


ARTICLE

# The Development Risks Defence in the Digital Age

Guillem Izquierdo Grau 

Department of Private Law, Autonomous University of Barcelona, Cerdanyola del Vallès, Catalonia, Spain and Institute of Law and Technology (IDT), Cerdanyola del Vallès, Catalonia, Spain

Email: [guillem.izquierdo@uab.cat](mailto:guillem.izquierdo@uab.cat)

## Abstract

One of the pillars on which product liability law is based is the defence for development risks. According to this defence, the producer is not liable for the damage caused to the injured party if, at the time the product was put into circulation, the state of scientific and technical knowledge did not allow the existence of the defect to be discovered. The Proposal for a Directive drafted by the European Commission and published on 28 September 2022 continues to provide, in Article 10.1.e), the defence for development risks. The Proposal for a Directive refers to this particular issue in Recital 39, which introduces some requirements for the assessment of such defence.

However, despite this recognition, does this defence fit into the digital paradigm, and how can it be applied to damage caused by defects in products with digital elements that incorporate artificial intelligence?

**Keywords:** artificial intelligence; cyber resilience; cybersecurity; development risks; producer liability; products with digital elements; vulnerabilities

## 1. Introduction

Private law is adapting to the new digital paradigm, and the European Commission has therefore begun the process of revising one of the longest-standing Directives: Council Directive 85/374/EEC of 25 July 1985 on liability for defective products.<sup>1</sup> Given the emergence on the market of products with digital elements and AI systems, it has become apparent that the principles of European product liability law should, if possible, be adapted to the new digital paradigm.

One of the most problematic aspects of the transition to the new digital paradigm is the case of the defence for development risks whereby the producer can exempt itself from liability if it proves that the state of scientific and technical knowledge at the time it placed the product on the market was not such that the defect could be discovered. Such a defence was the legislative reaction to the case of thalidomide, a drug that caused severe foetal malformations in women who took it when pregnant. As they were introduced within the context of the analogue paradigm of forty years ago, I wonder whether development risks should continue to apply in the current day, when goods with digital elements and artificial intelligence are gaining market share.

---

This article is published within the framework of the R&D&I project *Conducción autónoma y seguridad jurídica del transporte/Autonomous Driving and legal certainty of transport*. PI: Eliseo Sierra Noguero.

<sup>1</sup> 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, (1985) OJ L 210.

The Proposal for a Directive<sup>2</sup> that was published on 28 September 2022 merely incorporates the case law of the European Court of Justice on this issue. However, this does not clarify what the scope of application of development risks will be in the current context. Therefore, this paper addresses the regulation of development risks as envisaged in the Proposal for a Directive and consider its effectiveness in light of the risks of digitalisation. To do so, it starts with an analysis of the Proposal for a Directive and, in particular, of the new concept of product that it contains, which includes the software or AI system incorporated into a product. Then, it goes on to analyse the considerations that make it possible to assess the defectiveness of a product, in order to question whether these allow the producer to avail himself of the ground for development risks, in a context where products with digital elements and AI systems have a large presence. This paper starts from the assumption that, if the producer were able to claim the defence from development risks for damage caused by his products with digital elements that incorporate artificial intelligence, the injured party would not be able to claim for damage caused by this type of product. This would offer a way for the manufacturer to avoid liability, meaning that the possibility of applying development risks in this context should be eliminated or interpreted very restrictively. Questioning the applicability of development risks in the digital age, the unpredictability of artificial intelligence, the progressive increase in the autonomy of products and the potential impact of known or unknown vulnerabilities on the product are the main hypotheses.

## II. Scope of the proposal for a directive on product liability

### 1. Concept of product. Consideration of artificial intelligence and software as products.

The main reason why it is necessary to adopt a new directive in this area is the need to adapt the new regulation to the complexity of the products that have burst onto the market: the so-called goods with digital elements that can incorporate AI systems. As regards the specific characteristics of these types of product, it is possible to distinguish between, firstly, tangible movable goods (hardware) and, secondly, digital elements (content and services).<sup>3</sup> Moreover, in the digital era, not all products are tangible, and digital products or services (operating systems, computer programs, applications or AI systems) have been introduced on the market which are not necessarily incorporated within a tangible movable good and which can be downloaded and subsequently incorporated into products outside the producer's sphere of control (Recital 12 Proposal for a Directive).

The problems of fitting products of this type within the definition of product given by the extant Directive 85/374/EEC are well known.<sup>4</sup> This is why the Proposal for a Directive aims to close the doctrinal debate and include software and digital services and content within the scope of application of the future regulation. In this regard, Art. 4.1) of the Proposal for a Directive defines the concept of product as follows: *"all movables even if integrated into another movable or into an immovable. 'Product' includes electricity, digital manufacturing files and software."*

The definition of a product in the Proposal for a Directive is based on the definition contained in Directive 85/374/EEC. The core element of the new definition of product is

<sup>2</sup> European Commission, 'Proposal for a Directive of the European Parliament and of the Council on liability for defective products' COM (2022) 495 final 2022/0302 (COD) (Brussels 2022).

<sup>3</sup> Art 2.1) and 2) Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (hereinafter, DCDS).

<sup>4</sup> Report from the Expert Group on Liability and New Technologies, 'Liability for Artificial Intelligence and Other Emerging Digital Technologies' (2019) 28.

the fact that it may be movable and may be integrated into another movable or immovable product. This first part of the definition in the Proposal for a Directive contains nothing new. However, it then adds two new concepts that did not exist in the definition of product in Directive 85/374/EEC, in addition to electricity: digital manufacturing files or copies (Recital 14 of the Proposal for a Directive), and software.

In my view, the definition of product in the Proposal for a Directive is confusing because, together with movable goods, the definition includes certain types of goods that are intangible. It would have been desirable for the definition to include both movable goods, regardless of whether they incorporate digital elements or not, and the digital elements themselves (digital content and services), highlighting the need for these to be embedded in or interconnected with tangible movable goods, so that without them the product could not perform its functions. Furthermore, in order to build a coherent system aligned with the Directives on non-conformity of goods and digital content and services, i.e. Directives (EU) 2019/770 and 2019/771 (twin directives), I consider that it would be desirable that instead of referring to software, reference be made to digital services, and that these be defined by reference to the provisions of Directive (EU) 2019/770. The use of the same concepts would thus bring coherence to European legislation on contractual and non-contractual liability.<sup>5</sup>

It is also clear from the wording of Recital 12 of the Proposal for a Directive that AI systems or algorithms are considered to be computer programs (software) and, consequently, products. Therefore, the European legislator closes one of the most important debates<sup>6</sup> that existed around Directive 85/374/EEC, which did not make any reference to this issue, and the reform is thus a welcome one. It is clear from Recital 12 of the Proposal for a Directive that the European Commission has in mind software that may initially come integrated in products, or software that is stand-alone and subsequently integrated into the product. In other words, according to Recital 12 of the Proposal for a Directive, what determines whether software and AI systems are included within the scope of the Proposal for a Directive is their integration in or interconnection with products.

Recital 15 of the Proposal for a Directive refers to digital services. It has already been mentioned that the Proposal for a Directive does not provide a definition of digital services and the future Directive should refer to digital content or services by reference to the provisions of Article 2 DCDS. According to the provisions of Recital 15 of the Proposal for a Directive, in the case of digital services, the criterion of integration in or interconnection with tangible products is essential if the provisions of the Proposal for a Directive are to be applied to this type of product. Although Recital 15 of the Proposal for a Directive states that it should not apply to digital services as such, it is necessary to extend its effects to digital services when they are integrated in or interconnected with products in such a way that the product would not be able to perform its functions without them. Therefore, in my opinion, the criterion of the integration or interconnection of software and digital services in products is decisive for the Proposal for a Directive to be applicable to damage caused by intangible products.

