Review scientific paper DOI: 10.56461/iup_rlrc.2026.7.ch21

Maja PROSO*

MANUFACTURER LIABILITY FOR CYBERSECURITY DEFECTS IN DIGITAL PRODUCTS

The proliferation of new digital products on the internal market has evoked the need for a change in product liability rules, with focus on the perils connected with cybersecurity defects of digital products. These vulnerabilities present a significant risk of financial loss, including the potential for digital products to cause damage. The European Union has responded to those risks with a legal overhaul to hold manufacturers accountable for digital product security, centred on two key regulations. The first one is Directive (EU) 2024/2853 on liability for defective products which explicitly expands the definition of the "product" to include software and other digital products, establishing that a product is defective if it fails to meet the required safety level, with cybersecurity requirements becoming an explicit criterion for assessing defectiveness and manufacturer liability. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements, as a complementary act, sets mandatory cybersecurity standards for all digital products across the European Union. A digital product's compliance with Regulation (EU) 2024/2847 will be essential when assessing its safety and whether it is defective under the new Product Liability Directive. The aim of this paper, therefore, is to analyse how the new legal framework impacts the manufacturer's liability for cybersecurity defects in a digital product. The central thesis of this paper is that the manufacturer's legal position under the new regulation framework has evolved into a state of continuous liability for a defective digital product.

***Keywords*:** cybersecurity defects, digital products, defective products, manufacturer liability, EU cybersecurity regulation.

1. INTRODUCTION

Driven by digitalization, the global economy has moved beyond its industrial roots toward a technology-based structure (Zhao, Wallis & Singh, 2015, p. 734). According to the OECD (2019, p. 6), capitalizing on this shift requires coherent, cross-cutting strategies that balance innovation with risk management. The new Directive (EU) 2024/2853 on liability for defective products (hereinafter: PLD) replaces the outdated 1985 legislation (hereinafter: Directive

* Prof. dr. sc., Faculty of Law, University of Split, Croatia, ORCID: https://orcid.org/0009-0004-6055-1493, e-mail: *maja.proso@pravst.hr*

85/374/EEC) to align the legal framework with the challenges of digital transformation, the circular economy, and global markets. The PLD imposes stricter standards and an increased level of liability on economic operators within the European Union (hereinafter: EU). To respond to rapid digital developments, the PLD redefines the notion of the product as well as the notion of defect to be more inclusive. This expansion serves to ensure that the digital elements of contemporary business are covered under the new liability rules. Regulation (EU) 2024/2847 (hereinafter: CRA), simultaneously creates unified European rules for the cybersecurity of digital products. The CRA aligns with the European Union's overarching ambition to foster a Europe fit for the digital age (2019),[1] ensuring that the ongoing digital transformation delivers secure and tangible benefits to both private citizens and the commercial sector (Car & Luca, 2022, p. 2). Effective as of late 2024, with full enforcement beginning in December 2027, the CRA sets rigorous standards for the design and production phases while clearly outlining the manufacturers' legal responsibilities. Manufacturers are, therefore, required to integrate appropriate security measures into their products based on potential risks and, crucially, they must provide regular updates and maintain that security throughout the entire period during which the product is in use (Schoo, 2024, p. 245). Under the new framework, compliance with the CRA serves as the benchmark for product defectiveness under the PLD. Any failure by the manufacturer regarding cybersecurity or software updates that results in harm to the user is now effectively considered a defect, triggering liability and the right to compensation (Chiara, 2025, p. 479). The global WannaCry ransomware attack serves as a landmark example of the catastrophic risks posed by insecure products. By infecting over 200,000 Windows-based devices across 150 nations, this incident showed how cyber vulnerabilities can adversely impact digitally based society (Eckhardt & Kotovskaia, 2023, p. 149). To integrate modern digital devices, the definition of a product in the new PLD has been broadened to encompass both software and its associated services. Furthermore, the traditional, rigid *ex ante* evaluation of product defects, which previously only considered the product's state at the point of sale, has now been relaxed. This shift acknowledges the manufacturer's ongoing responsibility and control over the product through updates and remote management even after it has entered the market (Wagner, 2024, p. 188).

Accordingly, the aim of the paper is to analyse how the new legal framework impacts the manufacturer's liability for cybersecurity defects in a digital product. This article proceeds from the assumption that the manufacturer's legal position under the new regulation has evolved into a state of continuous responsibility for ensuring the safety of digital products. Following the introductory section, the second section critically explores the new rules on manufacturer's liability for defectiveness in digital products under the new PLD. The third section explores manufacturer's legal position under the requirements introduced by the newly enacted CRA mandates. Finally, the conclusion synthesizes the key findings of the conducted research.

