

The Consumer Voice in Europe

PRODUCT LIABILITY 2.0

How to make EU rules fit for consumers in the digital age



Contact: Alexandre Biard - consumer-rights@beuc.eu

BUREAU EUROPEEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45



Co-funded by the European Union

Ref: BEUC-X-2020-024 - 07/05/2020

Why it matters to consumers

Consumers are today surrounded by digital goods in all aspects of their everyday lives. However, when these products harm consumers, an enforceable right to claim compensation may not be at hand. Because of their wide dissemination, flaws in digital goods can have large-scale implications for consumers and society. The current legal framework established by the Product Liability Directive in 1985 is no longer adapted to the multiple challenges brought by new technologies in 2020. This situation creates legal uncertainty for both businesses and consumers, multiplies the risk of unequal treatment of consumers in the Single Market, prevents consumer redress and trust in digital goods in general. It is essential that the EU product liability rules establish a clear and enforceable legal framework that ensures effective access to justice for all consumers.

Summary

In 2020, the EU Product Liability Directive (PLD) turns 35. During this time, many 'offline' products have since been replaced by digital goods. 'Smart' products are now fed with continuous flows of data, can interact or 'talk' with other goods, may take autonomous decisions and are increasingly used as entry points to access a wide range of digital services and digital content. The PLD is no longer adapted to this new context and leaves many consumers unprotected when problems arise. That is why the EU's framework for product liability needs an urgent update.

Here are nine ways to ensure that the EU product liability framework remains fit for the digital age and delivers its full potential to consumers:

1. Clarify the objective and scope of the Product Liability Directive:

- Achieving high consumer protection should clearly be stated as a key policy objective for the PLD.
- The PLD should apply to all tangible and non-tangible goods, including digital services and digital content.

2. The notion of "defect" should be broadened and no longer limited to users' safety expectations:

- The PLD should build on an extended notion of 'defect' no longer only limited to users' safety expectations. A product should be considered 'defective' when it deviates from the reasonable expectations that users may have, which include: the product should be safe, it should be free from cybersecurity failures and other personal security risks and should be GDPR-compliant. In addition, a product using self-learning capacities and taking autonomous decisions should be deemed defective when its unintended behaviour has caused harm to the user.

- A lack of post-marketing updates by producers should be considered as a defect in case of harm to the user.

3. Review the notion of “time at which a product is placed on the market”:

- The time at which the product was placed on the market should no longer be relevant when assessing defects.

4. Revise the scope of compensable damage:

- The PLD should extend the scope of compensable damage to also cover damage to digital assets, including data.
- The €500 lower threshold should be removed.
- The maximum cap of €70m should be removed.

5. Reverse the burden of proof:

- The burden of the proof concerning defect and causation should be reversed. It should be enough for the injured party to prove the existence of damage resulting from a product.

6. Clarify the scope of liable persons (including online marketplaces):

- All professionals involved in the production of digital goods should be held jointly liable if their activities have affected the reasonable expectations which users may have about their products.
- Online marketplaces should bear subsidiary liability as ‘suppliers’ under the PLD. Online marketplaces should be held liable provided that at least one of the following conditions is fulfilled: (1) The producer cannot be identified; (2) The marketplace fails to inform the consumer in due time of the identity of the producer and does not enable communication between the consumer and the producer by providing relevant contact details; (3) The marketplace received clear evidence about non-compliant products on its platforms; (4) The producer is identified but does not take measures to remedy the harm, or if; (5) The marketplace has a predominant influence or control in the transaction chain.

7. Review the exemptions to liability:

- Abolish the risk-development defence.
- Compliance with standards should not be valid grounds for escaping liability.

8. Review timelines and prescription periods:

- The 10-year limitation period should be extended to 20 years.

9. Introduce greater transparency measures on defective products:

- Introduce concrete measures to enhance transparency and to monitor defective products (e.g. creation of a registry of product liability cases) within the PLD framework.

Contents:

1. 1985 is not 2020: the urgent need to review the EU product liability framework.....	4
1.1. New rules for new products	4
1.2. Time for action	5
2. The need for an integrated approach to EU product liability	7
2.1. Product liability, digital services and digital content	7
2.2. Product liability, product safety and cybersecurity	8
2.3. Product liability, data protection and privacy	8
2.4. Product liability and roles of intermediaries	9
2.5. EU product liability framework and additional targeted changes in national liability rules based on a risk-based approach	9
2.6. Product liability and enforcement	10
3. Towards EU product liability 2.0.....	11
3.1. Objectives of product liability rules.....	11
3.2. Updating the key notions of the EU product liability framework	12
3.2.1. The definition of “product”	12
3.2.2. The definition of “defect”	13
3.2.3. The notion of “damage”	15
3.2.4. Burden of proof	16
3.2.5. Liable persons	18
3.2.6. Exemptions to liability	19
3.2.7. Timelines and prescription periods	21
4. Additional issue: greater transparency for defective products	22

1. 1985 is not 2020: the urgent need to review the EU product liability framework

1.1. New rules for new products

In 2020, the EU Product Liability Directive ('PLD') **turns 35**.

When it was adopted in 1985, the legislation was regarded as "a bold and modern instrument"¹ and a milestone for consumer protection.² It established a strict liability regime (also referred to as 'liability without fault') where producers are liable for their defective products regardless of whether the defect is their fault. Under this liability regime, consumers can thus obtain compensation if they prove that the product was defective and that it caused damage. Strict liability is a fundamental principle that protects both the interests of consumers and society at large. It offers another layer of protection that national fault-based liability regimes may not provide.

However, the EU product liability framework was established well before the emergence of digital technologies. Products that the drafters of the PLD had in mind in the 1980s are only **a far cry** of those surrounding consumers nowadays. Products fuelled with continuous flows of data, powered by automated decision-making or using machine-learning software have permeated almost all aspects of our lives and are part of our daily routines: from wearables (connected watches, etc.), toys (speaking dolls, etc.), sports and leisure equipment (wristbands, activity trackers, etc.), household appliances (virtual assistants, smart lightening, etc.), and soon autonomous vehicles. Once equipped with sensors, almost all consumer products have the potential to become 'smart': they can track activities, customise users' experience, interact and communicate with their environments (an app can for instance remotely control the thermostat of a central heating system), sometimes in an unforeseeable manner. It is estimated that the number of Internet of Things (IoT) connections within the EU will increase from approximately 1.8 billion in 2013 to almost 6 billion in 2020.³

Since steam-powered machines, technological developments have served as a catalyst for changes in liability rules. Likewise, new technologies are today an opportunity to establish an updated, clear, and enforceable framework for product liability that is adapted to the challenges of the 21st century and to consumers' needs. Undoubtedly, digital goods can bring many benefits and new opportunities. A 2017 European Commission study, for example, highlighted that 67% of Europeans believe that digital technologies have a positive impact on their quality of life.⁴ However, the wide dissemination of digital goods is also a growing source of concern, since flaws in IoT can have dramatic implications for consumers and society.

