternative to physical labelling, see <www.seagullscientific.com/resources/labeling-guide/e-labeling/>.

45 The Expert Group was appointed by the EU Commission, see n 5.

46 Expert Group Report (n 5) 28.

47 Navas (n 16) 79 states the following: 'In my opinion, it could be treated as defect when designing the AI systems, the unpredictability has not been contemplated'. This 'test', however, will hardly work since the unpredictability (as defined earlier) will be inherent in any AI product and consequently, some amount of unpredictability will always be contemplated.

48 Piotr Machnikowski, 'Producers' Liability in the EC Expert Group Report on Liability for AI (2020) 11 *JETL* 137–149, 146. One might read para. 23 in the preamble to the Proposal for a new PLD as pulling in the same direction as it contains the somewhat general remark: 'The effect on a product's safety of its ability to learn after deployment should also be taken into account, to reflect the legitimate expectation that a product's software and underlying algorithms are designed in such a way as to prevent hazardous product behaviour'.

49 Cabral (n 15) 625 (in relation to causation).

This line of thinking seems to be based on what has been called 'the human operator' test.[50] According to this test, the acts based on an AI system should be assessed by comparing them to the acts of humans. If the AI system causes damage in a situation in which it must be assumed that a human operator would have avoided it, then the AI system should be regarded as defective. Although thinking about AI systems in this way may be intuitive, it may not be the right way to assess whether an AI product is defective. Moreover, in legal theory it has been argued that 'the human operator' test 'misses the mark'[51] since the AI system is not intended to work the same way as a human but in a different way. This also means that it will cause damage in different situations than humans. Thus, whereas an AI system may statistically be safer than a human operator, the systems may still in a concrete situation cause damage where a human would have avoided it.[52] If an AI product is deemed to be defective in such situations it would amount to 'holding the system to a standard it cannot live up to'.[53] Instead, it has been argued, that with regard to AI products, the concept of a design defect should be understood as a 'system oriented' concept which focuses on whether the entire fleet of cars operated by the same algorithm causes an unreasonable number of accidents overall.[54]

This raises the question how to identify what would be 'an unreasonable' number of accidents.[55] Under the risk/utility test the relevant question would be whether it would have been possible, at a reasonable cost, to design an alternative algorithm (the alternative design test) that would produce better results. It has been pointed out that the problem with applying the alternative design test to algorithms is that it will always be possible to create a slightly better algorithm and the test would imply deeming all other algorithms than the very best on the market defective.[56]

A similar problem was addressed in *Gee*[57] where Andrews J. made the following observation:

> Using another new product as the comparator would also lead to the absurd conclusion that even if all the new products showed an improvement on the existing established products in terms of safety, the new product that showed the smallest improvement by comparison with the others could nevertheless be regarded as defective, if the difference between them was of a sufficient magnitude.

[50] Wagner (n 31) 43.
[51] Wagner (n 31) 43, cp. Ryan Abott, *The Reasonable Robot* (Cambridge University Press 2020), arguing the general view that the law should not discriminate between AI and human behaviour.
[52] Wagner (n 31) 43 mentions 'the freak event that any human would have recognized an adapted his or her behaviour to'.
[53] Wagner (n 31) 43.
[54] Wagner (n 31) 44–45; Borghetti (n 26) 98.
[55] Cerre report (n 1) 54.
[56] Borghetti (n 26) 98–99.
[57] *Gee* (n 42).

As an alternative, a certain level of safety could be identified in practice as the required level, for instance, that an algorithm should as a minimum, statistically be at least 90% as safe as a 'reference' algorithm. In order to make such an assessment, data would be required on how the algorithm and other algorithms perform statistically and such data may not be easily obtainable.[58] This problem was also addressed in *Gee*. First, it was observed that the product causing the harm met all standards but no particular standard addressed what would be an acceptable rate of failure within a certain period of time.[59] Instead, it was examined whether data on failure rates of similar products could provide guidance. Eventually it was concluded that the product (Ultamet) could not be regarded as defective as

> There is insufficiently reliable evidence to establish that the Ultamet did have a materially worse failure rate than either the rate that was expected of a comparator at the time, or the actual failure rate of a comparator (insofar as it is possible to make a reliable assessment of the latter).[60]

The case shows that a systemic approach to the defectiveness assessment is already being used in relation to certain types of products. However, if applied to AI products it will have the downside that a product may be deemed non-defective even in situations where a human would most likely have avoided causing the damage. This may seem counterintuitive. In this way, a 'systemic' approach to the concept of a defect with regard to AI products can be seen as a radical variant of 'standardization'. In order to make it operational in practice it could be considered whether to incorporate the systemic approach in new types of standards developed for the purpose of establishing the acceptable failure rate of algorithms developed for different purposes.