2. NEW RULES ON MANUFACTURER'S LIABILITY FOR DEFECTIVE DIGITAL PRODUCTS UNDER THE PLD

The revision of the PLD marks a fundamental shift in how digital harm is addressed, particularly through the classification of software as a product, a move strongly supported

[1] A digital strategy launched in 2019 by the European Union to empower people and businesses with a new generation of technologies, while all the time helping it to achieve its target of a climate-neutral Europe by 2050.

by consumer advocates. Their arguments highlighted the fact that the change ensures that strict liability applies to digital products that cause physical or psychological harm (Micklitz, 2023, pp. 1–13).

2.1. What Constitutes a Product under the PLD

The updated PLD significantly broadens the legal interpretation of what constitutes a product[2] (Li & Faure, 2024, p. 154). The scope of the PLD has recently been extended to all forms of digital content, from software and AI systems to manufacturing files and digital services that are essential for the functionality of connected physical devices (PLD, Article 4(1) and (4), in conjunction with Recitals 12, 13, 15, and 16). By modernizing the definition of a product, the PLD effectively bridges the gap between traditional tangible goods and the complexities of the various digital products. In contrast to conventional physical goods, software, for example, is inherently versatile and has a wide range of functions that defy simple classification. It can manifest either as an embedded component, such as the code powering autonomous vehicle systems, or as a standalone application that functions locally on a device without the need for constant internet access (Li & Schütte, 2023, p. 580). A product is defective if it does not provide the safety which a person is entitled to expect or which is required under Union or national law (PLD, Article 7(1)). Some authors, however, point out the practical challenges of applying the consumer expectation standard regarding product safety (Wagner, 2024, p. 193). When assessing the defectiveness of a product, relevant circumstances that must be taken into account include the presentation of the product and its characteristics (such as its labelling, design, technical specifications, composition and packaging), the instructions for assembly, installation, use and maintenance and the expected and foreseeable use of the product. Relevant factors in assessing defectiveness include, as well, the effect on the product of any ability to continue to learn after its deployment, the interaction with other products (the reasonably foreseeable effect of other products on the product at issue, including the effect of interconnections), the time when the product was placed on the market or put into service or, where the manufacturer retains control over the product, the moment after that time. Other relevant factors include safety regulations and relevant safety requirements, cybersecurity requirements relevant to safety, official interventions (such as product recalls or other relevant actions by competent authorities or economic operators relating to product safety), the specific needs of the group of users for whom the product is intended, and the objective of preventing damage(PLD, Article 7(2)). A product is not considered defective merely because a better product, including updates or upgrades to a product, is already placed on the market or put into service or is subsequently placed on the market or put into service (PLD, Article 7(3)).

2.2. The Circle of Liable Economic Operators under the PLD

According to the updated provisions of the PLD (PLD, Article 8), the liability for defective products is established hierarchically, and the circle of liable economic operators is expanded.

[2] In *VI v KRONE-Verlag* case, the CJEU rejected the idea that inaccurate health advice in a newspaper constitutes a "defective product" under Directive 85/374/EEC. The case concerned a physical newspaper that published inaccurate health advice regarding a herbal treatment, which subsequently caused physical injury to a reader. The CJEU reasoned that the defect must be inherent to the physical characteristics of the product itself (such as the paper or ink) rather than the intellectual content or service provided within it. (*VI v KRONE-Verlag Gesellschaft mbH & Co. KG*, 2021, paras. 34-36).

The goal is to safeguard victims by ensuring they can still receive compensation even if the manufacturer cannot be held accountable. The liability system ensures that the injured party still has a realistic opportunity to obtain compensation (Rimkutė, 2025, p. 81). Economic operators that can be held liable for damage connected to product defectiveness are a manufacturer of a product or component, a provider of a related service, an authorised representative, an importer, a fulfilment service provider or a distributor (PLD, Article 4(15)). Primary liability rests with the manufacturer, which includes not only entities that manufacture physical items but also those who develop software or digital manufacturing files.[3] By redefining the notion of manufacturer to include software developers, the PLD ensures that software developers can be held accountable for digital product defects. If the manufacturer is established outside the EU, liability extends to the importer or the authorised representative, and in certain cases, to the fulfilment service provider. Furthermore, any person who presents itself as a manufacturer by affixing their name or trademark to the product is also considered a liable person, as is any person who carries out a substantial modification to the product outside the original manufacturer's control.[4] Finally, the subsidiary liability of the distributor exists in cases where the original manufacturer or importer cannot be identified. The rules set out in PLD Article 8(3) also apply to online platforms when they help consumers buy from traders, even if the platform itself isn't a traditional commercial business. However, this only applies if the platform meets the specific criteria set out in Regulation 2022/2065.[5] Some authors also point to an unintended consequence of this expansion. For instance, as online platforms become liable for defective goods, rising insurance costs to mitigate these risks could drive up overall prices for products and services (Veldt, 2023, p. 28).