Although the PLD is meant to be technology-neutral, there are **several fundamental issues** that are undermining its application in the digital context today. As the EU Commission has highlighted, "while in principle the existing Union and national liability laws are able to cope with emerging technologies, the dimension and combined effect of

¹ EU Commission, SWD (2018) 157 final, 7 May 2018.

² G. Risso, "Product Liability and protection of EU consumers: is it time for a serious reassessment?", *Journal of Private International Law*, 2019; G. Howells, "Protecting consumer protection values in the fourth industrial revolution", *Journal of Consumer Policy*, December 2019.

³ EU Commission, SWD (2016) 0110 Final, 19 April 2016.

⁴ EU Commission, Special Eurobarometer 460, "Attitudes towards the impact of digitalisation and automation on daily life", May 2017.

the challenges of AI could make it more difficult to offer victims compensation in all cases where this would be justified”.⁵

Several disruptive features in digital goods nowadays challenge liability rules:

- **Complexity:** digital goods are a composite of multiple parts (hardware, digital contents, etc.), sometimes sold separately and produced by multiple parties (manufacturers, apps developers, operators, programmers, designers, etc.). They are increasingly reliant on complex algorithms and can evolve in environments where several goods may interact with each other.
- **Opacity:** digital goods remain a “black box’ for most consumers. When problems arise, very few individuals have the knowledge that would enable them to identify the problem(s).
- **Autonomy and unpredictability:** digital goods may perform tasks with less or even without human intervention. When equipped with self-learning capacities, they may evolve in directions that were not initially expected by their producer(s) and may even take unintended decisions.
- **Vulnerability:** digital goods are increasingly dependent on the availability and quality of data. Connectivity problems or inappropriate collection or interpretation of data can have detrimental consequences for users and lead to damage. Consider for instance the case of a connected smoke detector failing to detect smoke due to a loss of connectivity. Their dependence on network connections and data also make them particularly vulnerable to cyberattacks.

Updated product liability rules must ensure strong consumer protection in the digital age. **Consumer protection should not be weaker for digital goods than for traditional ‘offline’ products.** This is about enhancing consumer access to justice, trust in products and services based on new technologies,⁶ providing legal certainty,⁷ encouraging innovation,⁸ and ultimately contributing to the proper functioning of the EU Single Market.

1.2. Time for action

In May 2018, the fifth report on the application of the PLD focused on the relevance and suitability of the Directive in the context of new technologies. It concluded that “even though products are much more complex today than in 1985, the PLD continues to be an adequate tool”.⁹ However, the Commission also highlighted that “we need to clarify the legal understanding of certain concepts (such as product, producer, defect, damage, burden of proof) and look closely at certain products such as pharmaceuticals, which may pose a challenge to the performance of the directive”.¹⁰ The Commission thus

⁵ EU Commission, “Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics”, COM (2020)64 final, 19 February 2020.

⁶ www.beuc.eu/publications/beuc-x-2017-137_securing_consumer_trust_in_the_internet_of_things.pdf ; www.consumersinternational.org/news-resources/news/releases/concerns-over-privacy-and-security-contribute-to-consumer-distrust-in-connected-devices.

⁷ As a study for the Commission pointed out in 2018, “both B2B and B2C transactions are suffering undue cost as a result (of the) uncertainty about the extent to which existing liability regimes might apply”, and “building trust in IoTs and its governance is crucial to tap the potential of IoT as a source of economic growth and innovation” (“Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability”, 2018).

⁸ “Internet of Things: implication for governance”, JRC conference and workshop reports, May 2019.

⁹ European Commission, COM (2018) 246 final, 7 May 2018 (p.2).

¹⁰ *Idem*.

acknowledged the existence of several fundamental issues undermining the application of the PLD in the digital context.

In April 2018, the Commission published a staff working document entitled “Liability for emerging digital technologies”,¹¹ which accompanied its Communication on “Artificial Intelligence for Europe”.¹² The purpose of this initiative (*inter alia*) was to establish an appropriate ethical and legal framework for automated decision-making, including guidance on existing product liability rules. The Commission set up an Expert Group in two ‘formations’ (a ‘Liability and New Technologies Formation’ and a ‘Product Liability Formation’) to provide the EU with expertise on the applicability of existing liability regimes to new technologies and new societal challenges. Product liability rules are a pivotal building block within this larger liability framework.

In May 2019, the European Parliament regretted “that no legislative proposal was put forward during [the last] legislature, thereby delaying the update of the liability rules at EU level and threatening the legal certainty across the EU in this area for both traders and consumers”.¹³

In November 2019, the ‘New Technologies Formation’ (the ‘Expert Group’) concluded that some aspects of liability regimes require clarification and, where necessary, amendments to address the new challenges in a fair manner for society. In particular, the Expert Group highlighted that “the progressive sophistication of the market and the pervasive penetration of emerging digital technologies reveal that some key concepts require clarification. This is because the key aspects of the PLD’s liability regime have been designed with traditional products and business models in mind.”¹⁴

In January 2020, the Committee on the Internal Market and Consumer Protection (IMCO) of the European Parliament submitted a motion for a resolution where it called on the Commission “to review the Directive and consider adapting such concepts as ‘product’ ‘damage’ and ‘defect’ as well as adapting the rules governing the burden of proof”.¹⁵ Since the beginning of 2020, the European Parliament has been working on a new initiative on “Civil liability regime for Artificial Intelligence”.¹⁶

In February 2020, the EU Commission published its White Paper on Artificial Intelligence¹⁷ accompanied by a report on the safety and liability implications of AI, the Internet of things and Robotics to consider possible adjustments to the existing EU legislative instruments, including the PLD.¹⁸

In parallel, at national level, Member States have been discussing several options for adapting their national liability rules to the challenges of new technologies. These patchy national approaches are likely to **significantly compartmentalise and complexify the functioning of the EU Single Market**. It is therefore in the interest of all stakeholders to push for a sound and coordinated revision of the EU framework for product liability.

¹¹ European Commission, SWD(2018) 137 final, 25 April 2018.

¹² European Commission, COM(2018) 237 final, 25 April 2018.

¹³ European Parliament, P8_TA(2019)0081, 12 February 2019 (pt 132).

¹⁴ Expert Group on Liability and New Technologies – New Technologies Formation, “Liability for Artificial Intelligence”, November 2019 - hereafter “Expert Group report” (pp.27-28).

¹⁵ IMCO Committee, Motion for a resolution on automated decision-making processes: ensuring consumer protection and free movement of goods and services, February 2020.

¹⁶ INL Civil Liability regime for Artificial Intelligence (ongoing – last updates May 2020).

¹⁷ European Commission, COM (2020)65 final, 19 February 2020.

¹⁸ European Commission, COM (2020)64 final, 19 February 2020.