## **2. What characterises a product that incorporates artificial intelligence? What risks does it entail?**

Having conceptualised the meaning of product as per the definition given in the Proposal for a Directive, it is now necessary to look at the characteristics of products with AI and their risks.

<sup>5</sup> C Wandehorst, 'Safety and Liability Related Aspects of Software' (2021) 19.

<sup>6</sup> For all, K Chagal-Federkorn, 'Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers' (2019) 30 *Stanford Law & Policy Review* 61.

Products, as they were conceived at the time of the adoption of Directive 85/374/EEC, were subject to the power of the individual, who used them to satisfy his needs according to the reasonable use that could be expected of the product (Art. 6.1.b) Directive 85/374/EEC). If they were equipped with software, even if it was incorporated into the product, it was pre-programmed and executed its functions according to the commands of the individual. In today's context, product software has acquired new functionalities, to the extent that it is capable of making its own decisions without the need for it to act according to a rigid, pre-programmed and unidirectional pattern: "if such a condition is met, then." In response to the circumstances in which the product finds itself and to external stimuli, the product is capable of making its own decisions.<sup>7</sup> This means that a product incorporating artificial intelligence could cause damage to third parties due to its unpredictable behaviour and that it is necessary to determine where the liability for this lies, which the Proposal for a Directive seems to resolve by pointing to the producer if the AI system is within the control of the product manufacturer (Recital 15 and Art 7 of the Proposal for a Directive).<sup>8</sup>

Furthermore, another common feature of products with digital elements and artificial intelligence is their ability to connect to other products or structures, making them possibly vulnerable to hacking by malicious third parties. Therefore, defects in product cybersecurity (Art 6.1.f) Proposal for a Directive) have become very relevant in the digital environment, to the point where the European legislator has been obliged to enact legislation in this field.<sup>9</sup>

### III. Does the ground of the defence for development risks apply to damage caused by products that incorporate artificial intelligence?

#### 1. The defence for development risks

When talking of development risks, these are understood as the risks associated with a product defect that cannot be detected given the state of science and technology at the time the product is released.<sup>10</sup>

Art. 7.e) Directive 85/374/EEC provides the defence for development risks. To understand the scope of this defence, it is necessary to go back to the origin of the institution to see that it was a legislative reaction to limit the liability of manufacturers of pharmaceuticals that caused damage to the body or health of persons.<sup>11</sup> The regulation of

<sup>7</sup> G Wagner, 'Liability Rules for the Digital Age' (2013) 13 Journal of European Tort Law 193. 4. R Abbott, *The Reasonable Robot* (Cambridge University Press 2020).

<sup>8</sup> A Beckers and G Teubner, *Three Liability Regimes for Artificial Intelligence* (Hart London 2022). These authors defend vicarious civil liability for damages caused by defective products incorporating AI systems.

<sup>9</sup> European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020' COM/2022/454 final (Brussels 2022). "(7) Under certain conditions, all products with digital elements integrated in or connected to a larger electronic information system can serve as an attack vector for malicious actors. As a result, even hardware and software considered as less critical can facilitate the initial compromise of a device or network, enabling malicious actors to gain privileged access to a system or move laterally across systems. Manufacturers should therefore ensure that all connectable products with digital elements are designed and developed in accordance with essential requirements laid down in this Regulation."

<sup>10</sup> For all, PS Coderch and JS Feliu, *Brujos y aprendices: los riesgos por desarrollo en la responsabilidad de producto* (Marcial Pons Madrid 1999) 29. Pablo Salvador Coderch & Antoni Rubí Puig, 'Riesgos de desarrollo y evaluación judicial del carácter científico de dictámenes periciales' (2008) 1 Indret 5. Christopher Newdick, 'The Development Risk Defence of the Consumer Protection Act 1987' (1988) 47(3) Cambridge Law Journal 455. Richard E. Byrne, 'Strict Liability and the Scientifically Unknowable Risk' (1974) 4(4) Marquette Law Review 660.

<sup>11</sup> PS Coderch (n 11) 6. Trent D. Stephens & Rock Brynner, *Dark Remedy: The Impact Of Thalidomide And Its Revival As A Vital Medicine* (Perseus, Cambridge, Massachusetts 2001). The effects of the drug thalidomide in Germany are well known. In this country, 4,000 people were born affected by embryopathies related to the ingestion of the drug

development risks can be traced back to the scandal around Thalidomide, which was first marketed in Germany from 1957 onwards as an over-the-counter drug claimed to have calming and anti-inflammatory effects. A German laboratory discovered the molecule and marketed it under the name Contergan without conducting animal or human clinical trials. The drug was prescribed to pregnant women to alleviate nausea during pregnancy. The result was catastrophic: 4,000 babies were born with malformations caused by the effect of the drug during pregnancy.<sup>12</sup>

Prior to the adoption of Directive 85/374/EEC, two proposals for directives were published which dealt with this issue in different ways, reflecting the debate which existed between Member States. The Proposal for a Directive of 9 September 1976 made the manufacturer liable for damage even if the defect could not be detected by the state of scientific or technological knowledge at the time the product was placed on the market.<sup>13</sup> Three years later, the European Parliament proposed to introduce an exception to limit the previous rule by exempting the manufacturer from liability if it could prove that the defect was not detectable at the time the product was placed on the market according to the state of scientific and technological knowledge.<sup>14</sup> The change in the text of the Proposal for a Directive led to tensions between Member States and, in the end, the final version of the draft reinstated the original proposal not to limit manufacturers' liability for development risks. As a result of the tensions between the Member States, the final text of Articles 7(e) and 15(1)(b) of Directive 85/374/EC adopts a solution that satisfies the interests of the Member States:

Art. 7(e) Directive 85/374/EEC: *"The producer shall not be liable as a result of this Directive if he proves:*

*[...]*

*(e) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered;"*

Art 15(1)(b) Directive 85/374/EEC: [Each Member State may] *"by way of derogation from Article 7 (e), maintain or, subject to the procedure set out in paragraph 2 of this Article, provide in this legislation that the producer shall be liable even if he proves that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of a defect to be discovered."*

It can be seen, then, that the ground for development risks has, from the outset, been very controversial and that it was a reaction to the health impacts of defects in medicines which could not be detected, and thus prevented, by the science and technology available at the time the medicines were marketed.

## 2. Treatment of the issue in the proposal for a directive

As mentioned above, on 28 September 2022 the European Commission published a Proposal for a Directive which forms the basis for the debate that will take place in the ordinary legislative procedure and which will culminate in the adoption of a new Directive

by pregnant women. The legislative reaction was the passing of the 1976 Medicines Act, which for the first time provided for liability for development risks.

<sup>12</sup> In a letter sent to *The Lancet*, Dr. WG McBride already warned in 1961 that 20% of babies were born with malformations and hypothesised that these malformations were due to the effect of thalidomide during pregnancy. W. G. McBride, 'Thalidomide and congenital abnormalities' (*The Lancet*, 16 December 1961).

<sup>13</sup> OJEC No. 241 of 14 October 1976. *"Le fabricant est également responsable, même si la chose en fonction du développement scientifique et technologique prévalant au moment où il l'a mise en circulation n'a pu être considérée comme défectueuse."*

<sup>14</sup> OJEC No. 127 of 21 May 1979. *"Le fabricant n'est pas responsable s'il apporte la preuve que la chose ne peut être considérée comme défectueuse en fonction de l'état de développement scientifique et de la technologie prévalant au moment de sa mise en circulation."*

repealing the extant Directive 85/374/EEC. The document explains that during the prior public consultation process most stakeholders expressed their opposition to the deletion of the defence for development risks.<sup>15</sup> This is understandable, given that the future Directive will apply both to damage caused by defective tangible movable property and electricity, which are properly speaking the products falling within the scope of Directive 85/374/EEC, and software or AI systems and digital content, which are considered as products in the Proposal for a Directive.