2.3. Burden of Proof and the Obligation to Disclose Evidence

Under the revised PLD, the manufacturer faces liability for damages caused by defects in digital products, including software, AI, and related services. The injured party is not required to prove negligence or fault on the part of the manufacturer, but only the existence of the defect, the damage, and the causal link between them. One of the most debated features of the proposed PLD is the introduction of a rebuttable presumption of defectiveness. According to the views of some, the adoption of probabilistic standards of proof over the traditional requirement for absolute certainty allows the PLD to lower the evidentiary threshold for victims, ensuring that the complexity of modern software does not become a legal barrier to compensation (Koch *et al.*, 2022, pp. 5–14). In contrast, industry representatives warned that such shifts in the burden of proof could inadvertently hamper European digital innovation (The Impact of the Product Liability Directive on Europe's Digital Innovation, 2023). The PLD

[3] According to the definition in PLD, Article 4(10) a manufacturer is any natural or legal person who develops, manufactures or produces a product, has a product designed or manufactured, markets that product under their own name or trademark or develops software or digital manufacturing files.

[4] According to the provision of Article 4(5) PLD a manufacturer maintains control if they execute or authorize the integration of components to the product, software patches, and product modifications. Additionally, it includes any scenario where the manufacturer possesses the capability to deliver software updates, either directly or through a third-party provider.

[5] Specifically, Digital Services Act Article 6(3) clarifies that the exemption from liability does not apply if the online platform presents the interface in a way that leads a consumer to believe the information, product, or service is provided by the platform itself (or by a trader under its authority/control), rather than by a third party.

Article 10 regulates mechanisms that significantly complicate the manufacturer's legal position. Consequently, one of the most debated features of the proposed PLD was the introduction of a rebuttable presumption of defectiveness. Industry representatives often warned that such shifts in the burden of proof could inadvertently hamper European digital innovation (The Impact of the Product Liability Directive on Europe's Digital Innovation, 2023). However, the PLD now stipulates three specific cases where the court is entitled to presume that the product is defective or that a causal link between defectiveness and damage exists. The first case is a situation when the manufacturer fails to comply with a court order for the disclosure of evidence available to them. The court is also entitled to presume that the product is defective or that a causal link exists if the injured party can prove that the product does not comply with mandatory safety requirements (under the EU or national law). The same rule applies when the defectiveness is demonstrated by an obvious malfunction. The PLD Article 10(4) is particularly significant, as it provides that in cases of high technical or scientific complexity, the court may presume defectiveness if the injured party proves it is likely that the product contributed to the damage, or if the injured party faces excessive difficulties in proving the defectiveness of the product or the causal link between its defectiveness and the damage, or both, thereby *de facto* shifting the burden of proof to the contrary onto the manufacturer. The manufacturer's new obligation of disclosure of evidence under the PLD Article 9 is a paradigm shift that places manufacturers in a more demanding legal position than under the old 1985 liability regime. Now, if the claimant shows a plausible case, the manufacturer is obliged to disclose all relevant evidence that is at the manufacturer's disposal. The PLD Article 9(6) specifically empowers courts to demand that all evidence be presented in an easily accessible and understandable manner. This could force the manufacturer to use their own resources to simplify and explain the evidence against them. If a manufacturer refuses to disclose a document, it triggers the aforementioned presumption of the product's defectiveness, in accordance with the provision of the PLD Article 10(2)(a). Consequently, manufacturers may now face substantial legal and administrative expenses due to the obligation to present evidence transparently. The new PLD still provides for specific exoneration grounds in which an economic operator (manufacturer included) is exempted from liability. According to the PLD Article 11, manufacturers and other liable economic operators can be exempt from liability if they successfully substantiate specific defensive grounds. Under Article 11(1), manufacturers or importers are exempt if they prove they did not place the product on the market (point a), or if distributors did not make the product available (point b). The same applies if the operator demonstrates that the defect likely did not exist at the time of distribution (point c), resulted from adherence to mandatory legal regulations (point d), or if the scientific and technical knowledge at the time made the defect undiscoverable (point e). Additionally, component manufacturers are protected if the defect stems from the final product's design (point f), while those who modify a product are not held responsible if the damage was caused by a part they didn't change (point g). Crucially, Article 11(2) of the PDL narrows these protections for the digital products. It stipulates that if the defect of the product occurs after its distribution, but still involves elements under the manufacturer's control, the manufacturer will not be exempt. This specifically includes defects linked to related services (point a), software updates or upgrades (point b), or a failure to deliver safety-critical updates (point c). Furthermore, this exemption is revoked if the defect arises from a substantial modification of the product (point d), effectively requiring manufacturers to remain accountable throughout the product's digital and operational life cycle.