2. The need for an integrated approach to EU product liability

Product liability rules in the digital age should not be viewed in isolation but seen instead as evolving in a complex and dynamic ecosystem. They stand at the crossroads of multiple interacting sectors with many inter-twining issues. The situation may be described as follows:



2.1. Product liability, digital services and digital content

Digital goods have blurred the distinction existing between products and services. As the Expert Group pointed out, “in AI systems, products and services **permanently interact and a sharp separation between them is unfeasible**”.¹⁹ It is regrettable that past EU initiatives on the liability of service providers have so far failed. In 1990, the Commission proposal for a Directive on the liability of suppliers of services was supposed to be a useful complement of the PLD but it never became a binding legal instrument.²⁰

The EU has already taken several steps to adapt the EU consumer law acquis to the digital environment: Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services, Directive 2019/771 on contracts for the sales of good are examples showing how existing legal frameworks can be adapted to digital contexts.

It is essential that product liability rules are approached with consistency regarding these recent initiatives and in line with developments of the EU consumer law acquis. It should also be aligned with the e-Commerce Directive (in the context of the ongoing discussions on the Digital Services Act).²¹

¹⁹ Expert Group report (p.28).

²⁰ European Commission, COM (90)482 final), 24 October 1990.

²¹ BEUC position paper “[Making the Digital Services Act work for consumers – BEUC's recommendations](#)”, May 2019.

2.2. Product liability, product safety and cybersecurity

An effective product liability regime must go hand-in-hand with updated product safety rules. Although both sets of rules follow different policy objectives, together they are two complementary branches of a broader complex system aimed at ensuring stronger consumer protection. In a 2020 Report, the EU Commission highlighted that, “at Union level, product safety and product liability provisions are two complementary mechanisms to pursue the same policy goal of a functioning single market for goods that ensure high levels of safety, i.e. minimise the risk of harm to users and provides for compensation for damage resulting from defective goods”.²²

Like the General Product Safety Directive (GPSD),²³ the PLD is not adapted to deal with new risks such as cyberattacks and other security vulnerabilities. As the Expert Group noted, “with enhanced complexity, openness and vulnerability, there comes a greater need to introduce new safety rules. Digital product safety differs from product safety in traditional terms in a number of ways, including by taking into account any effect a product may have on the user’s digital environment. Even more importantly, cybersecurity has become essential”.²⁴ The lack of cybersecurity measures in connected products is particularly acute and has been illustrated by numerous testing performed by consumer organisations on a wide range of products.²⁵ In February 2020, a research conducted by the Dutch consumer organisation Consumentenbond revealed that many ‘smart’ products are vulnerable to hacks. Consumentenbond tested 10 products and found security issues with two sex toys, two children's GPS watches and two baby cameras. In total, the investigations and hack tests revealed 27 vulnerabilities.²⁶ In May 2018, Test Achats/Test Aankoop installed 19 smart devices in a house (a fridge, an alarm system, a thermostat, a printer, a children's tablet, a door lock, a speaker and a connected vacuum cleaner) and challenged two ‘ethical hackers’ to find security vulnerabilities within a specific time period. Within five days, more than half of the products were found to be vulnerable.²⁷ In October 2017, a study conducted by the Norwegian Consumer Council found critical security flaws in several smartwatches for children.²⁸

Poorly designed interfaces can serve as entry points for cyberattacks and undermine the functioning and security of many IoT appliances, such as smart thermostats or door locks, and thus putting individuals at risk.

2.3. Product liability, data protection and privacy

Connected products can cause a much wider range of harm than other traditional ‘offline’ products. This includes the exposure of personal data, which has potentially damaging consequences for users.

It is essential that the PLD is aligned with and built on the EU General Data Protection Regulation (GDPR). The PLD should also support the privacy-by-design/privacy-by-default-rule for all IoT products. Compliance with the privacy-by-default/privacy-by-design rule should be considered as part of the reasonable expectations that consumers have for their digital products. Consumers should be able to rely on the PLD whenever the defect causes

²² European Commission, COM (2020)64 final, 19 February 2020.

²³ See “BEUC’s views for a modern regulatory framework on product safety Keeping consumer safe through a revision of the General Product Safety Directive” (forthcoming and soon available on BEUC website).

²⁴ Expert Group report (p.48).

²⁵ BEUC position paper, “Keeping consumers secure: How to tackle cybersecurity threats through EU law”, November 2019.

²⁶ www.consumentenbond.nl/nieuws/2020/fabrikanten-laks-met-veiligheid-slimme-apparaten

²⁷ www.test-achats.be/action/espace-presse/communiqués-de-presse/2018/hackable-home

²⁸ <https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-oktober-2017.pdf>

privacy-related harm caused by a violation of the privacy-by-design/privacy-by-default rule.

2.4. Product liability and the role of intermediaries

Updated product liability rules need to consider the development of online distribution channels and the role of the various intermediaries intervening in the supply chain. **Significantly, this now includes online marketplaces.**

Online marketplaces intervene in many ways (e.g. by collecting payments, advertising products, putting consumers and traders in contact etc.) and strongly influence the behaviours of traders and consumers. **They can no longer be regarded as passive intermediaries.** In parallel, dangerous and defective products can increasingly be found on online marketplaces as our members' testing demonstrates. In February 2020, a research conducted by the International Consumer Research and Testing (ICRT) revealed that, out of 250 key consumer products (e.g. toys, textiles, cosmetics, electric and electronic devices), two third were found to be unsafe and illegal on the European market.²⁹ As Which? points out, "people do not have the same protections as they do when buying from traditional retail outlets or websites, leaving them exposed to unsafe products".³⁰ If online marketplaces cannot be held liable for the defective products that they distribute, they may not be incentivised to prevent the circulation of such harmful goods.

For comparison purposes, it is noteworthy that Amazon was found liable in the United States for damage suffered by a consumer who was the victim of a defective product purchased through its online marketplace.³¹

2.5. EU product liability framework and additional targeted changes in national liability rules based on a risk-based approach

Other non-harmonised (contractual or non-contractual) liability regimes may apply to digital goods in parallel to the harmonised EU product liability rules. They give consumers several options for obtaining compensation. However, as the European Commission has highlighted, "the characteristics of emerging digital technologies like AI, the IoT and robotics challenge aspects of Union and national liability frameworks and could reduce their effectiveness (...). This means that liability claims based on national tort laws may be difficult or overly costly to prove and consequently victims may not be adequately compensated".³²

In its White Paper on AI, the European Commission noted that all options to adapt liability frameworks "should be carefully assessed, including possible amendment to the PLD and possible further targeted harmonisation of national liability rules". These additional targeted amendments to national liability rules would follow a risk-based approach that would differentiate "high-risk" AI applications (i.e., drones, autonomous vehicles), which are applications exposing the public at large and causing harm to important legal interest (e.g. life, health, etc), from other risks. High-risk AI applications would be accompanied by a strict liability regime whereas, for low-risk applications, some amendments to national liability rules (such as a possible adaptation to the burden of proof concerning causation and fault) would be enough.