F *Instruction Defects*

As described above, it must be presumed that standardisation is going to play an important role in the defectiveness assessment of AI products. However, standardisation may not be the only tendency. The complexity of the products on the market will increase the demand for proper instructions for the user. Indeed, it has been pointed out that with regard to AI products, information defects will become a more frequent type of defect.[61]

In EU countries, it has been debated what constitutes an instruction defect. Originally, it was the general view that there was no duty to inform on generally known risks.[62] Later on, the duty was broadened, and in 2014, it was assumed in legal literature

58 Borghetti (n 42) 99.
59 *Gee* (n 42) [489].
60 *Gee* (n 42) [498].
61 Navas (n 16) 81.
62 Verheyen (n 18) 50 with references.

https://doi.org/10.1017/9781108980197.011 Published online by Cambridge University Press

that there is a duty to warn against all known risks (broad warning test).[63] With regard to AI products it will be known that there are unknown risks. Presumably, there must be a duty to warn against this under the broad warning test.

In relation to AI products, it must also be presumed that information will become more technical and may require some kind of special knowledge on the part of the user.[64] This raises the question how to avoid an overload of information which in reality cannot be understood by a large number of users. Moreover, psychological research has drawn attention to the difficulties in designing efficient warnings.[65]

In this regard, it has been noted that information forming part of the presentation of the product needs to take into account the 'the different characteristics and purposes of the end user customer'.[66] This can be done in a generalised way so that the instructions take into account the type of user who would typically buy and use the product. However, in legal literature, it has been argued that this is not enough to free the producer of liability under the reasonable expectations test. Thus, Howells argues that a producer should only escape liability if the consumer knows, based on the information provided with the product, that *he* – with his special dispositions – will be the one that is struck by the hazard.[67]

To the extent that privacy issues can be tackled, new technologies may provide new possibilities with regard to precision in warnings and instructions. Thus, through algorithmic consumer profiling, information can be 'individualised' so it can be shaped to more precisely target the individual user. Using algorithms for consumer profiling is suggested as a tool for a 'reframing of the information duties' in consumer law so that the advice given to purchasers of a product rather than being standard advice, resembles 'the advice the honest salesman in the old corner shop would give to the buyer he knows personally'.[68] For instance, a buyer could be warned that the

[63] Verheyen (n 18) 50 with reference to Hans Micklitz, 'Liability for Defective Products and Services' in Norbert Reich, Hans-Wolfgang Micklitz, Peter Rott and Klaus Tonner (eds), *European Consumer Law* (2nd edn, Intersentia 2014).

[64] Navas (n 16) 81.

[65] SB Pape, *Warnings and Product Liability – Lessons Learned from Cognitive Psychology and Ergonomics* (Eleven International Publishing, 2012).

[66] Livak (n 1) 182.

[67] Geraint Howells, 'Information and Product Liability – A Game of Russian Roulette' in Andre Janssen and Geraint Howells (eds), *Information Rights and Obligations – A Challenge for Party Autonomy and Transactional Fairness* (Routledge 2005) 160. Howells uses the example of aspirin, explaining that even if the safety notice mentions the slight chance of internal bleeding, the producer should be held liable when it happens because the product does not provide the safety expected, because the user did not expect it to harm him.