2.4. The Development Risk Defence

Ever since the development risk defence was introduced (ex-Art. 7(e) Directive 85/374/EEC, now Article 11(1)-point e PLD), it has been a hot topic of debate (Hacker, 2022, p. 28). Essentially, the development risk defence means it would be unjust to punish an operator for legal compliance or for failing to address defects that were undetectable and beyond their control (Howells, 2007, p. 403). This suggests that the timeframe for evaluating digital products is not strictly limited to the point at which they are first introduced to the market. One of the most significant challenges in adapting product liability rules to the digital age concerns the development risk defence. This legal provision exempts producers from liability if they can demonstrate that the defect was undiscoverable in light of the scientific and technical knowledge available at the time the product was released. The development risk defence was established forty years ago (Izquierdo Grau, 2025, p. 197). The Court of Justice of the European Union (hereinafter: CJEU) clarified in its ruling that the "state of knowledge" required for the development risk defence to be effective should be measured by an objective standard, meaning what matters is whether the relevant information was objectively accessible at the relevant time (Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland, 1997, para. 29). Proponents of the development risk defence argued that it was an essential element in providing incentives for the development of high-tech and innovative products and reducing insurance costs, while opponents claimed that the defence would diminish the impact of Directive 85/374/EEC (Fairgrieve & Goldberg, 2020, pp. 479–480). The PLD in Recital 39 maintains the CJEU view on the objective standard of accessible scientific and technical knowledge, mandating that in order to ensure an equitable distribution of risk, manufacturers may be granted an exemption from liability if they can demonstrate that a product's defect was impossible to identify while under their control. Crucially, this defence is not based on what the specific manufacturer actually knew, but rather on the highest standard of objective, accessible scientific and technical knowledge available. Under the new PLD, Article 18, Member States are permitted to maintain or establish national laws that hold economic operators liable for defective products even when the defect was scientifically or technically undiscoverable at the time of release. To maintain existing liability rules, Member States must submit the relevant legal texts to the Commission by December 9, 2026. Furthermore, Member States may introduce new or amended measures of this type, provided they are restricted to specific product categories, motivated by clear public interest objectives, and remain proportionate to those goals. Any proposed new measures must be submitted to the Commission with a detailed justification; following notification, the Member State must observe a six-month period allowing the Commission to issue an opinion and other Member States to provide observations before the measure can be officially adopted. It is evident that, just as in the former PLD 1985, the legislator has chosen not to fully harmonize this aspect, leaving it to each Member State's discretion. The Republic of Croatia has incorporated the development risk defence into its legislation, meaning that manufacturers in Croatia can be exempted from liability if they prove that the defect could not have been foreseen given the scientific and technical knowledge at the time.[6] This

[6] The provision of Art. 7, point (e) has been fully transposed into Art. 1078, para. 1, subpara. 5 of the Civil Obligations Act, *Official Gazette* No. 35/2005, 41/2008, 125/2011, 78/2015, 29/2018, 126/2021, 114/2022, 156/2022, 145/2023, 155/2023.

means that the development risk defence in Croatia currently applies to all product categories, including medicines and food. The burden of proof rests solely on the manufacturer. Given that the new PLD requires transposition by December 2026, the Minister of Justice, Public Administration, and Digital Transformation of the Republic of Croatia presented proposed amendments to the Civil Obligations Act in January 2026. The development risk defence is specifically contained in amended Article 1078 (1) point 5, which stipulates that an economic operator shall be exempt from liability if they prove that the objective state of scientific and technical knowledge at the time the product was placed on the market or put into service, or during the period in which the product was under the manufacturer's control, did not allow the defect to be discovered. This means that Croatia has chosen to keep the development risk defence, yet there is an important change connected with the digital nature of products. The defence now covers the time the product was placed on the market "or during the period in which the product was under the manufacturer's control." The provision, therefore, significantly extends the manufacturer's liability period to include the duration of time a product remains under manufacturer's control, such as, for example, through ongoing software updates for smart devices.

The PLD significantly reshapes the regulation of digital products by making the cybersecurity aspects of products with digital elements a component of product safety,[7] as defined in Article 3(1) CRA, a central liability factor for economic operators.[8] As digital transformation advances exponentially, the protection of data and digital infrastructure has become a priority. In this sense, while digital advancements have brought many previously unknown vulnerabilities, they have also served as the primary impetus for modernization of cybersecurity frameworks (Bouhafs, 2025, p. 122). Some authors, however, point out that the new PLD unjustifiably excludes commercial property from the scope of recoverable damages, as well as the ambiguities surrounding the status of open-source software and the practical challenges of applying the consumer expectation standard regarding product safety (Wagner, 2024, pp. 181–193).