²⁹www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html

³⁰ <https://www.which.co.uk/policy/consumers/5234/onlinemarketplaces>

³¹ Case No. 18-1041; *Oberdorf v. Amazon*, United States Court of Appeals for the Third Circuit, 3 July 2019.

³² European Commission, COM (2020)64 final, 19 February 2020.

Yet, as far as liability rules are concerned, such a risk-based approach is problematic from a consumer perspective:

First, the risk-based approach is not in the interests of consumers because liability rules mostly intervene downstream. It does not matter whether the product that caused the harm has been classified as low- or high-risk. **What truly matters for consumers is a fair compensation for the damage suffered, regardless of what type of risk ultimately materialised.**

Second, it is crucial to **avoid adding another layer of complexity to already complex situations.** If a new legislation on AI liability were introduced for some categories of digital products, consumers may find it very confusing and difficult to understand which sets of rules apply to their case.

Third, the risk-based approach may be **difficult to enforce in practice and will raise many interpretive issues.** It also fails to consider the dynamic nature of digital goods: classifying goods as low- or high-risk might mean “freezing” their features at a specific moment in time. Unless there are clear obligations for traders to monitor their products and unless these obligations are strictly and carefully enforced, the risk classification may not properly follow the dynamic nature of digital products.

Fourth, the risk-based approach could **exacerbate the fragmentation of the Single Market for low-risk AI applications** as Member States may introduce different rules for these types of products. Again, this would go against the need for simplification and clarity that consumers are demanding today.

Therefore, amendments to national liability rules should by no means replace a sound revision of the PLD. It is essential that the PLD is updated in any event. If special liability rules were to be introduced anyway for some categories of digital products, it would be very important to **clarify the interplay between the upgraded EU product liability regime and the special liability rules targeting high-risk digital products.** Differences between liability regimes should be minimised. In any case, the EU product liability framework **should operate as a clear safety net for all consumers** when things go wrong with their digital and offline goods.

2.6. Product liability and enforcement

The PLD does not contain any specific provisions about access to court for injured parties. Harmed individuals must use national-level solutions, which may significantly differ across Member States.³³ Revised product liability rules should establish an enforceable legal framework ensuring effective access to justice for all consumers. It should not be unduly burdensome for injured parties to prove their claims when they have suffered harm resulting from defective products.

Furthermore, the specific features of digital goods can cause additional enforcement problems for consumers when seeking compensation. For example, if software were to be considered as a ‘product’ within the context of the PLD, the problem remains that many of them may be provided from countries that are located outside the EEA.³⁴ When problems arise, this situation is likely to make it very complicated (if not impossible) for consumers to seek redress and obtain compensation. It should therefore always be possible for consumers to channel liability to (at least) one actor in the supply chain operating in the EU.

³³ European Commission, COM/2011/0547 final, 10 May 2009.

³⁴ See presentation by Prof. Wendehorst at IMCO Public Hearing “Product Liability Directive: Protecting Consumers in the Digital Single Market”, 22 January 2020.

3. Towards EU product liability 2.0

3.1. Objectives of product liability rules

The PLD has been criticised for its **lack of clarity** when it comes to its policy objectives.³⁵ The first preamble of the PLD refers to the need to avoid the distortion of competition between Member States and to ensure the Single Market functions properly. However, the very same preamble also points out the undesirability of “a differing degree of protection of the consumer” in the EU. The fact that consumer protection is a key driver behind the PLD is evidenced by the fact that consumer protection is mentioned no less than 13 times in the preambles of the Directive.

When amending the EU product liability regime, it is essential to keep in mind the objectives that the rules intend to achieve. First, they should ensure **full compensation** to injured parties for the harm they have suffered. Second, they should provide the **right set of behavioural incentives to all parties involved in the supply chain**. These parties should be incentivised to fully internalise the risks of their products and to take the precautionary measures that would prevent harmful situations from occurring in the first place. Third, liability rules should be fair and cost-effective: the complexity and opacity of digital goods should neither deter injured parties from seeking compensation nor make their actions unduly costly or burdensome. **It should be up to the party that has access to the relevant information to investigate the cause of the problem when problems arise.**

Importantly, the specific characteristics of digital goods – in particular, their ever-changing nature through the availability of updates and increasingly through self-learning software - require **approaching these objectives in a dynamic way** as producers can today keep control over their products even after they have been put on the market. They should therefore be required to internalise the risks of their products and to compensate consumers for defects during the entire lifespan of the products.

Finally, in accordance with Article 12 TFUE³⁶ and Article 38 of the EU Charter of Fundamental Rights³⁷, a revision of product liability rules should aim at guaranteeing high consumer protection.

BEUC recommendation:

- **Achieving high consumer protection should be stated as a key policy objective for the PLD.**

³⁵ G. Howells & M. Pilgerstorfer “Product Liability”, in: C. Twigg-Flesner (ed.), *European Union Private Law*, Cambridge University Press, 2010 (p. 259).

³⁶ Art. 12 TFUE provides that “consumer protection requirements shall be taken into account in defining and implementing other Union policies and activities”.

³⁷ Art. 38 of the Charter provides that “Union policies shall ensure a high level of consumer protection”.

3.2. Updating the key notions of the EU product liability framework

3.2.1. The definition of a 'product'

- **What is the situation?**

The PLD applies to “movables” (Art.2), which essentially means tangible goods.³⁸ With the exception of electricity (expressly considered as a product under the PLD), the status of intangible goods is not addressed in the PLD.

- **Why this is problematic:**

The scope of the PLD is currently too restrictive. The need to broaden it has been acknowledged by public authorities, civil society organisations and even producers.³⁹ The current scope leaves many pivotal issues unresolved and left to diverging national interpretations. This situation has multiplied the risks of unjustifiable unequal treatments between consumers who live in different Member States.

It is usually accepted that a 'product' can also include digital content if they are embedded into a tangible media.⁴⁰ This covers the hardware/software bundle that characterises many IoT products, such as smart meters or connected household appliances. A problem with the embedded software renders the final 'hard' product defective, which ultimately triggers the liability of the producer.

However, it is open to debate whether digital content *itself* qualifies as a 'product' within the meaning of the PLD. The question is particularly acute for unbundled 'standalone' software that can be downloaded separately and added to existing hardware. In the near future, it can also be expected that hardware and software will no longer come as a bundle but will be purchased separately. Consumers may also have the possibility to change or modify pre-installed software. In this context, there is uncertainty as to whether software should be considered as a product or a service,⁴¹ and whether the PLD is ultimately applicable.⁴²

Views on the legal classification of digital content diverge across the EU and there is little guidance to solve this issue currently. Even though the Commission confirmed in 1988 that software is a product within the meaning of the PLD, this guidance is of little help today as software in the 1980s, which necessarily came with tangible media, is very different from software in the 2020s.