In the analysis of the Proposal for a Directive, it can be seen that the attention devoted to development risks is rather scarce, although there is an initial reference to them in Recital 39: *“In the interests of a fair apportionment of risks, manufacturers should also be exempted from liability if they prove that the state of scientific and technical knowledge, determined with reference to the most advanced level of objective knowledge accessible and not to the actual knowledge of the manufacturer in question, while the product was within their control was such that the existence of defectiveness could not be discovered.”* This recital therefore incorporates the doctrine laid down by the ECJ in case C-300/95 of 29 May 1997, which stated that the state of scientific and technical knowledge in Art 7.e) of Directive 85/374/EEC should be assessed objectively, regardless of the characteristics of the producer.<sup>16</sup> Furthermore, scientific and technological knowledge must be accessible to the scientific community. Nowadays, scientific and technical knowledge is more accessible due to the existence of highly sophisticated machine translators and artificial intelligence, making it difficult to claim ignorance of scientific and technical knowledge.<sup>17</sup>

Subsequently, the Proposal for a Directive devotes Art. 10 to the regulation of development risks in Art 10.e): *“in the case of a manufacturer, that the objective state of scientific and technical knowledge at the time when the product was placed on the market, put into service or in the period in which the product was within the manufacturer’s control was not such that the defectiveness could be discovered.”* As can be seen, the provision incorporates the ideas expressed in Recital 39 of the Proposal for a Directive. The approach adopted by Art 10.e) of the Proposal for a Directive, regarding the time to be taken into account when assessing the accessibility of scientific and technical knowledge, ie *“the time when the product was placed on the market, put into service or in the period in which the product was within the manufacturer’s control,”* makes it necessary to take into consideration a retrospective view of the moment in question. This need to consider the specific state of scientific and technical knowledge in retrospect also makes it difficult to judge the diligence of the producer in ensuring that a more advanced state of knowledge did not exist.

The main innovation to be highlighted is the disappearance, by virtue of the provisions of Art. 15.1.b) Directive 85/374/EEC, of the ability that Member States had to eliminate the possibility for manufacturers to excuse their liability on the grounds of development risks, something that Spain did with regard to defects in medicines, food and food products intended for human consumption (Art. 140.3 of the Consolidated Text of the General Law for the Defence of Consumer and User Rights [TRLGDCU]), and also France and Germany in relation to blood products and pharmaceutical products. In other words, given the

<sup>15</sup> The public consultation process is available at [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Directiva-sobre-responsabilidad-por-los-danos-causados-por-productos-defectuosos-Adaptacion-de-las-normas-de-responsabilidad-a-la-era-digital-la-economia-circular-y-las-cadenas-de-valor-mundiales\\_es](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Directiva-sobre-responsabilidad-por-los-danos-causados-por-productos-defectuosos-Adaptacion-de-las-normas-de-responsabilidad-a-la-era-digital-la-economia-circular-y-las-cadenas-de-valor-mundiales_es) (consultation held on 12 April 2023).

<sup>16</sup> Case C-300/95 *Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland* (1997) CJEU, para. 29. *“(29 It follows that, in order to have a defence under Article 7(e) of the Directive, the producer of a defective product must prove that the objective state of scientific and technical knowledge, including the most advanced level of such knowledge, at the time when the product in question was put into circulation was not such as to enable the existence of the defect to be discovered.”*

<sup>17</sup> J-S Borghetti, ‘Taking EU Product Liability Law Seriously: How Can the Product Liability Directive Effectively Contribute to Consumer Protection?’ (2023) 1 French Journal of Legal Policy 39.



maximum level of harmonisation of the Proposal for a Directive, there will not be certain product defects that prevent liability from being excused on the grounds of development risks and, therefore, manufacturers will be able to avail themselves of this defence if the conditions for its application are met.<sup>18</sup>

However, in June 2023, as part of the processing of the Proposal for a Directive under the ordinary legislative procedure, the Council published the amendments made to the text approved by the Commission, with particular emphasis on development risks. Specifically, the Council advocates the introduction of a more detailed regulation of this ground for exoneration from liability to satisfy the interests of all the Member States, something which reflects the discrepancies between them on this issue.<sup>19</sup> While the Proposal for a Directive published by the European Commission advocates maintaining the defence for development risks without allowing the Member States to introduce exceptions to its applicability, the Council is now open to introducing exceptions in the legislation transposing the Proposal for a Directive in the Member States.

The Council suggests the regulation of development risks in Art 15 of the Proposal for a Directive by providing, firstly, that even though recognition of the defence for development risks is envisaged in Art 10.1.e) of the Proposal for a Directive, Member States may choose to hold economic operators liable for damage caused by defective products even if the state of scientific and technical knowledge at the time the product was placed on the market, put into service, or during the period it was within their control, did not allow the defect to be discovered. It is, therefore, a rule that preserves a margin of discretion for the Member States, in a similar sense to the regulation contained in the current Art 15.2 Directive 85/374/EEC. In the event that a Member State decides to avail itself of this possibility, according to the second paragraph of Art. 15.1 of the Proposal for a Directive as amended by the Council, the Member States must notify this circumstance to the Commission within 24 months of the adoption of the Directive in order for the Commission to inform the other Member States.

According to Art 15.3 of the version of the Proposal for a Directive as amended by the Council, the possibility of making economic operators liable for development risks must be limited to special categories of products; it must be justified by public interest objectives; and it must be proportionate and suitable for attaining the objective pursued. In my opinion, this provision leads to the same situation as that resulting from Directive 85/374/EEC, whereby the Member States have determined that, for certain categories of products, it is not possible to invoke the defence for development risks, which leads to legislative fragmentation, something that is to be overcome by notifying the Commission and informing the other Member States. As far as artificial intelligence is concerned, this provision in favour of the Member States is essential in order to open the possibility of the Member States preventing economic operators from invoking development risks for damage caused by products that incorporate artificial intelligence. As can be seen, the Council has made no provision in this respect and leaves this matter in the hands of the Member States, so that in practice, if the Council's position is adopted in the final text of the Directive, the result could be unequal treatment as regards the liability of manufacturers for products that incorporate artificial intelligence, since in some

<sup>18</sup> F Rosselli, 'Analysis of the Economic Impact of the Development Risk Clause as provided by Directive 85/374/EEC on Liability for Defective Products' Final Report (2004) 27.

<sup>19</sup> Council of the European Union, 'Proposal for a Directive of the European Parliament and of the Council on liability for defective products - Letter sent to the European Parliament' 2022/0302(COD). The document provides that: "It should therefore be possible for a Member State to introduce new measures, including amending existing ones, extending liability in such situations to specific types of products, if it is deemed necessary, proportionate and justified by public interest objectives, such as those within the meaning of the Treaty on the Functioning of the European Union, namely public policy, public security and public health."

Member States it will be possible to claim the defence for development risks and in others it will not, despite the fact that applying it to artificial intelligence is extremely difficult.

Under the provisions of Art 15.5 of the Proposal for a Directive as amended by the Council, the Commission has the final word in the sense that, once a Member State has notified its willingness to make economic operators of certain categories of products liable for development risks, the Commission must issue a non-binding opinion on the appropriateness of this measure within a maximum period of six months. In the meantime, the Member State must hold the proposed measure in abeyance. The draft text therefore leaves it in the hands of the Commission to harmonise the products for which economic operators cannot be exempted from development risks, as it would be difficult for the Commission to adopt different criteria for the measures proposed by the Member States. In fact, the text proposed by the Council states that the Commission's decision will be made "taking into account any views of other Member States." I believe that the Commission's intervention will ensure uniformity in the transposition of the final text of the Directive, and in particular the effects of the defence for development risks.

In conclusion, therefore, as the text of the Proposal for a Directive currently stands, the wording reminds us of the provisions of Directive 85/374/EEC. However, if the Council's position is adopted, the intervention of the Commission in relation to the measures proposed by the Member States will ensure uniformity in the application of development risks.