3. MANUFACTURER'S LIABILITY UNDER THE CRA

The CRA, as previously stated, aims to support the cybersecurity of digital products. The CRA establishes clear rules for placing digital products safely on the market, mandating essential standards for their design, development, and production, as well as obligations of manufacturers and other economic operators. Its provisions apply to any device or software connected to

[7] The General Product Safety Regulation, 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 the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC OJ L 135, 23.5.2023 (hereinafter: GPSR) acts as a regulatory backstop for any risks that the Cyber Resilience Act (CRA) doesn't specifically cover. While the CRA focuses strictly on protecting digital products from hackers and data breaches, the GPSR remains in charge of general safety issues unless a more specific EU law already applies.

[8] Under CRA, Article 3(12): Economic operator is the manufacturer, the authorised representative, the importer, the distributor, or other natural or legal person who is subject to obligations in relation to the manufacture of products with digital elements or to the making available of products with digital elements on the market in accordance with CRA.

other devices or networks, but it excludes open-source software and products already covered by specific regulations, such as medical devices, motor vehicles, and aviation systems.[9] Because they oversee the initial conception, design, and development phases, manufacturers are typically best positioned to ensure a product's security from its inception (Zirnstein, 2022, p. 710). The path to the final version of the CRA was defined by intense negotiations between the European Parliament, the Council, and stakeholders.[10] A primary point of contention centred on the broad definition of a product,[11] specifically regarding its impact on Open-Source Software and the broader implications for technological development and internet freedom (Colonna, 2025, p. 10). Under Article 3(13) of the CRA, a manufacturer is defined as the entity whose name or logo appears on a digital product. Whether they developed the software themselves or outsourced the development, and whether they charge for the software or give it away, they remain the primary party responsible for cybersecurity compliance. Manufacturers are strictly mandated to address all vulnerability management protocols and ensure their products are distributed free of known exploitable flaws. However, for other essential requirements, the CRA grants manufacturers a degree of autonomy, allowing them to assess and determine which specific standards are applicable based on the unique nature and category of their product (Burri & Zihlmann, 2023, p. 30).

3.1. Mandatory Cybersecurity Standards

The CRA mandates that manufacturers take full lifecycle responsibility for the cybersecurity of products with digital elements. This begins with security by design, requiring a documented risk assessment that informs the entire development process and accounts for third-party or open-source components through rigorous due diligence. The concept of

[9] Under Article 2(2) CRA, several categories of products are explicitly excluded from its scope because they are already governed by *lex specialis*. These include medical devices under Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117, 5.5.2017 and Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, motor vehicles covered by Regulation (EU) 2019/2144, OJ L 117, 5.5.2017, civil aviation systems under Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91, OJ L 212, 22.8.2018, and marine equipment regulated by Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC, OJ L 257, 28.8.2014. Recitals 25, 26, and 27 CRA further clarify the reasoning behind these aforementioned exemptions, emphasizing that such sectoral legislation already ensures an equivalent or even higher level of protection, making the application of the CRA to these specific industries unnecessary to avoid regulatory overlap.

[10] For more on this see: European Parliamentary Research Service (EPRS), 2023; Eclipse Foundation, 2023; GitHub, 2023.

[11] The CRA extensive reach has sparked extensive debate. While some welcome its breadth, critics argue that the resulting regulatory burden creates prohibitive compliance costs that could stifle the competitiveness of SMEs. Industry groups like DigitalEurope, and ETNO GSMA supported the CRA extensive reach and unified security standards. See: Committee for European Construction Equipment, 2023; American Chamber of Commerce to the EU, 2023; European Cyber Security Organisation, 2022; DigitalEurope, 2023.

security by design is not a recent innovation in the cybersecurity landscape; rather, it is rooted in long-standing computer engineering principles. Over time, this framework has been increasingly championed as a primary strategy for neutralizing the unique security vulnerabilities inherent in the expanding Internet of Things (IoT) ecosystem (Bygrave, 2021, p. 126). Before being placed on the market, products must undergo a conformity assessment and receive CE marking.[12] Manufacturers are further obligated to provide a support period, generally a minimum of five years, during which they must effectively handle vulnerabilities, provide free security patches, and maintain a single point of contact for reporting flaws. Documentation, including the EU declaration of conformity and technical files, must be kept for at least 10 years or the duration of the support period. Finally, if a product is found to be non-compliant, the manufacturer must immediately take corrective action, such as issuing updates, withdrawing the product, or notifying authorities and users of a termination of operations (Article 13 CRA). Under Article 14 CRA, manufacturers must adhere to strict timelines for reporting actively exploited vulnerabilities and severe security incidents to ENISA[13] and the relevant national authorities via a centralized platform. Furthermore, manufacturers are legally required to inform impacted users about risks and corrective actions in an accessible format. If they fail to do so, authorities may intervene to alert the public. Article 15 CRA allows manufacturers and third parties to voluntarily report vulnerabilities, cyber threats and security incidents to ENISA or national authorities. If a third party reports a flaw, the authorities must inform the manufacturer immediately to ensure that the issue can be addressed promptly.

