


ARTICLE

Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?

Pier Giorgio Chiara 

Department of Law and ALMA-AI Research Centre, University of Bologna, Bologna, Italy
Email: piergiorgio.chiara2@unibo.it

Abstract

The swift proliferation of connected devices in the Internal Market brought attention to their weak cybersecurity standard, reflected by widespread and oftentimes unpatched vulnerabilities and successful cyberattacks. Attacks on cyber-physical systems have a critical impact not only on the Union's economy but also on consumers' health, safety, and fundamental rights. Against the background of the failure of the cybersecurity market of connected devices, the 10 December 2024 entered into force 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 (Cyber Resilience Act, CRA). After casting light on the three regulatory foundational choices underpinning this EU legal act in the field of cybersecurity (ie, horizontal approach, risk-based approach, product safety approach), the article investigates the extent to which the CRA enhances the protection of fundamental rights, as claimed in the Explanatory Memorandum of the Commission's proposal.

Keywords: cyber resilience act; cybersecurity; fundamental rights

I. Introduction

Connected products are notoriously nonsecure. The underlying hardware and software components are easy targets of cyber-attacks.¹ Provided that such digital products are increasingly interconnected, a security incident can affect an entire organisation, or even an entire supply chain with dramatic spillover effects.² The failure of the market of connected products to deliver optimal levels of cybersecurity is characterised by several externalities, such as free riding and public goods.

On the one hand, information asymmetries between vendors and buyers can contribute to market failures as consumers either do not possess the knowledge to assess the level of cybersecurity of the products they purchase or they cannot access such information; as a result, vendors are not incentivised to offer more secure products since buyers will not

¹ ENISA, "ENISA Threat Landscape 2023" (2023) 66, 95–6 available at <<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>> (last accessed 1 July 2024).

² ENISA, "ENISA Threat Landscape for Supply Chain Attacks" (2021) available at <<https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>> (last accessed 1 July 2024); ENISA, "Guidelines for Securing the Internet of Things – Secure Supply Chain for IoT" (2020) available at <<https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>> (last accessed 1 July 2024); see also Mattis van't Schip, "The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things" (2024) 15 *European Journal of Law and Technology* 1.

reward them. On the other hand, manufacturers of connected devices are not presented with the right economic and/or legal incentives to invest in security (eg, addressing vulnerabilities), resulting in a sub-optimal investment level.³

In the context of the EU Internal Market specifically,⁴ the European Commission identified the lack of cybersecurity requirements for ICT products in the regulatory framework (regulatory failure) as a major driver of this market failure.⁵ Thus, the EU legislative landscape in 2021 did not comprehensively cover hardware and software products, especially “non-embedded” software, about their cybersecurity.⁶ Hence, on 15 September 2022, the EU Commission proposed a regulation on horizontal cybersecurity requirements for products with digital elements, the Cyber Resilience Act (hereinafter CRA).⁷ The CRA entered into force in December 2024 as Regulation (EU) 2024/2847.⁸ At a higher level, the CRA aims to address the two major issues hindering the realisation of the digital products’ cybersecurity market: (i) widespread vulnerabilities of products with digital elements and insufficient provision of security patches; and, (ii) lack of understanding and limited access to cybersecurity information by users of such products.⁹

The CRA builds on the New Legislative Framework (NLF) principles and structures,¹⁰ that is, product safety. Harmonised product safety legislation limits to lay down the essential requirements (ERs) that products made available on the Internal Market have to meet. To demonstrate that products comply with these requirements, the NLF envisages different conformity assessment procedures, including the application of harmonised technical standards developed by European Standardisation Organisations (ETSI, CEN, and CENELEC).

While Regulation (EU) 2024/1689 laying down harmonized rules on Artificial Intelligence (AI Act) more explicitly combines three EU regulatory approaches, ie, risk-based, product safety, and rights-based,¹¹ the CRA integrates *prima facie* only the risk-based approach – which has become the “standard” model of governance of EU digital policies¹² – with the product safety approach. Like the AI Act, the CRA considers that not all products with digital elements are equally critical. Unlike the AI Act, however, the CRA declines the risk-based approach by differentiating between the products in scope, mainly with regard to the conformity assessment obligations the manufacturers have to follow. It follows that

³ European Commission, “Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715 Final Study Report” (2021) 34–7.