[68] C Busch and A De Franceschi, 'Granular Legal Norms: Big Data and the Personalization of Private Law' in Vanessa Mak, Eric Tjong Tjin Tai and Anna Berlee (eds), *Research Handbook on Data Science and Law*, Edward Elgar Publishing 2018) 9 with reference to Christoffer Busch, 'The Future of Pre-contractual Information Duties: From Behavioural Insights to Big Data' in Christian Twigg-Flesner (ed), *Research Handbook on EU Consumer and Contract Law* (Edward Elgar Publishing 2016) 233–234.

printer he is about to buy does not fit the computer he bought last week.[69] Also in tort law, it is being suggested that negligence law can be 'personalised' so that the applicable standard of care may be adjusted to the specific characteristics of the tortfeasor.[70] With regard to product liability issues, it could be considered whether consumer profiles could be used for individualising the instructions following a product so that consumers who have a profile showing technological skills at a high level receive instructions and information about the product at one level, whereas other consumers receive instructions and information at a different level. Consumer profiles may show that there is a greater need to warn certain consumers about a specific use of a product than others. Personalised instructions could, for instance, be considered with regard to pharmaceuticals and allergy reactions.[71] To the extent the provision of personalised instructions becomes a practical option for producers, the question arises whether not using this technique could render the product defective.

The possibility to provide personalised presentations of the product also gives rise to a more fundamental question. Thus, introducing such personalised instructions, for example in the shape of personalised labels on products, will affect the consumer expectations to a product.[72] The more information is personalised the more difficult it will become to maintain the notion of 'the legitimate expectations of the consumer' as a general concept that focuses on the expectations of the 'public at large' and on general standards defining these expectations. Interestingly, the Proposal for a new PLD includes both the criterion the expectations of 'the public at large' and the criterion 'the specific expectations of the end users for whom the product is intended' in the defectiveness test.[73]

Because of the problems inherent in the defectiveness assessment with regard to AI products some scholars have simply suggested that the defectiveness concept be abandoned altogether[74] and replaced by a truly strict liability system.[75]

III DISRUPTION OF THE VALUE CHAIN

The defectiveness assessment of the product is not the only challenge faced by product liability law in the reception of AI products. Thus, AI can have an influence not only on the way the safeness of a single product or algorithm is assessed but also on the structure of the entire value chain in which the product liability rules work.

69 Parallel example in Busch and De Franceschi (n 68) 8–9.

70 See in general, Omri Ben-Shahar and Ariel Porat, 'Personalizing Negligence Law' (2016) 91 *NYU L Rev* 627–686.

71 Joasia Luzak, 'A Broken Notion: Impact of Modern Technologies on Product Liability' (2020) 11(3) *European Journal of Risk* 630, 630–649, 631.

72 On interactive labels, see www.sciencedaily.com/releases/2020/03/200326144341.htm.

73 See the Proposal for a new PLD Article 6(1) and 6(1)(h). Compare Luzak (n 71) 646, 648, who finds that the solution lies in relying on standards in the defectiveness assessment.

74 Luzak (n 71) 637.

75 Borghetti (n 26) 99.

The PLD channels liability to the producer as the central player who is the better risk avoider, better risk distributer and therefore also the better risk carrier. It builds on the idea of the 'linear' value chain, that is, a value chain in which sub suppliers of components for a product sell the components to the producer who manufactures the product that is finally put on the market for consumers and other buyers. Moreover, internally in the chain, each actor carries liability only for the safeness of the product in the shape in which it was put on the market by the actor.[76] Thus, in a traditional value chain, liability can be described as 'compartmentalised' and resting on clearly defined risk spheres.[77]

AI systems may be distributed through this type of traditional value chain. For instance, an AI component could be sold by a software provider to the producer who integrates the AI component in a product, such as an autonomous vehicle, a vacuum cleaner, or a medical device, and then puts the entire product on the market. These types of products have been called 'bundled' products.[78]

However, today, consumers may choose to buy hardware from one manufacturer and software from another, combine the two, supplement with updates received from the producer itself or a third party, and users themselves may also be authorised to access the safety related software of a system. The functioning of products may also be dependent on the reception of services, such as signals for sensors, delivered by other actors. In other words, in a digitalised world, products will often be 'unbundled',[79] making the value chain less linear and much more complex and comparable to a network.

This type of value chain challenges several, basic product liability concepts that are thought out with a view to the 'traditional' supply chain.