³⁸ In some Member States (e.g. Austria), implementing legislations expressly defined “products” as tangible goods.

³⁹ European Commission, SWD (2018) 157 final, 7 May 2018.

⁴⁰ This approach is coherent with the PLD since the directive does not specify whether component parts also need to be tangible.

⁴¹ A distinction is sometimes made in the academic literature between “standardised software” and “bespoke software”: standardised and mass-produced software is usually considered as “a product”, while bespoke software is seen as an “individualised service” (see e.g. D. Fairgrieve, “Product Liability in the United Kingdom – Country report”, *EuCML* 4/2019; Howells G. and *al.*, “Product Liability and Digital Products”, in: T.E. Synodinou (Ed.), *EU Internet Law – Regulation and Enforcement*, Springer 2017).

⁴² On the one hand, computer code is not a movable and as such does not fall within the scope of the PLD. On the other hand, as some academics have pointed out, it may be possible to apply “an expanded, digitalised interpretation of the concept “movable””(see e.g. G. Wagner “Robot Liability” in: S. Lohsse, R. Schulze, D. Staudenmayer (Eds). *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019, p.42).

It is essential to revise the notion of a product to consider its full 'digitalised dimension' in which tangible items, digital services and digital content continuously interact and cannot be differentiated. All of them should be covered under the definition of a 'product'.⁴³

BEUC recommendation:

- **The PLD should apply to all tangible and non-tangible goods, including digital services and digital content.**

3.2.2. The definition of 'defect'

○ **What is the situation?**

The producer's liability is dependent on the finding of a defect. A product is considered 'defective' within the meaning of the PLD when it does not provide the "safety which a person is entitled to expect". Expectations must be assessed considering "all circumstances" and the PLD gives a non-exhaustive list of criteria (e.g. the presentation of the product, the use to which it could reasonably be expected that the product would be put, the time when the product was put into circulation, etc.).

○ **Why this is problematic:**

What constitutes a 'defect' in a digital context is a controversial matter.

First, the current notion of defect strictly focuses on the safety expectations of users, which refers to physical risks. It leaves aside other notions that, without being strictly safety-related, remain pivotal in the context of product liability for IoTs. For example, it is unclear whether **cybersecurity flaws or a loss of connectivity** can be regarded as a defect when they do not cause direct physical risks. The issue is now highly relevant: in January 2020, a survey showed that Europeans are increasingly less confident about their capacity to stay safe online. Many tend to worry about possible misuse of their personal data, fraud or identity theft.⁴⁴ The PLD should therefore build on an extended notion of 'defect' covering all kind of risks arising from the product according to its use and including cybersecurity risks, personal security risks, or risks related to a loss of connectivity.

Second, when it comes to digital contexts, users' reasonable expectations about their products are much wider than for traditional 'offline' products. In particular, digital goods are not in line with the reasonable expectations of users when they can cause harm stemming from data protection or privacy infringements. Consider for example the case of connected smart meters like connected watches 'leaking' personal data to third parties and causing harm. It is important that products' compliance with the privacy-by-design/privacy-by-default rule set down in the GDPR is considered as part of the reasonable expectations that users may have for their digital products. Deviation from this rule should render the product defective.

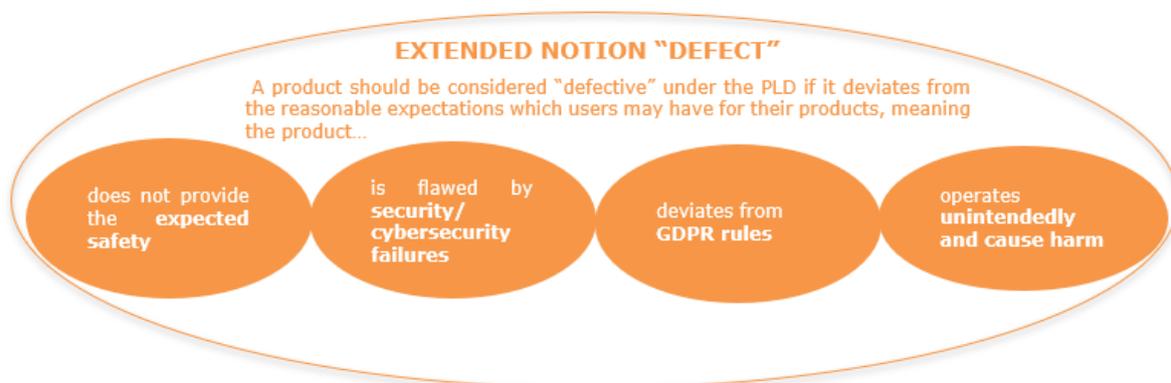
⁴³ For consistency with other EU initiatives, the definition of digital content and digital services should be aligned with the definitions provided for in the digital content Directive where 'digital content' means (a) data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software, (b) a service allowing the creation, processing or storage of data in digital form, where such data is provided by the consumer, and (c) a service allowing sharing of and any other interaction with data in digital form provided by other users of the service;

⁴⁴ Special Eurobarometer 499 - Europeans' attitudes towards cyber security, January 2020.

Third, in a context where an ever-increasing number of IoT products have self-learning capacities and are likely to take autonomous decisions, it should be clear that a product is defective when its unintended behaviour has caused harm or undesirable results to the user. Consider for example the case of virtual assistants like smart fridges ordering wrong groceries and causing economic losses due to their unintended behaviour. The unintended, autonomous behaviour of a robot should be considered as a 'defect' when it causes harm.⁴⁵

Users' safety expectations should no longer be the only benchmark to assess the defectiveness of a product. We propose to introduce an extended notion of 'defect' based on the reasonable expectations which users may have for their products.

This extended notion of defect could be summarised as follows:



In parallel, a defect shall be assessed considering "the time when the product was put into circulation" (Art.6.1.b). "Putting into circulation" is a notion that has triggered many interpretative questions.⁴⁶ Once again, **the problem is exacerbated in the context of digital goods**. With the possibility of updating their goods, producers keep a high degree of control over their products even after they have been put onto the market.⁴⁷ Therefore, as the Expert Group highlighted, "the point in time at which a product is placed on the market should not set a strict limit on the producer's liability for defects where, after that point in time, the producer or a third party acting on behalf of the producer remains in charge of providing updates or digital services".⁴⁸

The concept of 'defect' should fully embrace the dynamic nature of digital goods, and consumers should be able to expect producers to take care of their products on an on-going basis. For comparison purposes, the Digital Content Directive already provides that the trader (i.e. the seller) shall ensure that the consumer is informed of and supplied with updates, including security updates, that are necessary to keep the digital content or digital service in conformity for the period of time (Art.8 2b). Similarly, the Directive on the sales of goods (2019/771) also provides that a seller is liable for digital elements being in conformity with the product including for updates provided for as long as the consumer may reasonably expect (Art.7.3). A product should therefore be considered defective when the producer fails to provide (or provide insufficient) after-market updates, thereby preventing the harm from happening.