⁴ See I Nash, ‘Cybersecurity Landscape of Internet of Things (IoT) Devices: A Comparative Perspective’ in S Martinelli, P Perri and C Poncibò (eds), *EU Product Liability for Platforms, Internet of Things and Artificial Intelligence* (Routledge, forthcoming) for an analysis on extra-EU legal acts dealing with connected devices cybersecurity.

⁵ *Ibid.*, 69; 73.

⁶ *Ibid.*, 52–62.

⁷ 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.

⁸ 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) (Text with EEA relevance).

⁹ Cyber Resilience Act Proposal, Recital 1.

¹⁰ The New Legislative Framework Consist of Regulation EU 765/2008; Decision 768/2008; Regulation EU 2019/1020 (the latter being amended by the CRA), see European Commission, “The ‘Blue Guide’ on the Implementation of EU Products Rules 2022 (2022/C 247/01), Official Journal of the European Union.”

¹¹ T Evas, “The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI” (2024) 1 AIRe – Journal of AI Law and Regulation 98; M Almada and N Petit, “The EU AI Act: A Medley of Product Safety and Fundamental Rights?” (2023) Robert Schuman Centre for Advanced Studies Working Paper 2023/59 available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4308072> (last accessed 24 July 2024).

¹² G De Gregorio and P Dunn, “The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age” (2022) 59 Common Market Law Review 473; PG Chiara and F Galli, “Normative Considerations on Impact Assessments in EU Digital Policy” (2024) 1 MediaLaws 86, 105.

all products in the scope of the CRA will have to comply with the CRA's essential requirements.

Compared to the AI Act, the CRA does not *explicitly* and *directly* embrace a rights-based approach. However, the Explanatory Memorandum of the EU Commission to the CRA proposal claimed that the Regulation would “enhance to a certain extent the protection of fundamental rights and freedoms such as privacy, protection of personal data, freedom to conduct business and protection of property or personal dignity and integrity.”¹³ In this respect, the engagement of the AI Act with fundamental rights is used as a comparative benchmark for the analysis, given that, like the CRA, the AI Act builds on EU product safety principles and institutions, and both regulations (also) aim to protect fundamental rights. The AI Act finds indeed one of its regulatory justifications in dealing with fundamental rights issues raised by AI systems. This notwithstanding, fundamental rights “appear sparingly in the main text [of the AI Act], and are always accompanied by the health and safety imperatives that are the traditional object of EU product safety law.”¹⁴ On the other hand, references to fundamental rights appear even less in the main text of the CRA. In this respect, the final version of the CRA does not refer to risks to fundamental rights *per se*, like the AI Act, but to compliance with obligations under Union or Member States law intended to protect fundamental rights.

By unfolding the CRA along its main pillars, the paper aims to cast light on the regulatory foundational choices underpinning the Cyber Resilience Act (section II). In particular, the normative analysis takes into account the extent to which the CRA will uphold fundamental rights, which is in line with other legal acts in EU “digital” law (section III).¹⁵ In particular, the CRA and AI Act are assessed against the background of the degree of fundamental rights protection afforded by the two legal instruments, even though the rights impacted by products with digital elements, on the one hand, and AI systems, on the other hand, might not coincide. Finally, section IV draws some conclusive remarks.

II. Understanding the regulatory approach of the Cyber Resilience Act

From a regulatory perspective, similar to the AI Act, the CRA builds on three foundational choices: (1) a horizontal framework; (2) a risk-based approach; (3) a product safety approach. Whereas the AI Act enhances the latter with a rights-based approach to uphold fundamental rights and societal values,¹⁶ it is worth asking to what extent the CRA deploys mechanisms to ensure that products with digital elements respect fundamental rights. Suppose the original goal of the Commission, as stated in the Explanatory Memorandum of the CRA, as seen above, would prove to be true. In that case, another question that ought to be asked is whether and to what extent CRA's product safety mechanisms are well suited to address fundamental rights challenges. However, before delving into the “fundamental rights conundrum” of the CRA, it is necessary first to understand how the three above-mentioned regulatory approaches interact in this piece of EU product safety legislation.

¹³ Explanatory Memorandum to the Cyber Resilience Act proposal (COM(2022) 454 final) 8.