### **3. Does it really make sense to talk about development risks in products that incorporate artificial intelligence?**

Prior to the publication of the Proposal for a Directive on 28 September 2022, the European Commission and case law considered the advisability of maintaining or eliminating the defence for development risks in product defects.<sup>20</sup> Finally, the Proposal for a Directive recognises this defence in Art 10.e), with the nuances adopted by the Council to bridge the existing discrepancies between Member States.

However, should the producer really be able to invoke this defence for the risks of digitalisation? So far, there have been contributions from some authors calling for development risks to be interpreted in the light of the new reality, i.e. taking into account the greater ease of access to the most advanced level of scientific and technical knowledge (Recital 39 of the Proposal for a Directive).<sup>21</sup> However, despite these contributions, few authors have given an opinion on the application of the exemption from liability due to the risks of digitalisation, and those that have been put forward have mostly been negative, i.e. they consider that economic operators should be prevented from avoiding their liability by taking advantage of this defence. These authors argue that the development of artificial intelligence and the ability of products to learn by themselves means that products can behave in a totally unpredictable way the moment they are introduced into the market.

<sup>20</sup> According to the explanatory memorandum of the Proposal for a Directive, most consumer and business organisations opposed the removal of this defence. However, legal opinion was more divided. In this sense, Mónica Navarro-Michel, 'Vehículos automatizados y responsabilidad por producto defectuoso' (2020) 5 *Revista de Derecho civil* 215. M<sup>a</sup> Pilar Álvarez Olalla, 'Responsabilidad civil en la circulación de vehículos autónomos' in Esther Monterroso Casado & Alberto Muñoz Villarreal (eds), *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento* (Tirant lo Blanch Valencia 2019) 160. R de Bruin, 'Autonomous Intelligent Cars on the European Intersection of Liability and Privacy Regulatory Challenges and the Road Ahead' (2016)) 7(3) *European Journal of Risk Regulation* 491. 17. Melinda Florida Lohmann, 'Liability Issues Concerning Self-Driving Vehicles' (2016) 7(2) *European Journal of Risk Regulation* 339.

<sup>21</sup> BA Koch et al, 'Response of the European Law Institute. European Commission's Public Consultation on Civil Liability. Adapting Liability Rules to the Digital Age and Artificial Intelligence' (European Law Institute Vienna 2022) 20. Miquel Martín-Casals, 'An approach to some EU initiatives on the regulation of Liability for damage caused by AI-systems' (2022) 2 *Revista Ius et Praxis* 18.



Therefore, when unpredictability is an inherent characteristic of products incorporating artificial intelligence, producers must assume this product risk, and the authors are opposed to the possibility that, should an unpredictable decision be taken by the algorithm, a producer may be covered under development risks for damage caused by these products and artificial intelligence.<sup>22</sup> Therefore, the only possible option that has been considered in the academic literature is whether producers could claim development risks given the unpredictability of the decision taken by the AI system. However, this paper considers whether this claim might be applicable in other circumstances that could lead to the possible exoneration of liability for development risks. For example, could the increase in autonomy (and the consequent damage) of a product once it has been introduced on the market allow the manufacturer to claim development risks? Can the manufacturer be excused from development risks if a third party takes advantage of an unknown vulnerability of a product and, as a result of this tampering, the product causes damage to third parties? These are hypotheses that have not yet been dealt with in the literature and that can be looked at by considering the circumstances that make a product defective.

In the field of autonomous driving, some authors have argued that development risks are key to the harm caused by artificial intelligence: *“Since AV are technological advanced products, the state-of-the-art defence [Art. 7(e)] is expected to play a key role, despite the very high requirements for its establishment. This will have special importance in the case of learning algorithms, which might prove to be inadequate and lead to avoidable accidents. A cost-benefit analysis should be undertaken in which various factors are taken into account, such as the seriousness and the probability of risks, the expected benefits from the use of the product, the cost and feasibility of constructing a safer product; however, regarding personal injuries the risks have to be minimal.”*<sup>23</sup> In my view, the above paragraph demonstrates the difficulties that exist in establishing the difference between the grounds for exemption from liability, in this case development risks, and the defectiveness of the algorithm. The authors relate development risks to the damage caused by algorithms as a result of their inability to prevent accidents, i.e. when they incorrectly execute commands that result in an accident, the probability of risk inherent to the product, etc. I shall therefore look at the circumstances that determine whether a product is defective in the light of the Proposal for a Directive.

#### *a. How should the defectiveness of a product that incorporates artificial intelligence be assessed?*

In order for a producer to be exempt from liability, he must first have placed a product on the market and the product must be found to be defective according to the circumstances of Art. 6 of the Proposal for a Directive. In other words, the defectiveness of the product and consequent occurrence of the damage is a precondition for the producer to be exempt from liability if any of the causes foreseen for this purpose occur.

In order to assess the defectiveness of the product, the Proposal for a Directive adopts the criteria of the “consumer expectation test,” which refers to the product safety that the general public is entitled to expect. However, reasonable expectations are not to be assessed individually with regard to a specific person, rather Art 6 Proposal for a Directive refers to the public at large, which seems to lead to a more objective analysis of product

<sup>22</sup> J-S Borghetti, (n 18) 39. Piotr Machnikowski, ‘Producers’ Liability in the EC Expert Group Report on Liability for AI’ (2020) 2 Journal of European Tort Law 137. European Commission ‘Expert Group on Liability and New Technologies - New Technologies Formation, Liability for Artificial Intelligence and Other Emerging Digital Technologies’ (2019).

<sup>23</sup> M Chatzipanagiotis and G Leloudas, ‘Automated vehicles and third-party liability: A European perspective’ (University of Illinois Journal of Law, Technology & Policy 2020) 127.

defectiveness.<sup>24</sup> In order to interpret this article, Recital 22 of the Proposal for a Directive establishes some guidelines: (1) Consumer expectations refer to the safety of the product expected by the general public; (2) The safety expected of a product by the general public must be measured objectively; and (3) Safety must be judged taking into account the purpose and properties of the product, its objective characteristics and the specific requirements of the group of users. Recital 22 of the Proposal for a Directive then contains a provision which I consider to be extremely relevant and which serves to introduce the following section: “*Some products, such as life-sustaining medical devices, entail an especially high risk of damage to people and therefore give rise to particularly high safety expectations.*” On the basis of such a provision, it could be asked whether the higher the implicit risk of the product is, the higher the expectations of the general public are, to the point of not admitting any error on the part of the algorithm or AI system (expert level). Thus, if the risk implicit in the product is lower, the expectations of the general public should not be so high (medium level).

In my view, in the area of products with digital elements and AI systems, the safety expectations of the general public are particularly high, given the risks to safety and life in general. The criterion adopted by the Proposal for a Directive is therefore not new and, as things stand at present, some suggest the adoption of the “risk-utility test” to determine the defectiveness of the design of an AI system, instead of the consumer expectation test adopted in the Proposal for a Directive. According to this criterion, a product is defective when the harm could have been reduced or avoided with an alternative design at a reasonable cost, thus disregarding the reasonable expectations of users, which may be illusory in the case of AI systems. Applying this criterion to an AI system such as that integrated in an autonomous vehicle, there will be a defect in the system if there is an AI system on the market capable of reducing or avoiding the harm at a lower cost.<sup>25</sup>

If Art. 6 of the Proposal for a Directive is analysed, there are new circumstances for assessing the defectiveness of a product that essentially refer to products with digital elements that incorporate algorithms or AI systems.

#### *b. Cases that could eventually lead to the defence of development risks in the digital age*

- *Ability for self-learning and the unpredictability of artificial intelligence.* First of all, Art 6.c of the Proposal for a Directive refers to the “*effect on the product of any ability to continue to learn after deployment.*” For its part, the Council proposed replace the reference to “*deployment*” for “*it is placed on the market or put into service*”. Focusing, therefore, on the circumstance of Art. 6.c) of the Proposal for a Directive, the first conclusion is that the European legislator has foreseen, as a circumstance revealing the defectiveness of a product, the effect of the self-learning of the AI system.