3.2. Evaluating Manufacturers' Obligations and the Implementation Gap

Furthermore, to meet the requirements of Article 31 and Annex VII CRA, manufacturers must prepare thorough technical documentation before launching a product and keep the documentation updated as long as the product is supported. The documentation must remain accessible to regulatory authorities upon request (Teichmann, 2026, p. 4). The technical documentation must include a clear description of the product's purpose and software versions, as well as a detailed look at its internal architecture and development processes. Under Article 13 CRA, a manufacturer must provide a risk assessment and records of any security standards or tests which were used to ensure the product is safe for the market. Under Article 18 CRA, a manufacturer can appoint an authorised representative in order to handle specific compliance tasks. While this representative cannot take over the manufacturer's core design or development duties (as outlined in Article 13), they act as a local point of contact for

[12] Under CRA, Article 3(31) The CE marking serves as a manufacturer's official declaration that both their digital product and their internal development processes meet the mandatory cybersecurity standards defined in Annex I of the CRA, as well as any other relevant EU safety laws. Essentially, it is a visible guarantee that the product complies with all applicable European "harmonization" rules before it is sold.

[13] The European Union Agency for Cybersecurity (ENISA) is the European Union's centre of expertise for digital security, tasked with achieving a high common level of cybersecurity, as regulated by Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019. Headquartered in Greece, ENISA supports Member States and EU bodies by providing technical advice, coordinating large-scale crisis responses, and developing the European cybersecurity certification frameworks mandated by the CRA Under the CRA, ENISA manages the platform for reporting vulnerabilities and incidents. Available at https://www.enisa.europa.eu/ (19. 2. 2026).

authorities. Their primary responsibilities include keeping the EU declaration of conformity and technical documentation available for at least 10 years (or the duration of the product's support period), providing proof of compliance upon request, and cooperation to resolve any security risks associated with the product. Under Article 21 CRA, an importer or distributor is considered the manufacturer if they sell a digital product under their own name or brand, or if they make a substantial modification to a product that is already placed on the market. In these cases, they have the same level of responsibility as the manufacturer. It should be emphasized that any individual or company that makes a substantial modification to a digital product and then puts it back on the market is regarded as a manufacturer. This means they also must comply with all security and documentation obligations of the manufacturer. These obligations apply specifically to the modified parts of the product. However, if the change affects the security of the entire product, the subject who made the modification becomes responsible for the compliance of the whole product (Article 22 CRA). These obligations are designed to ensure user security while assuring that products remain operational and receive necessary support throughout their entire lifecycle (Collona, 2025, p. 9). While the CRA sets out a broad set of cybersecurity requirements and obligations for the manufacturer, the analysis of its provisions shows the CRA lacks precise practical guidance, leaving its requirements difficult for manufacturers to translate into practice. This suggests that manufacturers might struggle with inconsistent regulatory interpretations of adequate security levels across the EU, leading to legal uncertainty. Such an implementation gap complicates the development and maintenance of products that meet the regulation's standards. In our view, this ambiguity represents a significant hurdle because without concrete frameworks, compliance remains largely speculative, an argument already expressed by industry experts who argue that legislative intent cannot succeed without technical clarity (Schoo, 2024, pp. 245–251). Moreover, we find that the CRA may unintentionally benefit big tech companies with vast compliance budgets at the expense of small businesses because the cost of certification and compliance can be disproportionately high.

4. CONCLUSION

It is widely accepted that establishing a transparent and robust liability framework for digital products would significantly enhance the overall security and resilience of global cyberspace (González Fuster & Jasmontaite, 2020, p. 110). As discussed above, the notion of cybersecurity has evolved significantly, moving beyond a purely technical understanding of IT security to become a complex social, economic, and multidisciplinary challenge. Cyberattacks today can violate fundamental human rights, compromising physical safety, causing disruptions and severe financial loss in businesses and the broader community (Chaira, 2022, p. 271). Because digital products function through continuous interaction with third-party data and numerous interconnected participants, traditional liability frameworks are no longer sufficient. Liability rules have therefore been modified to impose a broader duty of care on manufacturers, ensuring they remain liable for damages even when harms arise from the complex digital nature of the product (Koch, 2020, p. 120).