¹⁴ M Almada and N Petit (n 12) 11–12.

¹⁵ Starting from the General Data Protection Regulation which furthers a fundamental right (Article 8 of the Charter of Fundamental Rights of the European Union), other recently enacted EU “digital” legal acts hinge *inter alia* on the protection of fundamental rights. That is the case of Regulation (EU) 2024/1689 (AI Act); Regulation (EU) 2022/2065 (Digital Services Act). See S Seubert and C Becker, “The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection” (2021) 22 German Law Journal 31.

¹⁶ T Evas (n 12) 100.

1. The horizontal approach

As mentioned in the introduction, one of the regulatory drivers underlying the CRA proposal was the fragmented EU legal framework with regard to mandatory cybersecurity requirements for products (with digital elements).¹⁷ Therefore, the Commission opted for a horizontal regulatory approach rather than (continuing to rely on) sectoral legislation to ensure legal certainty, avoid further market fragmentation, and minimise the compliance burden on manufacturers generated by several legal acts.¹⁸

Accordingly, the CRA introduces objective-oriented and technology-neutral cybersecurity essential requirements that apply to all the products in scope. The broad, cross-sectorial scope of the Regulation is a direct consequence of such a horizontal foundation. The CRA applies to all products with digital elements (hereinafter, PDE) “the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.”¹⁹

To understand the extent of such horizontal scope, it is necessary to unravel the notion of PDE. Within the meaning of “product with digital elements” falls any piece of hardware and software, including the software in the absence of which the product cannot perform one of its functions (ie, remote data processing solutions),²⁰ even if placed on the market separately.²¹ This notwithstanding, not all stand-alone software will have to comply with CRA’s essential requirements.

In fact, Recital 11 clarifies that remote data processing solutions, such as cloud solutions, fall in the scope of the CRA only insofar as they are necessary for a product to perform one of its functions, such as a mobile application requiring access to an API or to a database developed by the manufacturer. Thus, Directive (EU) 2022/2555 (NIS2) already applies to entities providing cloud computing services and cloud service models such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS).²²

In this respect, DIGITALEUROPE warned the EU legislator to clarify the interplay between the NIS2 and the CRA as many “cloud-based software tools will be subject to both the CRA and the NIS2, despite these targeting different aspects of the cybersecurity domain.”²³ As a result of such pleas, the final text of the CRA contains a provision that requires the Commission to publish guidance to facilitate the implementation of the CRA by economic operators and ensure the consistency of such implementation.²⁴ In particular, these documents should address *inter alia* the scope of the CRA, “with a particular focus on remote data processing solutions and free and open-source software.”²⁵

Moreover, a partial carve-out is provided, by negative, for free and open-source software (FOSS) if it is not made available on the market, that is, supplied for distribution or use in the course of a commercial activity.²⁶ Thus, policymakers felt that regulating

¹⁷ European Commission, “Staff Working Document Impact Assessment Report Accompanying the Document Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020” SWD(2022) 282 final, 2. See also Cyber Resilience Act, recital 3.

¹⁸ *Ibid.*, 8. See also PG Chiara, “The IoT and the New EU Cybersecurity Regulatory Landscape” (2022) 36 *International Review of Law, Computers & Technology* 118, 130–1. The same choice has been made with regard to the AI Act, see recitals 8 and 9 of Regulation (EU) 2024/1689.

¹⁹ Cyber Resilience Act, Article 2(1).

²⁰ Cyber Resilience Act, Article 3(2).

²¹ Cyber Resilience Act, Article 3(1).

²² Cyber Resilience Act, recital 12.

²³ DIGITALEUROPE, “The Single Market Love Story: 10 Digital Actions to Save the 30-Year Marriage” (2024) p 20 available at <<https://cdn.digitaleurope.org/uploads/2024/02/DIGITAL-EUROPE-THE-SINGLE-MARKET-LOVE-STORY-FINAL-WEB.pdf>> (last accessed 19 July 2024).

²⁴ Cyber Resilience Act, Article 26(1).

²⁵ Cyber Resilience Act, Article 26(2)(a).

²⁶ Cyber Resilience Act, recital 18.