For a better understanding of how the self-learning capacity of products works, I will give an explanation based on autonomous vehicles. These are made up of two main elements: firstly, the tangible movable good itself and, secondly, the software, which, in turn, consists of AI technology (machine learning) and programming for the execution of rules, tasks and symbol recognition. Furthermore, the AI system integrated in an autonomous vehicle is capable of performing four main functions. Firstly, it observes and analyses its own data (machine learning). Secondly, as a result of prior data analysis, these

<sup>24</sup> G Wagner, (n 8) 204. This author considers that the criterion of reasonable expectations based on the public at large allows for a more abstract assessment of the product and does not rule out the application of the risk-utility criterion.

<sup>25</sup> G Wagner, ‘Robot Liability’ in Horst Eidenmüller & Gerhard Wagner (eds), *Law by Algorithm* (Mohr Siebeck, Tübingen 2021) 86. Gitta Veldt, ‘The New Product Liability Proposal - Fit for the Digital Age or in Need of Shaping Up? An Analysis of the Draft Product Liability Directive’ (2023) 1 *Journal of European Consumer and Market Law* 26. Anna Beckers & Gunther Teubner, (n 9) 86. MA Lemley and B Casey, ‘Remedies for Robots’ (2019) 86(5) *The University of Chicago Law Review* 1383. Ryan Abbott, (n 8) 69.

systems are able to advise the user on the best possible alternative. Thirdly, the system itself can decide between all possible alternatives and, finally, it is able to execute one of them. Therefore, the autonomous vehicle is a product endowed with limited artificial intelligence. The vehicle must make a decision, based on the machine learning it integrates, which evolves with the experience of the vehicle itself and the other autonomous vehicles in the fleet (Art. 6.1.c) Proposal for a Directive).

Due to the fact that the autonomous vehicle's AI system is based on data that is generated while the vehicle is driven and data that has been generated by other vehicles in the fleet with which it is in contact, it is difficult for a producer to invoke the defence for development risks. Faced with a new and critical situation, the autonomous vehicle will make the decision that is most reasonable according to the experience of all autonomous vehicles. Therefore, as the autonomous vehicle's decision is based on a data storage system, the predictability of the vehicle's decision is increased, so that the exemption of the autonomous vehicle manufacturer from liability<sup>26</sup> is not justified. Consequently, the artificial intelligence of the autonomous vehicle leaves little room for unpredictability and, in any case, unpredictability will be limited by the user's experience and by the driving conditions. This makes it more difficult for the autonomous vehicle producer to try to exempt itself from liability on the grounds of the defectiveness of the decision taken by the autonomous vehicle, leaving it liable for the damage caused. This is true for any product. I consider that, although the product can make its own decisions, these decisions will be based on the data available to the product and on the basis of which it acts autonomously. Furthermore, another element limiting the unpredictability of the decision taken by the algorithm is the user's experience and the reasonable and predictable use of the AI-equipped product, as well as its ability to connect to other products with digital elements that can provide it with information on which it bases its decisions. These circumstances therefore limit the unpredictability of the decision taken by the algorithm and limit the unpredictability resulting from the progressive increase in self-learning capability. This means that unpredictability cannot be considered an unknown risk, since even though it is limited, it is an implicit risk in any product that incorporates artificial intelligence.<sup>27</sup>

Likewise, the reasonableness<sup>28</sup> of the decision taken by the autonomous vehicle to avoid dangerous behaviour, based on the algorithm and machine learning, should not be a ground for invoking the protection afforded by development risks. The defence for development risks is based on the impossibility of recognising a defect in a product due to the state of the art of scientific and technical knowledge at a given time, but not on the

<sup>26</sup> S Van Uytsel, 'Different Liability Regimes for Autonomous Vehicles: One Preferable Above the Other?' in Steven Van Uytsel & Danilo Vasconcellos Vargas (eds), *Autonomous Vehicles. Business, Technology and Law* (Springer, Singapore 2021) 77. Hannah Yeefen Lim, *Autonomous Vehicles and the Law* (Edward Elgar Publishing, Singapore) 92. J-S Borghetti et al, 'Relevance of Risk-benefit for Assessing Defectiveness of a Product: A Comparative Study of Thirteen European Legal Systems' (2021) 1 *European Review of Private Law* 91.

<sup>27</sup> GB Spradley, 'Defensive Use of State of the Art Evidence in Strict Products Liability' (1983) 1353 *Minnesota Law Review* 379.

<sup>28</sup> On the reasonableness of the decision taken by an algorithm, K Chagal-Federkorn, 'How Can I Tell If My Algorithm Was Reasonable?' (2021) 213 *Michigan Technology Law Review* 256. The author proposes a method for assessing the reasonableness of the decision made by an algorithm. Firstly, it is necessary to compare the decision taken by the algorithm in the specific circumstances with the decision that would have been taken by a person acting with an average standard of care (Art. 1094 Civil Code). A positive result in the first test is not sufficient to make a positive assessment of the reasonableness of the decision taken by the algorithm. Subsequently, the decision of the algorithm must be compared with the decision that would have been taken by the programmer or the manufacturer of the AI product. Only if the result is positive in both tests can the algorithm's decision be said to be rational. Therefore, even if the autonomous vehicle has caused damage after having observed the circumstances, decided on the best alternative and executed the decision, the decision is not necessarily unreasonable.

reasonableness of the decision taken by a product with artificial intelligence because, as has been explained, its decision is predictable, although not necessarily reasonable.

- *Upgrading, modification and acquisition of new features after the product has been released onto the market.* Another aspect that must be taken into account is that the Proposal for a Directive continues to envisage that a product cannot be considered defective if it is updated or improved after having been placed on the market, provided that the upgrade or enhancement is performed within the scope of the manufacturer's control. Recitals 37 and 38 of the Proposal for a Directive refer to this issue, which is also included in Art 6.2 of the Proposal for a Directive. Therefore, if the autonomous vehicle's software is updated once it has been placed on the market and it is able to improve its functions, the vehicle will not be defective. In other words, it is expected and desirable that the technology will continue to evolve in the future, meaning that, in my opinion, it is extremely difficult for the producer to excuse himself from development risks, given that the product remains under his control and can be updated in the event of new risks presented by digitalisation.

The concept "within the control of the manufacturer" is essential in order to be able to impute liability on the original manufacturer rather than a third party. According to Recital 37 of the Proposal for a Directive, it is considered that *"Such software or related services should be considered within the manufacturer's control where they are supplied by that manufacturer or where that manufacturer authorises them or otherwise influences their supply by a third party."* Therefore, if a third party modifies the product and, as a result, the product causes damage to third parties, liability could be attributed to the person who modified the product, who is considered the manufacturer by virtue of the fact that he modified the product (Art 7.4 Proposal for a Directive), in which case the original manufacturer would be exonerated by the unauthorised intervention of a third party.

Consequently, it is a matter of imputing the damage to the person who has modified the product, rather than claiming exoneration from liability for development risks. In this case, the person who has made the substantial modification to the product can claim the cause of exoneration provided for in Art 10.1.g) Proposal for a Directive, which allows him to impute liability on the original manufacturer if he can prove that the damage is not caused by the modification of the product. On the contrary, if the modification is carried out by the manufacturer himself, who, even after introducing the product on the market, modifies it or introduces improvements while the product is within his control, the product will not be considered defective, and the damage caused after having made the improvement or upgrade cannot be covered by the claim of development risks.