⁴⁵ G. Howells and al., "Product Liability and Digital Products", in: T.E. Synodinou (Ed.), *EU Internet Law – Regulation and Enforcement*, Springer 2017.

⁴⁶ See e.g. CJEU Case C-127/04 *Declan O'Byrne v. Sanofi Pasteur MSD*, 9 February 2006 (ECLI:EU:C:2006:93).

⁴⁷ BEUC Position paper "[AI Rights for consumers](#)", 23 October 2019.

⁴⁸ Expert Group Report (p.43).

BEUC recommendations:

- **The PLD should build on an extended notion of 'defect', which is no longer only limited to users' safety expectations. A product should be considered 'defective' when it deviates from the reasonable expectations that users may have, which include: the product should be safe, it should be free from cybersecurity failures or other personal security risks and should be GDPR compliant. Moreover, a product using self-learning capacities and taking autonomous decisions should be deemed defective when its unintended behaviour has caused harm to the user.**
- **The time at which the product was placed on the market should no longer be relevant when it comes to the defect.**
- **A lack of after-market updates by the producer(s) should be considered as a defect in case of harm to the user.**

3.2.3. The notion of 'damage'

○ **What is the situation?**

The PLD only covers physical injuries and damage to property arising out in non-professional activities with a lower threshold of €500 (Art. 9). France and Greece initially transposed the PLD without this threshold. The Court of Justice of the European Union ruled that both countries had violated their obligation to correctly transpose the Directive as the PLD is of full harmonisation.⁴⁹ In addition, Member States were given the possibility to set a maximum ceiling of €70m (Art.17). Some Member States used the possibility to introduce such a cap.

○ **Why this is problematic:**

- *Compensable harm*

The PLD leaves aside compensation for pure economic losses. Yet with the life of consumers being increasingly virtualised, **digital products have triggered significant changes in the types of harm likely to impair their wellbeing** (e.g. loss of data, identify theft, privacy, etc). In this context, it is unclear whether data loss falls within the scope of the PLD. As the Expert Group has noted, it is "not universally accepted throughout Europe that damage to or the destruction of data is a property loss since in some legal systems the notion of property is limited to corporeal objects and excludes intangibles".⁵⁰ In line with the recommendation of the Expert Group,⁵¹ damage to data should be regarded as a damage compensable under the PLD.

- *The €500 lower threshold*

Consumers have long indicated that the €500 threshold unduly restrains the number of cases for which consumers can claim compensation.

⁴⁹ CJEU, case C-52/00 *Commission v. France*, 25 April 2002 (ECLI:EU:C:2002:252).

⁵⁰ Expert Group report (p.19).

⁵¹ Expert Group report (p.4).

First, the threshold was initially adopted to avoid a flood of small cases against producers.⁵² However, in practice, this concern has been more hypothetical than real.⁵³ Conversely, **this threshold has contributed to impairing consumers' access to justice** and limiting their compensation. As the Commission noted in 2018, "according to the information obtained, in four out of five cases a compensation is not claimed as the damage is below the threshold".⁵⁴

Second, the threshold has given rise to diverging national interpretations. In some Member States, the threshold is regarded as a deductible (i.e. the amount of damages awarded to the claimant is reduced by this amount in case of success) while in others this amount is a minimum, below which no damages can be recovered. Consumers may therefore suffer from different levels of protection across the EU, which is not acceptable from a Single Market perspective.

Third, should a loss or destruction of data eventually be regarded as a compensable harm, quantifying such a loss may lead to different results in Member States. For example, some Member States may take the view that a loss of data is below the threshold. This would create the risk of unequal treatment between consumers.

Fourth, there is a contradiction between, on the one hand, current EU efforts to facilitate law enforcement and compensation for small-value claims (see for example the proposal for a Directive on representative actions for consumers) and, on the other hand, the €500 threshold, which precisely hinders such claims from being brought.

- *The maximum ceiling of €70m*

The maximum ceiling of €70m creates an unfair distribution of risks for product liability in the case of damage to persons caused by identical items with the same defect. This cap should be removed as well in order to respect the fundamental right of redress for damage suffered. **Damage should always be fully compensated.**

BEUC recommendations:

- **The PLD should also cover damage to digital assets, including data.**
- **The €500 threshold should be removed.**
- **The maximum cap of €70m should be removed.**

3.2.4. Burden of proof

○ **What is the situation?**

The injured party must prove the damage, the defect and the causal relationship between the damage and the defect (Art.4). If proving the damage is often relatively simple, this however does not constitute the proof that the product is defective. The claimant must still prove the defect and the causal link. In many cases, consumers cannot provide proof and therefore their rights cannot be enforced.

⁵² Recital 10 of the PLD ("a lower threshold of a fixed amount in order to avoid litigation in an excessive number of cases").

⁵³ See e.g. the situation in Spain where an academic observer highlighted, "after more than three decades of PLD, the fear of an avalanche of claims against producers the threshold of 500 Euros was aimed to contained has not materialized. Thus, some scholars advocate for eliminating the threshold" (T. Rodriguez de las Heras Ballell, "Product Liability in Spain – Country report", *EuCML*, 4/2019).

⁵⁴ European Commission, SWD (2018) 157 final, 7 May.

The burden of proof is clearly the pivotal element upon which rests the right to compensation.⁵⁵ As the 2018 report on the evaluation of the PLD highlighted, “the most frequent reasons to reject claims relate to the proof of the defect and its link with the damage, which together account for **53% of the cases of rejection**. Difficulties in applying the definition of defective product and subsequently in proving the link between damage and defect seem to be particularly relevant in cases of complex products, such as pharmaceuticals”.⁵⁶

Under certain circumstances, the Court of Justice of the European Union has cleared national rules that help injured parties to substantiate their claims. For example, in *Boston Scientific* (joined cases C-503/13 and 504/13), the Court ruled that products of the same batch or production series with a potential defect may be considered as defective without the need to establish the defect of the actual product.⁵⁷

Furthermore, in *Sanofi Pasteur* (case C-621/15), the Court cleared national evidentiary rules allowing factual evidence to constitute serious, specific and consistent evidence of a defect and to constitute the causal link with the damage, even in the absence of conclusive scientific evidence.⁵⁸

However, the PLD leaves it up to the Member States to decide on evidentiary rules.