FOSS cybersecurity was necessary amidst recent supply chain attacks involving open-source components (eg, Log4Shell or XZ Utils).²⁷ In order not to hamper the development and deployment of FOSS, the EU legislator opted for a “light-touch” regulatory regime, including “softer” obligations for legal persons (open-source stewards) providing support on a sustained basis for the development of FOSS intended for commercial activities (eg, foundations supporting specific FOSS projects; or companies developing FOSS for their use that make it available; or not-for-profit entities developing FOSS in a business context).²⁸ Despite such a “light-touch” approach, the FOSS community still fears that the new rules may eventually conflict with its decentralised and cooperative inherent nature.²⁹

Then, some PDEs are outright excluded from the scope of the CRA as the Union sectoral legal acts that apply to them adequately address cybersecurity and information security risks. That is the case of medical and in-vitro devices,³⁰ motor vehicles,³¹ aeronautical equipment certified under Regulation (EU) 2018/1139, and marine equipment in the scope of Directive 2014/90/EU.

Lastly, the CRA does not apply to spare parts made available on the market intended to replace identical components in PDE, provided that they are manufactured according to the exact specifications and PDE are developed exclusively for national security or defense purposes.³²

2. The risk-based approach

The CRA hinges on a risk-based approach in line with recent EU legislation regulating the digital sphere. Accordingly, products are clustered into categories depending on their cybersecurity risk. CRA’s understanding of cybersecurity risk is functional and traditional at the same time. It is functional since it generally and neutrally refers to “the potential for loss or disruption caused by an incident,”³³ leaving therefore enough room to encompass unintentional and intentional acts. It is traditional as it aligns with well-established risk assessment methodologies where risk is expressed as a combination of two variables, ie, the magnitude of the impact (ie, the loss or disruption) and the likelihood of occurrence of the incident.³⁴

Besides a “default” category, products with digital elements are “important” if their core functionality is listed in Annex III.³⁵ The rationale underlying this classification lies in the higher severity of the exploitation of potential vulnerabilities of such products due to either their cybersecurity-related functionality or the performance of a function carrying a significant risk of adverse effects in terms of its intensity and ability to damage other products with digital elements or to the health, security or safety of its users, through direct

²⁷ L Colonna, “The End of Open Source? Regulating Open Source under the Cyber Resilience Act and the New Product Liability Directive” (2025) 56 *Computer Law & Security Review* 106105, 4–5; J Tridgell, “Open or Closing Doors? The Influence of ‘Digital Sovereignty’ in the EU’s Cybersecurity Strategy on Cybersecurity of Open-Source Software” (2025) 56 *Computer Law & Security Review* 106078.

²⁸ Cyber Resilience Act, recital 19; Article 24. In a nutshell, OSS stewards (1) put in place a cybersecurity policy with a view to fostering the development of a secure product as well as an effective handling of vulnerabilities; (2) cooperate with market surveillance authorities; (3) have several reporting duties vis-à-vis incidents and vulnerabilities, but only to the extent that they are involved in the development of such products.

²⁹ See Liane Colonna (n 28) 16–18.

³⁰ For which Regulation (EU) 2017/745 and Regulation (EU) 2017/746 apply respectively.

³¹ For which Regulation (EU) 2019/2144 applies.

³² Cyber Resilience Act, Article 2(7).

³³ Cyber Resilience Act, Article 3(37).

³⁴ In this regard, “significant cybersecurity risk” is the risk that is very likely to lead to a severe negative impact, including by causing considerable material or non-material loss or disruption.

³⁵ Cyber Resilience Act, Article 7(1).

manipulation.³⁶ This products category is further divided into two classes, I³⁷ and II³⁸: products listed in class II reflect a higher level of cybersecurity risk as an incident might generate greater negative impacts.³⁹

The last category of products is that of “critical” PDEs. Using the same approach seen above, products with digital elements whose core functionality is listed in Annex IV are critical.⁴⁰ The classification builds on the criteria adopted with regard to important products and adds two other conditions: NIS2 essential entities have a critical dependency on the category of products, and/or incidents and exploited vulnerabilities concerning such category of products can lead to serious disruptions to critical supply chains across the EU market.⁴¹

The main normative implication of such risk-based taxonomy lies in the different conformity assessment procedures the manufacturers of such products have to follow. As addressed in the next section, important and critical products with digital elements have to undergo stricter conformity assessment procedures than the internal control procedure,⁴² that is, a self-assessment performed by the manufacturer.