As well as being upgraded and modified after being introduced on the market, the product may have new features as a result of increased autonomy. This would be a qualitative improvement in the product's performance as a result of the development of its AI system. This possibility is introduced by the Council in Art 6.1c) Proposal for a Directive. In my opinion, this scenario is not too different from that envisaged in Art 6.2 Proposal for a Directive, concerning the upgrading of the product once it has been placed on the market. As long as the product remains within the manufacturer's control, the manufacturer is in control of the product, so that a qualitative improvement of the product that gives it new features could be equated to a substantial modification<sup>29</sup> carried out by the manufacturer himself and, therefore, liability arising from the damage could not be imputed to a third party (Recital 29 of the Proposal for a Directive). The Council's

<sup>29</sup> The text revised by the Council introduces a definition of the concept of substantial product modification: *"substantial modification" means a modification of a product after it has been placed on the market or put into service: (a) that is considered substantial under relevant Union or national rules on product safety; or (b) where relevant Union or national rules lay down no threshold on what is to be considered substantial modification, that: (i) changes the product's original performance, purpose or type, without this being foreseen in the manufacturer's initial risk assessment; and (ii) changes the nature of the hazard, creates a new hazard or increases the level of risk".*

review of the Proposal for a Directive makes it clear that: “Where a substantial modification is carried out by the original manufacturer, or within its control, and where such a substantial modification makes the product defective, that manufacturer should not be able to avoid liability by arguing that the defect came into being after it originally placed the product on the market or put it into service. [...] Since products also allow for modifications through changes to software, including upgrades, the same principles of substantial modification should apply.”

Consequently, the key idea that emerges from the Proposal for a Directive is that in the case of any product upgrade, any modification or any substantial modification that results in new features, if these operations are carried out by the manufacturer himself, he remains responsible for the new risks posed by the product and for any damage it may cause to third parties, meaning he cannot subsequently claim development risks.

- *Safety.* In order to determine whether a product is defective in terms of safety, Recital 22 adopts the criterion of the reasonable expectations of the public at large, ie the consumer expectations test. According to this test, when a consumer purchases a product, he expects it to have certain functions, characteristics or properties and, furthermore, he does not expect the purchased product to give rise to other inappropriate or undesirable circumstances. This analysis must be carried out objectively and with the general public in mind, thus disregarding the legitimate expectations of any particular consumer. This is not new, as it is the criterion adopted by Art 6 of Directive 85/374/EEC to determine the defectiveness of a product.

The novelty lies in Recital 24 of the Proposal for a Directive, which makes it compulsory to take into account the safety and cybersecurity requirements of products when analysing the defectiveness of the product, a circumstance that is not expressly included in Art 6 of Directive 85/374/EC. This circumstance for determining the defectiveness of the product appears in Article 6.1.f) of the Proposal for a Directive. According to this provision, compliance with the product’s safety and cybersecurity requirements has a bearing on its consideration as a defective product.

We shall now analyse this circumstance for determining whether a product is defective, in the light of the provisions of the new Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety (GPSR)<sup>30</sup> and the Proposal for a Regulation on Artificial Intelligence.<sup>31</sup>

As things stand at present, reference should first be made to Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, hereafter the GPSD, which was repealed by the GPSR.<sup>32</sup> Article 2(b) GPSD contained the definition of a safe product: “safe product” shall mean any product which, under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product’s use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account the following points in particular:

- (i) *the characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance;*

<sup>30</sup> Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and of the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (2023) OJ L 135.

<sup>31</sup> European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules in the field of artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts’ COM(2021) 206 final. 2021/0106(COD) (Brussels 2021).

<sup>32</sup> Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (2021) OJEC L 11.



- (ii) *the effect on other products, where it is reasonably foreseeable that it will be used with other products;*
- (iii) *the presentation of the product, the labelling, any warnings and instructions for its use and disposal and any other indication or information regarding the product;*
- (iv) *the categories of consumers at risk when using the product, in particular children and the elderly.”*

In view of this definition, there are two concepts for determining that a product is safe. On the one hand, the strict concept of a safe product refers to the fact that the product presents no or only minimal risks. The GPSD contained a definition of “serious risk” which does not clarify what should be understood by risk: *“any serious risk, including those the effects of which are not immediate, requiring rapid intervention by the public authorities.”* However, recently, Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and of the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC,<sup>33</sup> was adopted, which does contain new definitions of the concepts of “safe product,” “risk” and “serious risk”:

- “(2) ‘safe product’ means any product which, under normal or reasonably foreseeable conditions of use, including the actual duration of use, does not present any risk or only the minimum risks compatible with the product’s use, considered acceptable and consistent with a high level of protection of the health and safety of consumers;*
- (4) ‘risk’ means the combination of the probability of an occurrence of a hazard causing harm and the degree of severity of that harm;*
- (5) ‘serious risk’ means a risk which, based on a risk assessment and taking into account the normal and foreseeable use of the product, is considered to require rapid intervention by the market surveillance authorities, including cases where the effects of the risk are not immediate.”*

The new definition of safe product in the GPSR does not introduce major changes compared to the definition of safe product in the GPSD. However, the main changes that do exist are to be found in the definitions of “risk” and “serious risk”. Both concepts hinge on the combination of the probability that a hazard exists or will occur as a consequence of the normal and foreseeable use of the product. Therefore, both the GPSD and the proposed GPSR recognise that non-existent product risk is practically impossible to achieve, and that safety is therefore about tolerating minimal risks.

Furthermore, the broad concept of safe product refers to compliance with minimum requirements for the protection of health and safety. These are general requirements and at a minimum level, in the sense that all products placed on the market must comply with them. Therefore, if a product exceeds the minimum health and safety protection requirements, it can be placed on the market and made available to individuals and consumers.

From all of the above we can draw the conclusion that the fact that a product is safe does not imply that it cannot be defective, either because it has no risk associated with it (a practically impossible assumption) or because, even if it does entail risks, these are

<sup>33</sup> According to the text of the GPSR, the Regulation shall not apply until 13 December 2024 (Art 52 GPSR).



minimal and do not prevent the product from exceeding the minimum requirements for the protection of health and safety and it is then found to be defective once on the market.<sup>34</sup>

The European legislator is aware of the importance that products incorporating AI systems have acquired and how these systems affect product safety in general. However, the GPSR has done away with the idea that products incorporating artificial intelligence do not fall within the scope of the GPSR, which was provided for in the Proposal for a Regulation preceding the GPSR.<sup>35</sup>

The European legislator therefore wishes to regulate product safety in a manner that is horizontal, uniform and coherent (Recital 6 GPSR), although it is envisaged that the safety of certain products shall be governed by sector-specific rules (Art. 2 GPSR). The GPSR does not contain specific provisions for products incorporating artificial intelligence and, therefore, as such products are not excluded from its scope, they should also be understood to be covered. Even so, one cannot overlook the fact that the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,<sup>36</sup> which may have an impact on safety issues for products integrating artificial intelligence, is currently in the process of being finalised.

According to the definition of “artificial intelligence system” included in the Artificial Intelligence Act, this can be defined as “‘AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;” Artificial intelligence can generate a wide range of economic and social benefits, but it can also generate risks and harm certain public interests (Recitals 3 and 4 of the Artificial Intelligence Act). There is a definition of the concept of “risk” in the Artificial Intelligence Act, which is referred to the: “combination of the probability of an occurrence of harm and the severity of that harm.” At no point is there any reference to development risks applicable to artificial intelligence.

The focus of the Artificial Intelligence Act is on high-risk AI systems, which are those that qualify as such under Annex II to the Artificial Intelligence Act and, for these systems, a risk management system will be implemented which will consist of a continuous iterative process to be run throughout the lifecycle of a high-risk AI system and which will identify “known and foreseeable risks” associated with each high-risk AI system, estimate and evaluate the risks that may emerge when the high-risk AI system is used as intended and under conditions of reasonably foreseeable misuse, and evaluate other risks that may arise from the analysis of data gathered through the post-market monitoring system.