- **Why this is problematic:**

New technologies have exacerbated evidentiary difficulties for consumers who must bear the burden of proof. In practice, this means that their rights cannot be enforced and that they are denied access to justice. This view is also supported by academics stressing that the burden of proof “will weigh even more heavily upon the person injured by digital goods than the one injured by traditional products”.⁵⁹

- **Proving the defect:** defects in digital goods can be multi-faceted and multi-centred. As the Expert Group pointed out in November 2019, “the interconnectivity of products and systems makes it hard to identify defectiveness”.⁶⁰ In addition, traditional methods for evaluating defects may no longer be adapted when it comes to complex algorithms.⁶¹
- **Establishing the causal link:** problems resulting from digital goods can have a multitude of complex concurring causes. As the Expert Group noted, “it will become much more of an issue in the future, given the interconnectedness of emerging digital technologies and their increased dependency on external input and data, making it increasingly doubtful whether the damage at stake was triggered by a single original cause or the interplay of multiple (actual or potential) causes”.⁶²

As the Expert group also noted, “features of emerging digital technologies, such as opacity, openness, autonomy, and limited predictability may often result in unreasonable difficulties or costs for the victim to establish both what an average user is entitled to expect, and the failure to achieve this level of safety. At the same time, it may be significantly easier

⁵⁵ European Commission, SWD (2018) 158 final, 7 May 2018 (p.25).

⁵⁶ *Idem*.

⁵⁷ Joined cases C-503/13 and 504/13, *Boston Scientific*, 5 March 2015 (ECLI:EU:C:2015:148).

⁵⁸ Case C-621/15 *N.W and Others v Sanofi Pasteur*, 21 June 2017 (ECLI:EU:C:2017:484).

⁵⁹ See e.g. references given in G. Wagner “Robot Liability” in: S. Lohsse, R. Schulze, D. Staudenmayer (Eds). *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019.

⁶⁰ Expert Group report (p.28).

⁶¹ J.-S. Borghetti, “How can Artificial Intelligence be Defective?”, in: S. Lohsse, R. Schulze, D. Staudenmayer (Eds). *Liability for Artificial Intelligence and the Internet of Things*, Nomos, 2019.

⁶² Expert Group report (p.22).

for the producer to prove relevant facts. **This asymmetry justifies the reversal of the burden of proof**".⁶³

For reasons of fairness, and to mitigate the informational asymmetries impairing the situation of injured parties, we call for a reversal of the burden of proof concerning defect and causation. It should be enough for the injured party to prove the existence of damage resulting from a product. It should then be up to the producer to provide the proof that the product was free of defects where a damage occurred. It should be the responsibility of the company with access to relevant information and technical means to investigate the cause of the damage.

BEUC recommendation:

- **The burden of the proof concerning defect and causation should be reversed. It should be enough for the injured party to prove the existing of a damage resulting from a product.**

3.2.5. Liable persons

○ **What is the situation?**

Under the PLD (Art.3), liability rests on the 'producer,' which covers:

- The manufacturer of the finished product.
- The producer of any raw material or the manufacturer of any component part.
- Any person, who, by putting their name or other distinguishing feature on the product, presents themselves as a producer.

The following persons may also be held liable under the PLD:

- The person who imports a product into the EU.
- The person supplying a product where the producer or the importer cannot be identified and where the supplier fails to inform, within a reasonable time, the injured person of the identity of the producer or of the person who supplied them with the product.

○ **Why this is problematic:**

Current EU product liability rules do not apply to all parties involved in the supply chain. Many actors who come to be in contact with the product still fall outside the scope of the PLD.⁶⁴ Yet in practice, digital goods require **the intervention of many different parties** (e.g. manufacturers, software developers, creators of digital content etc.) It is, for example, unclear whether stand-alone software developers fall within the scope of the PLD. If the PLD is revised to also cover digital content and digital services, those providing digital input should also be considered as "manufacturers of any component part", and thus be held liable as well. In any case, all professionals involved in the production of digital goods should be held **jointly liable** if their activities have affected the reasonable expectations which users may have about their product. Consumers' options for recourse should not be prevented by problems in identifying the relevant liable party in situations where different parties are involved in the production chain.

⁶³ Expert Group report (p.44).

⁶⁴ The Court of Justice of the EU illustrated this restrictive approach in a decision *Skov Æg v. Bilka* where it considered a provision in Danish law making the vendor liable for safety defects on the same basis as the producer to be an incorrect transposition of the PLD (case C-402/03, *Skov v Bilka*, 10 January 2006-ECLI:EU:C:2006:6).

In addition, specific attention should be given to the role of **online marketplaces**. They can play an important role in minimising the harm as they have substantial control over the transaction chain and can remove defective products from circulation. Furthermore, online marketplaces can be clear 'go-to-points' for consumers when things go wrong. A 2019 study by our German Member vzbv noted that "there is (...) a need for clarification with regard to the liability of online platforms under product liability law."⁶⁵

The PLD already provides for a subsidiary liability for "suppliers" (Art. 3.3) which can be applied to online marketplaces distributing defective products.

Therefore, online marketplaces should be **liable as "suppliers"** under the PLD when at least one of the following conditions is fulfilled:

- (1) The producer cannot be identified.
- (2) The marketplace fails to inform the consumer in due time of the identity of the producer and does not enable communication between the consumer and the producer by providing them with relevant contact details.
- (3) The marketplace received clear evidence about non-compliant products on its platforms.
- (4) The producer is identified but does not take measures to remedy the harm; or
- (5) The marketplace has a predominant influence or control in the transaction chain.

BEUC recommendations:

- **All professionals involved in the production chain of digital goods should be jointly liable if their activities have affected the reasonable expectations which users may have about their products.**
- **Online marketplaces should bear subsidiary liability as 'suppliers' under the PLD and be liable when at least one of the following conditions is fulfilled: (1) the producer cannot be identified, (2) the marketplace fails to inform the consumer in due time of the identity of the producer and does not enable communication between the consumer and the producer by providing them with relevant contact details, (3) the marketplace received clear evidence about non-compliant products on its platforms, (4) the producer is identified but does not take measures to remedy the harm, or if (5) the marketplace has a predominant influence or control in the transaction chain.**

3.2.6. Exemptions to liability

When it is established that a product is defective, the PLD provides the defendant with several defences to escape liability. Two are particularly controversial in the context of new technologies, namely the so-called 'development-risk defence' and the 'regulatory compliance' defence.

⁶⁵ vzbv, "Effektiver Verbraucherschutz im online-handel: Verantwortung und Haftung von Internetplattformen – Rechtsgutachten im Auftrag des Vzbv, November 2019", p.10 (www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf).

- *Development-risk defence*

o **What is the situation?**

The development risk defence (Art. 7e) provides that the producer shall not be liable if the state of scientific and technical knowledge at the time when the product was put into circulation was not such as to enable the existence of the defect to be discovered.

o **Why this is problematic:**

The development-risk defence was initially not in the first legislative proposal and the Commission objected to it. It was so controversial that Member States were given an option on whether to introduce this liability defence in their national systems. Most Member States retained the development-risk defence and only few excluded it. The wording of the development-risk defence has however raised many interpretive issues. As an observer highlighted, "more generally, one could say that the more innovative the industry, the less clear (but the more important) the application of the [development risk defence] seems to get".⁶⁶ In November 2019, the Expert Group further noted that the risk development defence "may become much more important practically with regard to sophisticatedly AI-based products".⁶⁷

Many digital goods may change after they have been put onto the market. It is therefore essential that an injured person who suffers damage be always compensated regardless of whether the defect was detectable or not. As the Expert Group noted, "the producer should be strictly liable for defects in emerging digital technologies even if said defects appear after the product was put into circulation, as long as the producer was still in control of updates to, or upgrades on, the technology. A development risk defence should not apply". It is noteworthy that some Member States are currently considering removing the development-risk defence for some categories of products.⁶⁸

A common argument supporting the development risk defence and often brought by the industry regards the alleged explosion of product insurance rates in the event this defence was removed. This argument is not new and was already raised as early as in 1985. Yet there is no evidence that this concern has actually materialised in practice.

