Council of the European Union

Brussels, 8 February 2023
(OR. en)

6201/23

LIMITE

JUSTCIV 18
JAI 126
CONSOM 35
COMPET 90
MI 92
FREMP 30
CODEC 144
TELECOM 32
CYBER 24
DATAPROTECT 32

Interinstitutional File:
2022/0302(COD)

NOTE

From:	Commission Services
To:	Delegations
Subject:	Commission non-paper on digital elements of the proposal for a new Product Liability Directive

Delegations will find in Annex a Commission non-paper on digital elements of the proposal for a new Product Liability Directive.

———————————

Non-paper on digital elements of the proposal for a new PLD

This non-paper clarifies a number of digital-related elements of the proposal for a new PLD.

1. Relationship between products and components

The PLD provides that the manufacturer is liable for damage caused by a defective product. The current regime refers to the manufacturer of the 'finished product', but given that products today develop after being placed on the market (e.g. through software updates or machine learning), this term no longer seems fit for purpose and was not retained in the proposal. However, as in the 1985 PLD, a manufacturer is liable for the whole product, which itself may be composed of different elements/parts. Since other elements, including new or separate products in their own right, can be added to products outside of the manufacturer's control (e.g. a replacement tyre on a car or a new app on a smartphone), the proposal includes a definition of "component". This ensures that the manufacturer shoulders liability only for items that it has integrated or interconnected with its product or that a third party has integrated or interconnected under the manufacturer's control. Elements added outside the manufacturer's control are not caught by the "component" definition, and therefore the manufacturer cannot be held liable: only the manufacturer of the defective element can be held liable.

2. Inclusion of software

Under the 1985 Directive it is unclear whether a software is a movable, and hence whether it is a product. The proposal maintains the same definition for product, but clearly states now that *'software'* must be understood as a product.

No definition of software is included in the proposal, because this would not be future proof: trying to define what software is, particularly due to its different forms, might accidently limit the application of the regime to future types of software. For instance, software in the 90's would have been defined as 'computer program' and would not have covered today's software, for instance, an operating system, a mobile application on a smartphone or an AI system. Nonetheless the corresponding recital provides examples:

Recital 12

[...] Software, such as **operating systems, firmware, computer programs, applications or AI systems**, *is increasingly common on the market and plays an increasingly important role for product safety. Software is capable of being placed on the market* **as a standalone product and may subsequently be integrated into other products as a component, and is capable of causing damage through its execution**. *In the interest of legal certainty it should therefore be clarified that software is a product for the purposes of applying no-fault liability,* **irrespective of the mode of its supply or usage, and therefore irrespective of whether the software is stored on a device or accessed through cloud technologies**.

Moreover, the recital explains that any software, no matter how it is used or supplied, or how it is integrated or interconnected, is software and therefore a product. This includes software supplied by so-called **"as-a-service"** models. In the same way as other products that are used in the course of a service and might cause damage due to being defective (e.g., defective plane), software used or supplied via a service are also covered.

Not only component software but also standalone software is also covered. For example, medical device software that defectively fails to notify the doctor of a patient's heart attack, causing death; or a navigation app that is defectively designed in that it dangerously distracts the driver, leading to an accident and personal injury[1].

---

[1] https://finance.yahoo.com/news/lyft-sued-defective-app-design-010008447.html; in its first order the court ruled that the transportation application is a product and not a service; https://www.law.com/dailybusinessreview/2022/10/10/lyft-to-face-jury-trial-over-app-flaws-in-precedential-florida-product-liability-ruling.

3. Inclusion of digital manufacturing files

As part of the adaptation of the PLD to the digital age, it was important to answer the long-standing question of whether digital manufacturing files (such as CAD files used to create 3D-printed goods) are products. Since digital manufacturing files are not software as such, but are the digital version of movables, it was necessary to add them explicitly to the definition of "product".