Firstly, whereas it is common ground that 'bundled' products such as the ones mentioned above come within the scope of the PLD, it is not clear whether 'standalone' AI products, such as an AI service offered to a medical doctor for diagnosing purposes, are covered by the product liability regime at all. Thus, according to Article 2 of the Directive a product is defined as a 'movable'. Since code is something intangible it is likely not covered by the definition of a product as it stands today.[80] However, for some time it has been under consideration to expand the definition of a 'product' and to include software and digital devices

[76] See Articles 6, 7, and 11 of the PLD.

[77] See also Koch (n 40) 102, describing the time when the product is put into circulation as the Directive's 'magic moment'.

[78] Wagner (n 31) 47; 'BEUC Report, Review of Product Liability Rules' (2017) 12 <www.beuc.eu/publications/beuc-x-2017-039_csc_review_of_product_liability_rules.pdf>.

[79] Wagner (n 31) 47–49.

[80] It seems to be broadly accepted that software is covered by the Directive if it is embedded in a physical object such as a disk or a USB stick, Cerre (n 1) 50; 'BEUC report' (n 71) 12. However, today such devices are less used and programs are often downloaded directly from the internet. For a discussion, see for example, Wagner (n 31) 11; Livaak (n 1) 180–181.

https://doi.org/10.1017/9781108980197.011 Published online by Cambridge University Press

in the concept of a 'product'.[81] This would bring the PLD in line with other recent legislative initiatives such as the recently adopted sale of goods directive[82] and the directive on the supply of digital content and digital services.[83] Also the recent CJEU decision (*Krone*), finds that liability for a defective service could be conceivable if the service is part of the product's inherent characteristics.[84] In the Proposal for new PLD it is suggested that software should be defined as a product (Proposal Article 4(1)).

Including software in the definition of a product would enable suits to be brought not only against the producer of a bundled product but also against the software producer. It would also pave the way for product liability suits against producers of other 'stand-alone' AI products such as AI systems offering advice in a range of areas, including health and disease treatments. Revising the concept of a product further to also include the broader notion of digital products might enable product liability suits to be brought against providers of digital updates for a system, but such an enlargement might on the other hand make it difficult to uphold the distinction between products and services in the Directive,[85] raising the question of whether liability for defective services should be included.

Moreover, the introduction of new types of products with new vulnerabilities has inspired the question whether the definition of damage should be extended to cover not just physical damage but also non-economic loss such as loss of data due to hacker attacks.[86] Including software and data content in the definition of a 'product' may also call for a revision of the definition of a 'producer'. In the Directive,

81 See <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en>. For an overview, see, for instance, Kathrin Bauwens, 'Product Liability and AI (Part 2) – The EU Commission's Plans for Adapting Liability Rules to the Digital Age' (*Linklaters*, 16 July 2021) <www.linklaters.com/en/insights/blogs/productliabilitylinks/2021/july/product-liability-and-ai-part-2-eu-commissions-plans-for-adapting-rules-to-the-digital-age>.

82 Directive (EU) 2019/771.

83 Directive (EU) 2019/770.

84 Case C-65/20 *VI v KRONE – Verlag Gesellschaft mbH & Co KG*.

85 On the distinction between products and services with regard to AI systems and digital content, Cerre (n 1) 51; Cabral (n 15) 619–620 The Proposal for new PLD does not include 'digital products' or 'digital content' in the definition of a product, cp. Article 4 (1). The Proposal also does not include 'providers of digital updates' in the list of 'economic operators' that can be held liable under the directive, cp. Article 7. The intention seems to be that the manufacturer of the product who also delivers updates can be held liable for defective updates (digital services), see preamble, paras 15 and 37.