The conducted research demonstrated that the manufacturers' legal position under the new defective digital product legislation in the European Union is defined by a synergy between the provisions of the CRA and the PLD that have created a challenging legal environment for the

manufacturer. This synergy resulted, in our assessment, in a regime of continuous manufacturer liability throughout the product's whole lifecycle. Traditional manufacturer liability often ended when a product left the factory. For digital products, liability now extends throughout the period the manufacturer retains control, such as through the ability to push software updates or mandatory cybersecurity requirements, including security by design. In other words, the manufacturer's liability now encompasses a substantially longer duration, reflecting the product's extended expected security lifecycle. While the CRA imposes administrative mandates and security by design requirements onto manufacturer, in order to prevent unsafe digital products on the internal market, the PLD ensures that manufacturers are held liable if a defective digital product causes damage. Crucially, the two documents, as the conducted analysis has shown, are linked through the new definition of a defect. The CRA creates the benchmark for product safety expectation, meaning that if a manufacturer fails to comply with the CRA's essential requirements that failure can be used in court as evidence that the product was legally defective. A manufacturer's failure to meet CRA obligations does not result only in administrative fines but makes the manufacturer's legal position in the case of a cybersecurity breach quite difficult. In the context of the new regulatory framework of digital products in the European Union, the development risk defence allows manufacturers to avoid liability if they can prove that the state of scientific and technical knowledge at the time they put the product on the market was not advanced enough to discover the defect. However, the new framework significantly narrows this defence. Even though the PLD maintains the development risk defence, its application is now conditioned upon the manufacturer's rigorous adherence to the CRA's security by design mandates. Despite noted deficiencies, we expect this regulatory framework to catalyse innovation and trigger a judicial redefinition of liability for cybersecurity defects.

LIST OF REFERENCES

A Europe fit for the digital age: Empowering people with a new generation of technologies. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en (18. 2. 2026)

Bouhafs, H. 2025. Cybersecurity in the Digital Era: Between Digital Transformation and Protection Challenges. *Law and World*, 11(35), pp. 111–125. https://doi.org/10.36475/11.3.8

Burri, M. & Zihlmann, Z. 2023. The EU Cyber Resilience Act – An Appraisal and Contextualization. *Zeitschrift für Europarecht (EuZ)*, 2, B1-B45. Available at: https://ssrn.com/abstract=4375552 (18. 2. 2026). https://doi.org/10.36862/eiz-euz015

Bygrave, A. L. 2021. Security by Design: Aspirations and Realities in a Regulatory Context. *Oslo Law Review*, 8(3), pp. 126–177. https://doi.org/10.18261/olr.8.3.2

Car, P. & Luca, S. 2022. *EU Cyber Resilience Act: Briefing.* Luxembourg: European Parliament. Available at: https://www.europarl.europa.eu/thinktank/hr/document/EPRS_BRI(2022)739259.

Chiara, P. G. 2022. The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *International Cybersecurity Law Review*, pp. 255–272. https://doi.org/10.1365/s43439-022-00067-6

Chiara, P. G. 2025. Understanding the regulatory approach of the Cyber Resilience Act: protection of fundamental rights in disguise? *European Journal of Risk Regulation*, 16 (2), pp. 469–484. https://doi.org/10.1017/err.2025.9

Colonna, L. 2025. The end of open source? Regulating open source under the cyber resilience Act and the new product liability directive. *Computer Law & Security Review*, 56, 106105. https://doi.org/10.1016/j.clsr.2024.106105

Eckhardt, P. & Kotovskaia, A. 2023. The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review,* 4, pp. 147–164. https://doi.org/10.1365/s43439-023-00084-z

Fairgrieve, D. & Goldberg, R. S. 2020. *Product Liability*. 3rd ed. Oxford: Oxford University Press.

González Fuster, G. & Jasmontaite, L. 2020. Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In: Christen, M. Gordijn, B. & Loi, M. (eds.), *The Ethics of Cybersecurity*. Berlin: Springer Open, pp. 97–115. https://doi.org/10.1007/978-3-030-29053-5_5

Hacker, P. 2022. The European AI liability directives – Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, 51, 105871. https://doi.org/10.1016/j.clsr.2023.105871

Howells, G. (ed.). 2007. *Law of Product Liability*. 2nd ed. London: LexisNexis Butterworths.

Izquierdo Grau, G. 2025. The Development Risks Defence in the Digital Age. *European Journal of Risk Regulation*, 16(1), pp. 197–216. https://doi.org/10.1017/err.2024.43

Koch, B. A. 2020. Liability for Emerging Digital Technologies: An Overview. *Journal of European Tort Law*, 11(2), pp. 115–136. https://doi.org/10.1515/jetl-2020-0137

Koch, B. A. *et al*. 2022. Response of the European Law Institute to the Public Consultation on Civil Liability – Adapting Liability Rules to the Digital Age and Artificial Intelligence. *Journal of European Tort Law*, 13(1), pp. 25–63, https://doi.org/10.1515/jetl-2022-0002

Li, S. & Faure, M. 2024. The Revised Product Liability Directive: A Law and Economics Analysis. *Journal of European Tort Law*, 15(2), pp. 140–171. https://doi.org/10.1515/jetl-2024-0010