Furthermore, the Ethics Guidelines for Trustworthy Artificial Intelligence prepared by the High-Level Group on AI have also stressed the importance of **vigilant post-marketing behaviour** and highlighted that, "AI systems should have safeguards that enable a fall-back plan in case of problems. This includes the minimisation of unintended consequences and errors (...)".⁶⁹

BEUC recommendation:

- **The development risk-defence should be abolished.**

⁶⁶ B. Koch, "The development risk-defence of the EC Product Liability Directive", *Pharmaceuticals Policy and Law*, 20/2018, 163-176 (p.165).

⁶⁷ Expert Group report (p. 29).

⁶⁸ Removing the development risk defence for pharmaceuticals is for example discussed in France (see "Projet de réforme de la responsabilité civile", March 2017).

⁶⁹ "Ethics Guidelines for Trustworthy AI" prepared by High-Level Expert Group on AI, April 2019 (p.16).

- *Regulatory compliance defence*

o **What is the situation?**

The defence based on compliance (Art. 7d) provides that the producer shall not be liable if the defect is due to compliance of the product with mandatory regulation issued by public authorities. As observers have noted, "this clearly cannot be interpreted as a broad statutory compliance defence (...)".⁷⁰ In its transposition, France for instance made it clear that a producer can be held liable for a defect although the product was manufactured in accordance with the rules of the trade or existing standards or although it was the subject of an administrative authorisation.⁷¹ The European Commission raised the issue of regulatory compliance in its 2006 report on the application of the PLD, and noted that "some stakeholders, and in particular representatives of the pharmaceutical industry, have argued strongly for the introduction of a defence of regulatory compliance, which would apply to a product whose safety was closely regulated, provided that the product complied fully with the applicable regulations".⁷²

o **Why this is problematic:**

The pace at which new technologies evolve is changing rapidly. This situation makes standards quickly out-of-date. It is essential that producers remain required to identify new threats and possible defects likely to impair consumers' wellbeing on an ongoing basis. Therefore, compliance with standards should not exonerate producers from their liability for defective products.

BEUC recommendation:

- **Compliance with standards cannot be valid grounds for escaping liability.**

3.2.7. Timelines and prescription periods

o **What is the situation?**

The PLD establishes two deadlines: the PLD no longer applies **three years** after the injured party knew or could have become aware of the relevant facts (i.e. the damage, the defect and the identity of the producer) (Art. 10), and it ends **ten years** after the date the product was put onto the market (Art. 11).

o **Why this is problematic:**

The PLD introduced these time limits to counterbalance the strict liability regime and to avoid hindering innovations.⁷³ However, these timelines are no longer appropriate.

First, when it comes to digital goods, producers keep significant control over their products even after they have been put onto the market. When digital contents are provided on a continuous basis, it is essential that consumers be protected during the entire lifespan of the product.

⁷⁰ D. Fairgrieve and G. Howells, "Rethinking product liability: a missing element in the European Commission's third review of the European Product Liability Directive", 70 *Mod. L. Rev.* 962, 2007.

⁷¹ See Art. 1245-9 of French Civil Code.

⁷² European Commission, COM/2006/0496 final, 14 September 2006.

⁷³ EU Commission, COM (1999)396 Final, 28 July 1999.

Second, the time limits are not appropriate for certain types of products such as foodstuffs or pharmaceutical products where damage is likely to occur long after the product has been put into circulation. The Commission already pointed out this problem in its 2000 report on the application of the PLD.⁷⁴

Third, these time limits should be regarded as a **violation of the right of access to justice**. In a decision *Moor v. Switzerland*,⁷⁵ which concerned the rights of Asbestos victims, the European Court of Human Rights held that the application of a ten-year limitation period had deprived the victim of access to a court.

Fourth, BEUC calls for a more sustainable consumption where products have a longer lifespan. This preoccupation is in line with the European Green Deal,⁷⁶ and goes hand-in-hand with the right to have products repaired. Therefore, liability rules must ensure that the time limits in which producers shall be held liable match consumer expectations on long-lasting products. Furthermore, spare parts can also have an impact on product safety, so it is important that in the event of harm stemming from the replacement of parts and components, consumers have a right to recourse against the parts producer.

Ultimately, it is important that the PLD strikes a balance between the need for flexible prescription periods adapted to the dynamic features of digital goods and the need to provide legal certainty for all stakeholders. Moreover, the need for harmonisation is needed to avoid the risk of patchy national legislations that would set different timelines. In 1998, the European Parliament proposed a **20-year period** in case of hidden defects.⁷⁷

BEUC recommendation:

- **The limitation period should be extended to 20 years.**

4. Additional issue: greater transparency for defective products

The PLD does not contain specific provisions to promote transparency. For example, it does not establish a registry that would collect relevant information about product liability cases. Producers are also not obliged to keep a record of claims against them, nor are national authorities required to register cases brought to their attention.

It is essential to encourage transparency and to provide consumers with up-to-date information. If risks exist, or if products have already caused damage, consumers must be informed. There is no excuse not to request greater transparency from companies and authorities.

BEUC recommendation:

- **Introduce concrete measures to enhance transparency and monitor defective products (e.g. creation of a registry with product liability cases).**

⁷⁴ EU Commission, COM (2000) 893 final (p.21).

⁷⁵ ECHR, *Howald Moor and Others v Switzerland*, March 2014, 52067/10 and 41072/11.

⁷⁶ EU Commission, COM (2019) 640 final, 11 December 2019.

⁷⁷ The amendment of the EP read as follows: "if because of a hidden defect the damage does not occur until after the expiry of a period of 10 years, the rights conferred upon the injured person pursuant to this Directive shall not be extinguished until after the expiry of a period of 20 years from the date on which the producer put the product into circulation."

(<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:1998:359:FULL&from=EN>).

Other relevant BEUC publications:

- BEUC position paper '[Making the Digital Services Act work for consumers – BEUC's recommendations](#),' May 2020.
- BEUC position paper '[Keeping consumers secure: How to tackle cybersecurity threats through EU law](#),' November 2019.
- BEUC position paper '[AI Rights for consumers](#),' October 2019.
- BEUC's "Views for a modern regulatory framework on product safety - keeping consumers safe through a revision of the General Product Safety Directive" (*forthcoming*)



This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).

The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.