It is considered disproportionate to cover other digital content, such as media files or ebooks, in the definition of "product", because such digital content does not have the capability of causing damage through its execution (see recital 12). Such digital content, however, could be a component under the new definition of "component".

4. (Digital) components and related services

> *(3) 'component' means **any item, whether tangible or intangible, or any related service, that is integrated into, or inter-connected with**, a product by the manufacturer of that product or within that manufacturer's control;*

The definition of 'component' has been included to ensure that the manufacturer of the overall product is liable for any elements integrated within its control. This is particularly relevant for digital products, where digital elements of the product can either be added during the manufacturing process or at a later stage independently by the user.

Member State delegates have drawn parallels with Directives (EU) 2019/771 and 2019/770, which include the term "goods with digital elements". That term is not needed in the PLD, because there can be no doubt that goods are products whether they contain digital elements or not. The definition of "product" sufficiently covers these types of goods.

Furthermore, referring only to the notions of "digital content" and "digital service" comprising the term "digital element" would be insufficient for the purposes of the new PLD. In Directives (EU) 2019/771 and 2019/770, the term "digital content" refers to any "data which are produced and supplied in digital form" and would therefore be already covered by the definition of "component" above, which explicitly refers to both tangible and intangible items.

The term "digital service" covers only "(a) a service that allows the consumer to create, process, store or access data in digital form; or (b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service". A limitation to such specific and consumer-oriented digital services would not have achieved the intended objectives of the new PLD, which is to cover related digital services that can determine the safety of a product (in the same way that other physical or digital components can) while maintaining the general principle that services by themselves do not fall within the scope of the new PLD.

As a result of these considerations, the PLD proposal introduces the term "related service", in line with the logic of the Data Act proposal[2], and its definition of "related service" makes clear that it must be a digital service.

Examples of services that could be related services:

– continuous supply of traffic data in a navigation system (example from recital 14 of Directive (EU) 2019/771);

– continuous supply of AI training data for machine learning abilities of a product;

– temperature control service, a digital service that monitors and regulates the temperature of a product (e.g. a fridge) to ensure its proper functioning and a defectiveness could for example spoil food or beverages;

– voice control assistant service, which allows control of a product by using voice commands. If defective, it could trigger wrong reactions to commands leading to damage;

– a health monitoring service, which relies on sensors of a physical product to track the user's physical activity or health metrics;

– data backup service, e.g. via the cloud. A service that backs up the user's data to prevent loss in the event of a hardware failure.

---

[2]   Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022)68.

Lastly, such related services have to be distinguished from other digital services that might be necessary for the product to function, in particular telecommunications connectivity services. Outages of such services can have an impact on the functioning and the safety of a product, but will normally occur outside the sphere of control of a manufacturer. Therefore, the new PLD introduces the concept of "manufacturer's control" to ensure that failures or outages of such connectivity services would not amount to liability of a manufacturer.[3]

5. Manufacturer's control

The notion of manufacturer's control is relevant for a number of key provisions in the PLD proposal:

To determine if a component is a "component" (Art. 4(3)). If a manufacturer does not itself integrate a component into its product but authorises or influences its integration by a third party, the manufacturer should remain liable for damage caused by the component's defectiveness. If its integration is outside of the manufacturer's control, the component is not a "component" within the meaning of Art. 4(3), but rather a separate product.

–   E.g. if a smart TV is presented as including a video application, but the user is required to download the application from a third party's website after purchase of the TV, the TV manufacturer should still be held liable for damage caused by the video application's defectiveness. If, on the other hand, a user installed an application that was neither authorised nor influenced by the manufacturer, it should not be possible to hold the manufacturer of the smart TV liable.

To determine the relevant moment in time when assessing defectiveness (Art. 6(1)(e)). Under the 1985 PLD, the relevant moment was the moment of placing on the market, since for legacy products this is always the moment at which a product leaves the control of the manufacturer. For today's digital products, this is not the case: manufacturer's retain control, in particular through the ability to provide or authorise updates for digital components.