86 'The EU Commission's Inception Impact Assessment report' 4 <www.ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en>; Cabral (n 15) 629; Navas (n 16) 79. The Proposal for a new PLD defines damage as 'material loss' cp. Article 4(6) and includes material loss resulting from 'loss or corruption of data that is not used exclusively for professional purposes (Article 4(6)(c)). According to the preamble, para 16, the intention seems to be that loss or corruption of data should be considered 'damage' within the meaning on the Proposal for a new PLD.

a producer is defined in Article 3 as 'the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trademark or other distinguishing feature on the product presents himself as its producer'. It has also been argued that the engineer designer should be included in this definition.[87] Moreover, if digital content is considered a product it should be considered who could be regarded as 'producers' of this content and whether they should also be included in the definition of a producer in the PLD. More broadly, it could be considered whether the definition of the potentially liable actors in the PLD should be aligned with the corresponding definitions in the proposed AI regulation. This would mean considering whether a 'provider' and a 'product representative' as mentioned in the proposed AI regulation should also be regarded as potentially liable actors under the Directive.[88] Similarly, it has been argued that the potential liability for digital platforms as key players in the value chain and providers of data should be considered.[89] In line with this, the Proposal for a new PLD extends the group of actors who can be held liability for product injury. It uses the term 'Economic Operator' to specify who can be held liable for product liability, see Article 7. The list includes the 'Authorised Representative' as a potential subject of liability (Article 7(2)). It also includes the 'fulfilment service provider'.

Finally, the new type of value chain challenges the compartmentalisation of liability based on the idea of separated risk spheres between the different participants in the value chain. Thus, according to the PLD, a product is to be regarded as defective if it does not meet legitimate expectations with regard to safety at the time when the product was put on the market.[90] In other words, the producer is not liable for damage caused by changes to the product that occur after it has been put on the market (the so called 'later defect defence'). The reason for this is that with regard to ordinary products, the producer no longer has control over the product once it has been put on the market. However, with regard to digital products, the situation may be different. Thus, a producer may be able to update and thereby change the

[87] Navas (n 16) 81 with further references. The Proposal for a new PLD in Article 4(11) largely relies on the current definition of the producer (manufacturer) but includes other actors that can also be held liable as 'Economic Operators', see further below.

[88] Proposed AI Regulation Article 3 (1) and (5).

[89] See for instance Christoph Busch, 'When Product Liability Meets the Platform Economy: A European Perspective on Oberdorf v. Amazon' (2019) 8 *Journal of European Consumer and Market Law* 173–174, V Ulfbeck and P Verbruggen 'Online Marketplaces and Product Liability: Back to the Where We Started?' (2022) 30(6) *European Review of Private Law* 975. The Proposal for a new PLD introduces the concept of the 'fulfilment service provider' as a new potential subject of liability, but only to the extent that there is no EU producer, EU importer or Authorised Representative in the EU to make claims against (Article 7(3)). In Article 7 (6), it also makes clear that a provider of an online platform can be held liable if the consumer could reasonably believe that it were contracting with the platform. This principle is also established in DSA Article 6(3).

[90] On the notion of defectiveness, supra Section II.

https://doi.org/10.1017/9781108980197.011 Published online by Cambridge University Press

system after it has been put on the market. In the proposal for the new AI Regulation it is even stated that there should be general monitoring duties after the product has been put on the market.[91] This raises the question of whether the later defect defence in the Directive should be abolished.[92]

The obstruction of the traditional value chain structure begs the question of whether the traditional principles for risk allocation between the parties in the chain can be upheld, in particular whether it makes sense to channel the liability to the producer.[93] Views differ in this regard.

According to European Law Institute, there is no reason to make fundamental changes in risk allocations. Rather, it is stated that: '…liability should be allocated to the person who [is] most likely to have caused the harm, … liability should fall on the person best placed to absorb the loss. There is no reason why this rationale should not be maintained in the digital era'.[94]

However, upholding the traditional system will give rise to some practical problems. As Wagner puts it:

> …the victim would have to investigate whether the accident was caused by defective hardware, defective software marketed by the supplier of the original software, software manufactured by a third party and added to the device by the user, or by other modifications made by the user subsequent to acquisition of the device. This burden may deter many victims from bringing suit and may seriously undermine the success even of meritorious actions.[95]

And further:

> For unbundled products there simply is no single responsible party that controls the safety feature of all components. Thus, liability must be apportioned between all the actors who contributed to the safety features of the device that caused the accident at the time of the accident.[96]

This line of thinking is further developed by Beckers and Teubner who distinguish between different uses of AI systems and consider a 'network and enterprise liability'

[91] Proposal for AI Regulation Article 61.