Li, S. & Schütte, B. 2023. The proposal for a revised Product Liability Directive: The emperor's new clothes? *Maastricht Journal of European and Comparative Law*, 30(5), pp. 573–596. https://doi.org/10.1177/1023263X231216941

Micklitz, H.W. 2023. *The Role of Standards in Future EU Digital Policy Legislation*: *A Consumer Perspective, Executive Summary.* Brussels: BEUC. Available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-152_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation-Exec_Summary.pdf

Organization for Economic Co-operation and Development (OECD). 2019. *Going Digital: shaping policies, improving lives*. Paris: OECD Publishing. Available at: https://www.oecd.org/en/publications/going-digital-shaping-policies-improving-lives_9789264312012-en.html

Rimkutė, D. 2025. The New EU Product Liability Directive: Doctrinal Analysis. *Access to Justice in Eastern Europe*, 8 (Spec.), pp. 74–97. https://doi.org/10.33327/AJEE-18-8.S-c000160

Schoo, P. 2024. Navigating the CRA: A Brief Analysis of European Cyber Resilience Act and Resulting Actions for Product Development. *Proceedings of the 9th International Conference on Data of Things, Big Data and Security*, pp. 245–251. https://doi.org/10.5220/0012690500003705

Teichmann, F. 2026. The cyber resilience act as a new paradigm for product security: a compliance roadmap. *International Cybersecurity Law Review*, 7, pp. 1–17. https://doi.org/10.1365/s43439-025-00162-4

The Impact of the Product Liability Directive on Europe's Digital Innovation – Creating a Proportionate Product Liability Directive, Brussels: DigitalEurope, 2023, pp. 1–10. Available at: https://cdn.digitaleurope.org/uploads/2023/03/DIGITALEUROPE-PLD-position-March-2023.pdf

Zhao, F., Wallis, J. & Singh, M. 2015. E-government development and the digital economy: A reciprocal relationship. *Internet Research*, 25(5), pp. 734–766. https://doi.org/10.1108/IntR-02-2014-0055

Zirnstein, Y. 2022. Der Entwurf des Cyber Resilience Act. *Computer und Recht,* 38(11), pp. 707–714. https://doi.org/10.9785/cr-2022-381108

Veldt, G. 2023. The New Product Liability Proposal – Fit for the Digital Age or in Need of Shaping Up? *Journal of European Consumer and Market Law*, 24, pp. 24–31.

Wagner, G. 2024. Next Generation EU Product Liability – For Digital and Other Products. *Journal of European Tort Law*, 15(2), pp. 172–224. https://doi.org/10.1515/jetl-2024-0011

Internet sources

American Chamber of Commerce to the EU (AmCham EU). 2023. *Our position, Cyber Resilience Act proposal*. Available at: https://www.amchameu.eu/system/files/position_papers/cyber_resilience_act_proposal_final.pdf (18. 2. 2026).

Committee for European Construction Equipment (CECE). 2023. *CECE issues a position paper on the Cyber Resilience Act*. Available at: https://www.cece.eu/news/cece-issues-a-position-paper-on-the-cyber-resilience-act (18. 2. 2026).

DigitalEurope. 2023. *Cybersecurity everywhere: deciphering the Cyber Resilience Act*. Available at: https://www.digitaleurope.org/ (18. 2. 2026).

Eclipse Foundation. 2023. *Open Letter to the European Parliament: Potential Impacts of the Cyber Resilience Act on the Open-Source Ecosystem*. Available at: https://www.eclipse.org/ (18. 2. 2026).

ETNO-GSMA. 2023. *ETNO-GSMA joint position paper on the Cyber Resilience Act*. Available at: https://www.gsma.com/gsmaeurope/wp-content/uploads/2023/03/ETNO-GSMA-joint-CRA-position (18. 2. 2026).

European Cyber Security Organisation (ECSO). 2022. *Position Paper, Cyber Resilience Act*. Available at: https://ecs-org.eu/ecso-uploads/2023/01/ECSO_position_on_the_CRA.02.pdf (18. 2. 2026).

European Parliamentary Research Service (EPRS). 2023. *Briefing: Cyber Resilience Act – Strengthening the Security of Hardware and Software*. Luxembourg: European Parliament.

GitHub. 2023. *Policy Brief: Navigating the Cyber Resilience Act for Open-Source Communities*. Available at: https://github.blog/ (18. 2. 2026).

Legal sources and case law

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, (2024) OJ L, 2024/2853.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, OJ L 277, 27.10.2022 (Digital Services Act)

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), (2024) OJ L, 2024/2847.

CJEU, C-300/95, *Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland*, ECLI:EU:C:1997:255

The General Product Safety Regulation, 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 the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC OJ L 135, 23.5.2023.

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.

Judgment of 10 June 2021, C-65/20, *VI v KRONE-Verlag Gesellschaft mbH & Co. KG*, ECLI:EU:C:2021:471