<sup>34</sup> CAR Garcia and IM Garcia, ‘Producto inseguro y producto defectuoso. Conceptos de producto peligroso, producto seguro y producto defectuoso en la Directiva 2001/95, el Real Decreto 1801/2003 y la Ley 22/1994’ (2006) 4 Indret 1.

<sup>35</sup> European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council’ COM(2021) 346 final (Brussels 2021).

The Explanatory Memorandum states: “The legislative proposal on artificial intelligence (AI) lays down harmonised rules for the placing on the market, putting into service and use of artificial intelligence systems in the EU. The rules need to ensure a high level of protection of the public interests, in particular on health and safety, and people’s fundamental rights and freedoms. It lays down specific requirements with which high-risk AI systems must comply and imposes obligations on providers and users of such systems.

This proposal takes into consideration these provisions and provides a safety net for products and risks to health and safety of consumers that do not enter into the scope of application of the AI proposal.”

<sup>36</sup> European Parliament & The Council, ‘Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)’ 2021/0106(COD) (Brussels 2024).

The Artificial Intelligence Act therefore measures the risks of AI systems in the present (known risks) and in the future (foreseeable risks and risks that may arise). This fits poorly with the concept of development risks, which looks at the future state of science and technology to assess whether, when a product was introduced on the market, the state of scientific and technical knowledge existing at that time made it possible to detect the product's defect. The same can be said of the understanding of risk in the GPSD and the GPSR.

- *Cybersecurity.* According to Art. 6.1.f) of the Proposal for a Directive, the defectiveness of a product must also be assessed on the basis of compliance with the minimum cybersecurity requirements (Recital 23 of the Proposal for a Directive). In this regard, it is worth highlighting the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements,<sup>37</sup> the so-called Cyber Resilience Act.<sup>38</sup> The recitals of this Proposal for a Regulation refer to the need to improve the functioning of the internal market by establishing essential cybersecurity requirements for placing products with digital elements on the market, so that these products are put into circulation with fewer vulnerabilities and thus increased security (Recitals 1 and 2 Proposal for a Regulation on cybersecurity). Furthermore, the minimum cybersecurity requirements for digital products set out in the Proposal for a Regulation constitute a horizontal regulatory framework applicable to all digital products (Recitals 4 and 6 of the Proposal for a Regulation on cybersecurity). Therefore, the Proposal for a Regulation on cybersecurity has a general scope of application and the applicable sectoral legislation should be taken into account in order to complete the horizontal regulatory framework that it envisages.<sup>39</sup> Indeed, Art 3 of the Proposal for a Regulation on cybersecurity provides that it will not apply to products with digital elements in certain areas, including vehicles.

As regards the cybersecurity risks of digital products, Art 3.36) of the Proposal for a Regulation on cybersecurity contains the definition of “significant cybersecurity risk”: *“a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption.”* Again, the essence of the definition hinges on the more or less high probability that the product with digital elements will suffer an accident leading to material or immaterial damage.

The placing on the market of products with digital elements shall be authorised when these products comply with the essential requirements set out in Annex I of the Proposal for a Regulation, which envisage that products with digital elements shall be designed, developed and produced to ensure an adequate level of cybersecurity in relation to the

<sup>37</sup> European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020’ COM/2022/454 final (Brussels 2022).

<sup>38</sup> For a general approach to the proposal for a Regulation on cyber resilience, Pier Giorgio Chiara, ‘The Cyber Resilience Act: the EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements’, (2022) 3 International Cybersecurity Law Review 255.

<sup>39</sup> In this regard, in the automotive sector, it is worth mentioning Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJEU 325/1 of 16 December 2019). Recital 26 of the Regulation refers to the possibility of unauthorised remote access in the vehicle and of wireless software modification. For this reason, it expresses the need to incorporate UN cybersecurity standards.

risks; be delivered without known vulnerabilities that could be exploited by a malicious third party; be delivered with a secure by default configuration; ensure protection against unauthorised access through appropriate control mechanisms, and protect the confidentiality of personal or other processed data through state-of-the art mechanisms.

As regards AI systems that are classified as high-risk under the Proposal for a Regulation on Artificial Intelligence, Art 8 of the Proposal for a Regulation on cybersecurity states that the essential requirements set out in Annex I are applicable to such systems and, therefore, compliance with these requirements will determine their compliance with the cybersecurity requirements set out in Art 15 of the Proposal for a Regulation on Artificial Intelligence.

As mentioned above, it is Annex I of the Proposal for a Regulation on cybersecurity that sets out the essential cybersecurity requirements for products with digital elements. Without attempting an exhaustive examination of these essential requirements, the provision contained in the second paragraph stands out, according to which: *“products with digital elements shall: (aa) be placed on the market without any known exploitable vulnerabilities.”*<sup>40</sup> The Proposal for a Regulation on cybersecurity does not define what should be understood by “known exploitable vulnerability,” so the future regulation governing this matter should ideally provide a definition of this concept.<sup>41</sup> However, a definition of “vulnerability” is found in Article 3(38), which refers to the definition of “vulnerability” in Article 6(15) of the so-called NIS2 Directive: *“weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat.”*<sup>42</sup> Therefore, that the concept of vulnerability includes the concept of weakness, which refers to the lack of properties that make the product robust against third party intrusions. In conclusion, a product will meet the essential cybersecurity requirements if it is delivered without any known vulnerability that could be exploited. Otherwise, the product will be defective because it does not meet the essential cybersecurity requirements.

At this point, the question that arises is the following: can a vulnerability or defect in the cybersecurity of a product discovered after the product was introduced on the market,

<sup>40</sup> Council of the European Union, ‘Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 - Mandate for negotiations with the European Parliament’ 2022/0272(COD). The Council has amended this paragraph of Annex I of the Proposal for a Regulation to refer to the placing on the market of the product with no known vulnerabilities: *“be placed on the market without any known exploitable vulnerabilities.”* In addition, a new recital (19a) referring to known vulnerabilities has been added: *“Actively exploited vulnerabilities concern instances where a manufacturer establishes that an attempted or successful security breach affecting its users or any other natural or legal persons has resulted from a malicious actor making use of a flaw in one of the products with digital elements placed on the market by the manufacturer.”*

<sup>41</sup> European Commission, ‘Study on the need of Cybersecurity requirements for ICT products - No. 2020-0715. Final Study Report’ (Brussels 2021) 99. The study classifies known vulnerabilities into four groups: (1) cybercrime; (2) attacks by hacktivists; (3) state-sponsored attacks; and (4) insider attacks. Among the target objectives listed under these vulnerabilities are property damage resulting in death or bodily injury to third parties and loss or corruption of data.

<sup>42</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, (2022) OJ L 333. Sandra Schmitz & Stefan Schiffner, ‘Responsible Vulnerability Disclosure under the NIS 2.0 Proposal’ 12 (2021) JIPITEC 447. *“A vulnerability is a set of conditions that allows the violation of a security (or privacy) policy. Such conditions might be created by software flaws, configuration mistakes and other human errors of operators, or unexpected conditions of the environment a system runs in.”* Ian J. GOODFELLOW, Jonathon SHLENS & Christian SZEGEDY, ‘Explaining and Harnessing Adversarial Examples’, in *Proceedings of International Conference on Learning Representations* (2015). Alexey KURAKIN, Ian J. GOODFELLOW & Samy BENGIO, *Proceedings of International Conference on Learning Representations* (Toulon 2017). Ian J. GOODFELLOW, Patrick MCDANIEL & Nicolas PAPERNOT, ‘Making Machine Learning Robust Against Adversarial Inputs’ (2018) 61 Communications of the AC 7, 56. Mobasher BAMSHAD, Robin BURKE & Runa BHAUMIK, ‘Toward Trustworthy Recommender Systems: An Analysis of Attack Models and Algorithm Robustness’ (2007) ACM 7 Transactions on Internet Technology 4, 23.

and the consequent occurrence of damage associated with this vulnerability, exempt the producer from liability for development risks? The considerations set out in the previous points regarding general product safety can be extrapolated to the field of cybersecurity in order to affirm that, even if a product with digital elements meets the essential requirements in terms of cybersecurity, this does not prevent it from being considered defective if it causes damage to third parties after it has been placed on the market. Thus, a product can become defective after it has been placed on the market because of an unknown or actively exploited vulnerability related to lack of cybersecurity, even though its cybersecurity was certified at the time because it complied with the essential cybersecurity requirements. However, given the known vulnerabilities of products with digital elements, it is difficult to think of a vulnerability that could not have been detected or foreseen.