[92] This has been thoroughly considered, see 'The EU Commission's Inception Impact Assessment report' (n 86) 4. The Proposal for a new PLD suggests a new formulation. Thus, according to Article 6(e), when making the defectiveness assessment, one must take into consideration 'the moment in time when the product was placed on the market or put into service or, where the manufacturer retains control over the product after that moment, the moment in time when the product left the control of the manufacturer'. According to Article 6(c), also 'the effect on the product of any ability to continue to learn after deployment' must be taken into consideration. These criteria to some extent modify the 'later defect' defence in the PLD.

[93] Koch (n 40) 112. This view can be seen as reflected in the Proposal for a new PLD, which in Article 7 expands the number of possible liability subjects.

[94] See 'ELI Guiding Principles for Updating the Product Liability Directive for the Digital Age', Guiding principle no 5.

[95] Wagner (n 31) 48.

[96] Ibid. 49.

and 'prorata network share liability' for situations in which there is a close collaboration between human and machine.[97]

Overall, and as also reflected in the Proposal for a new PLD, it can be argued that the realities of the new value chains could call for a number of adjustments of central product liability concepts. Such adjustments would basically widen the scope of the product liability rules. In contrast to what is the case with regard to the defectiveness concept, the adjustments discussed in this section can in principle be achieved by political decisions to revise the concepts in the Directive. As will be elaborated further in Section IV, the difficult question here is only how far to go.

IV CONCLUSION AND PERSPECTIVES

The analysis above shows that carrying out a defectiveness assessment with regard to AI products will not be an easy task and the Proposal for a new PLD does not solve this problem. However, the types of difficulties are not entirely unknown. Parallels can be found in relation to the defectiveness assessment of pharmaceuticals and medical implants. Until now, these problems have been handled on a case by case basis. However, with the introduction of AI products, the problems regarding the defectiveness assessment will not primarily be confined to such products as pharmaceuticals and medical implants but will appear in relation to a broad range of everyday products. In particular, the role played by standards and a 'systemic' approach to the defectiveness assessment have attracted interest. The systemic approach can be seen as a radical version of standardisation and could itself be standardised.

At the same time, not only standardisation tendencies may come to play a role in the defectiveness assessment. Paradoxically, individualisation may also be relevant and may challenge the basic idea of operating a general test of legitimate consumer expectations, including the application of standards. Consequently, it seems that the introduction of AI products could generate rather contradictory approaches to defectiveness assessment in product liability law. This reflected in the Proposal for a new PLD which in Article 6 as defectiveness criteria include both the expectations of 'the public at large' and 'the specific expectations of the end-users for whom the product is intended'. It is an interesting question whether, in the longer run, technological advances will make the individualised method prevail. The problems related to the defectiveness assessment have led to suggestions of abandoning the concept of defectiveness altogether and introducing a truly strict liability regime.

Not only the concept of defectiveness, but also basically all concepts related to the value chain, are challenged by the new type of products. This is reflected in the number of adjustments of basic product liability concepts which are suggested

[97] Anna Beckers and Günther Teubner, *Three Liability Regimes for Artificial Intelligence – Algorithmic Actants, Hybrids, Crowds* (Hart Publishing 2022) 101, 106.

in the Proposal for a new PLD. Whereas the concept of defectiveness generates difficult questions of interpretation, the problems pertaining to the value chain concepts can, to a large extent, be solved by political decisions to adjust the concepts. The concept of a product could be extended to cover software and digital content, the liability period could be extended to also cover the post marketing phase, the concept of damage could be expanded to also cover non-economic loss cases and the list of potentially liable actors in the value chain could be expanded. Currently, changes with regard to all of these parameters are to some extent suggested in the Proposal for a new PLD. However, if technological developments continue to blur the traditional boundaries in product liability law and possibly even call for giving up the concept of defectiveness, the needed changes may become so fundamental that it no longer makes sense to speak about 'product liability'.

This also means that whereas one might intuitively think that the product liability regime will come to play a vital role in an era where machines take over from humans, it may in fact be the other way around: AI may end up dissolving the very concept of product liability.