---

[3]   This does not preclude liability for the defectiveness of the product itself, e.g. if an autonomous car would veer off the street, because it does not have 5G connection anymore, rather than coming to a safe stop, this could likely amount to a defectiveness of the car itself.

To determine if a manufacturer can make use of the later-defect defence in Art. 10(1)(c) and Art. 10(2). This provision is the natural corollary of Art. 6(1)(e). A manufacturer should ordinarily be exempted from liability if its product becomes defective only after the moment it is placed on the market. But this should not be allowed when the product becomes defective due to a related service, software or lack of required software that is within the manufacturer's control. Some examples:

– If a defective navigation service in an autonomous vehicle causes damage, the vehicle manufacturer should not be allowed to use the later-defect defence, because that would render impossible any liability under the PLD for related services (N.B. the notion of manufacturer's control is already embedded in the notion of related service).

– In the smart TV example, if the TV manufacturer provides defective software updates itself or authorises software updates by a video application provider, the manufacturer should not be able to use the later-defect defence.

– If a machinery product injured a user as a result of defectiveness residing in the absence of a software update required to maintain safety, the manufacturer should not be allowed to use the later-defect defence unless such updates are not within its control. Ex ante legislative requirements, such as those in the proposal for a Cyber-Resilience Act, will be relevant for informing the court's decision about whether the product lacked the safety the public at large were entitled to expect.

To determine the relevant moment in time when assessing the objective state of knowledge (Art. 10(1)(e). This provision follows the logic of Art. 6(1)(e) and Art. 10(2). A manufacturer should ordinarily be exempted from liability if, despite the product being defective at the moment it was placed on the market, the objective state of knowledge at that time was such that the defectiveness could not have been discovered. But this should not be allowed if the manufacturer was still able to discover the defectiveness while the product was within its control, meaning that it has the ability to provide updates itself or authorise/influence their provision by a third party.

– E.g. if a self-learning robot injured a user, the fact that the robot's defectiveness (e.g. flawed algorithms) could not have been discovered at the moment of placing on the market should not lead to an exemption of liability so long as the product remains within the manufacturer's control, in particular through the ability to provide updates to address the flawed algorithms.

To determine if an original manufacturer remains liable for the overall product following a substantial modification (Art. 7(4)).

–   E.g. If the original manufacturer of an x-ray machine substantially modifies the machine by fully refurbishing it and makes it available on the market, it is in any event still the manufacturer. If a third-party manufacturer makes the substantial modification without the authorisation/influence of the original manufacturer, the new manufacturer can be held liable (unless the exemption in Art. 10(1)(g) applies). If the original manufacturer authorised the modification, it should remain liable for the substantially modified product.

6. Updates

<u>Who can be held liable?</u> Since software is now defined clearly as a product in the PLD proposal, providers of software updates should also be held liable for damage caused by defective software updates. Where the provision of such updates are within the control of the manufacturer of the overall product (by virtue of providing updates directly, or by authorising or influencing provision by third parties), the manufacturer of the overall product is also liable. This approach recognises that it is in the nature of software to be maintained and improved by updates, without an entirely new product being deemed to have been placed on the market. This approach also avoids any need for the victim to identify whether the hardware, original software or software update is defective – it is enough to say the overall product is defective and the liable economic operators remain unchanged.

If, however, a software update substantially modifies the product, the subsequent software would be considered as a product in its own right. This would also be the case if a software update entirely replaces the underlying software. The original manufacturer or the original software manufacturer would not be liable anymore and liability would fall only on the software provider that has performed the substantial modification and essentially placed new software on the market.

How long can economic operators be held liable? Manufacturers can be held liable under the PLD until 10 years after placing the defective product on the market. For software, as for legacy products, the 10-year period should restart only if it is substantially modified. For example, modifications that change the performance and risk profile of the product: a software module that is capable of changing the movement span of a robot; or software that changes the maximum speed of a motorbike.

_____