In addition, as regards vulnerabilities, the NIS2 Directive mandates the European Union Agency for Cyber Security (ENISA) to develop and maintain a European vulnerability database.<sup>43</sup> This database should focus on the field of product cybersecurity, in order for manufacturers to identify the essential risks related to the properties of products with digital elements at the time they are introduced on the market and thereafter (Recital 32 Proposal for a Regulation on cybersecurity). In other words, manufacturers must ensure that the essential cybersecurity requirements of their products are met throughout their entire lifecycle.<sup>44</sup> Therefore, to the extent that the product, despite having been placed on the market, remains under the producer's control and considering that producers will have at their disposal the European database developed by ENISA, it prevents producers from exempting themselves from liability by claiming development risks, in this case, for vulnerabilities that were not known at the time they placed the product on the market and that have been detected subsequently.

Recitals 38 and 41 of the Proposal for a Directive deals with the manufacturer's liability for the vulnerabilities of its products. In order to ensure consumer protection, economic operators are prevented from avoiding their liability by proving that a defect occurred after they placed the product on the market or put it into service when the defectiveness of the product consists in the exploitation of a vulnerability by a third party, whether known or unknown. The European legislator's intention is therefore to prevent vulnerabilities in the cybersecurity of a product with digital elements from being used as a pretext for avoiding liability for damage caused. This position can be interpreted in the sense that the manufacturer is liable for product defects deriving from an undiscovered risk (the vulnerability). In other words, it is not the case here of an unknown risk, such as the lesser or greater degree of unpredictability of the AI system as a consequence of its self-learning capacity, but rather that the risk had not been discovered at the time the product was introduced into the market.<sup>45</sup>

<sup>43</sup> Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 - Mandate for negotiations with the European Parliament' 2022/0272(COD). The amended version of the Proposal for a Regulation submitted by the Council imposes on ENISA the duty to produce a biannual report on cybersecurity risks that may affect products with digital elements.

<sup>44</sup> Opinion of the European Economic and Social Committee on the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022) 454 final - 2022/0272 (COD)) (2023/C 100/15). As part of the ordinary legislative procedure, the European Economic and Social Committee has proposed that manufacturers should be required to provide rapid remedies free of charge in the event of new vulnerabilities, should regularly check the "robustness" of the products with digital elements that they place on the market and should eliminate the vulnerabilities detected by means of regular software updates.

Furthermore, Art. 11 of the Proposed Regulation on cyber resilience foresees the obligation for manufacturers to inform ENISA of vulnerabilities that are being actively exploited by third parties without undue delay and in all cases within 24 hours.

<sup>45</sup> GB Spradley, (n 28) 380.

#### IV. Conclusion

Development risks are defined as “those caused by a defect in a product which was not recognisable in the light of the state of scientific and technical knowledge existing at the time the product was placed on the market.”<sup>46</sup> Development risks entail liability for the producer when damage is caused to third parties by defects that were not recognisable at the time the product was placed on the market. Therefore, development risks involve an ex-post judgement whereby the manufacturer will be exempt from liability if he proves that the state of scientific and technical knowledge made it impossible to appreciate the existence of the defect.

The option included in Directive 85/374/EEC and maintained by the Proposal for a Directive that is to repeal it is to impute the damage caused by development risks to the manufacturer, but recognising the possibility for the manufacturer to exempt himself from liability on the grounds of development risks (Art 7.e) Directive 85/374/EEC and Art 10.1.e) of the Proposal for a Directive), despite the fact that Member States are envisaged as having the possibility of preventing the exemption of the producer's liability on this ground (Art 15.1.b) Directive 85/374/EEC). Currently, the Proposal for a Directive published by the Commission on 28 September 2022 continues to provide for the development risks defence, and the main novelty lies in preventing Member States from excluding, in certain cases, that manufacturers can avail themselves of this defence, something that undoubtedly contributes to providing greater legal certainty in European tort law. However, it appears that the final text may change substantially, given the amendments made by the Council, which advocate allowing Member States to maintain, amend or introduce into their national law rules under which manufacturers can be held liable for damage caused by defective products even if the defectiveness of the product could not be detected according to the state of scientific and technical knowledge at the time when they placed the product on the market, put it into service, or it was under their control. This would lead to a situation similar to that currently created by Directive 85/374/EEC. The novelty lies in the duty of the Member States to notify the Commission of the use of this power, whereby the Commission will then inform the other Member States, and in the issuing of a non-binding opinion on the measure, which will affect a special category of products in view of the objectives pursued by the Proposal for a Directive (public security and health). In my opinion, the Commission's intervention is welcome and desirable and will contribute towards harmonising the application of development risks if the amendment is eventually included in the final text.

Traditionally, the scope of application of development risks has been limited to medicines and pharmaceuticals. Cases such as that of thalidomide raised the need to limit producers' liability for development risks. However, this defence was designed for this type of case and, although the Proposal for a Directive still recognises it, it is questionable whether it is suitable in the digital era, where goods with digital elements have burst onto the scene. This paper started from the assumption that such a defence does not fit well with the damage caused by products with digital elements that incorporate AI systems. These products are vulnerable to malicious interference by third parties and that, therefore, the security and cybersecurity of these products is one of the key elements in assessing their defectiveness. However, despite the fact that a product may be considered safe, certified as such and placed on the market due to compliance with the essential safety and cybersecurity requirements, this does not prevent it from subsequently proving to be defective.

If the Directive to be adopted on product liability finally incorporates such a defence, it will have to be reinterpreted in the new context of the digital age, where products with

<sup>46</sup> PS Coderch and J S Feliu, (n 11) 29.

digital elements and AI systems carry risks like all products, but are also vulnerable. In view of the provisions of the Proposal for a Directive (Recital 37), it seems that as long as the product with digital elements is within the manufacturer's control, the manufacturer cannot claim development risks for damage caused by his products due to a defect. Therefore, this leads us to a scenario where development risks may only be claimed when a modification has been made to the product outside the manufacturer's sphere of control and, in this sense, reference must be made to the concept of product vulnerability.

The Proposal for a Regulation on cybersecurity makes it possible to certify a product's cybersecurity if it does not have any known vulnerability that could be exploited by malicious intruders. But in the case of a vulnerability at the time the product is put into circulation that is subsequently detected with the improvement of technology and techniques, and that has caused damage to third parties, should the manufacturer be able to exempt himself from liability by claiming for development risks? This is the key question for development risks in the digital age. In my view, the known vulnerabilities referred to in the Proposal for a Regulation on cybersecurity can be used to reinterpret development risks in the new digital paradigm. However, the provision of a European vulnerability database and the possibility for producers to update their products once they have been put into circulation makes it very difficult to invoke this defence. Likewise, taking into account the provisions of Recital 38 of the Proposal for a Directive, it follows that a vulnerability in a product's cybersecurity cannot lead to a reduction or cancellation of the economic operator's liability.

According to the study conducted on the possible applicability of the development risks in the digital paradigm, I conclude that its application in the development of artificial intelligence, machine learning and cybersecurity is extremely complicated. Therefore, its scope of application will continue to be that of pharmaceuticals, medicines and food. This is the area where, in order to safeguard the fair balance of risks between producers and victims, it must be possible to invoke this defence.<sup>47</sup>

<sup>47</sup> Cour de cassation, civile, Chambre civile 1, 5 May 2021, 19–25.102.