In this respect, the CRA operationalises the risk-based approach in a different fashion than the AI Act, where AI systems, classified according to several levels of risk – as in the CRA, are associated with different safeguards to compensate for the risk they pose to protected values, such as fundamental rights, safety, and democracy. The rationale underlying the CRA opposes the view that minor risks require minimal precautions. For all the products falling in the scope of the CRA have to comply with the essential requirements set out in Annex I, whilst requirements set out in section 2, chapter 3 of the AI Act only apply to high-risk AI systems.

Similar to the AI Act,⁴³ however, the CRA predetermines the level of risk of specific products with digital elements without leaving room for an ex-post re-determination based, eg, on risk management measures as in the logic of Article 35 GDPR.⁴⁴ Moreover, such ex-ante pre-determination of the risk levels does not take into account the context where important or critical products are deployed.

Finally, the CRA deploys mechanisms to mitigate, besides cybersecurity risks, other risks such as the archetypical EU product safety health & safety risks, but also novel categories of risk, as is the case of the risk to compliance with obligations under Union or national law intended to protect fundamental rights; to the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by NIS2 essential entities or to other aspects of public interest protection.⁴⁵ Section IV further elaborates on the risk to compliance with fundamental rights obligations.

³⁶ Cyber Resilience Act, recital 43; Article 7(2).

³⁷ This class includes browsers, password managers and physical network interfaces, smart home general purpose virtual assistants, etc.

³⁸ This class includes hypervisors, firewalls, intrusion detection/prevention systems, tamper-resistant microprocessors, etc.

³⁹ Cyber Resilience Act, recital 44.

⁴⁰ This category includes hardware devices with security boxes; smart meter gateways within smart metering systems and smartcards.

⁴¹ Cyber Resilience Act, Article 8(2).

⁴² Module A of Decision No 768/2008/EC.

⁴³ C Novelli, F Casolari, A Rotolo, M Taddeo and L Floridi, “Taking AI Risks Seriously: A New Assessment Model for the AI Act” (2023) 38 *AI & Society* 1, 1.

⁴⁴ E Kosta, “Article 35 Data Protection Impact Assessment” in C Kuner, LA Bygrave, C Docksey and L Drechsler (eds), *The EU General Data Protection Regulation: A Commentary* (Oxford, Oxford University Press 2020) 665–679; D Hallinan and N Martin, “Fundamental Rights, the Normative Keystone of DPIA” (2020) 6 *European Data Protection Law Review* 178.

⁴⁵ Cyber Resilience Act, Article 57(1).

3. The product safety approach

The EU “product safety approach” hinges on ensuring that products – in this case, products with digital elements – are safe before they are made available on the Internal Market. It follows, therefore, an ex-ante, that is, pre-market regulatory logic. In a nutshell, the EU product safety acquis aligns with the so-called “New Legislative Framework” (NLF). Adopted in July 2008, the NLF consists of Regulation (EU) 765/2008, Decision 768/2008, and Regulation (EU) 2019/1020 and reformed the “New Approach” developed in 1985.⁴⁶

The New Approach replaced the Old Approach, where national authorities drew up highly prescriptive technical legislation (and sometimes delivered certificates of conformity themselves). From the 80s, legislative initiatives, the Court of Justice case-law (in particular, the *Cassis de Dijon* Case),⁴⁷ as well as the systematic application of the principle of mutual recognition aimed at preventing barriers for products within the EU market and promoting the free movement of goods. The New Approach legislative technique picked up the principles established in *Cassis de Dijon*, in particular: (i) harmonised legislation is limited to set out “essential requirements” that products placed on the EU market must meet; (ii) EU harmonised technical standards specify how products can meet such requirements from a technical perspective; (iii) products manufactured in compliance with harmonised technical standards (which is voluntary) benefit from a presumption of conformity with the relevant requirements.⁴⁸

The NLF complemented and reformed the New Approach by taking into account several elements: accreditation, notification, the conformity assessment procedure (so-called “modules” were introduced), CE marking, and market surveillance. To make a product available in the EU market, manufacturers have to demonstrate the conformity of their products with the corresponding essential requirements through specific conformity assessment procedures. Consistently with NLF principles, besides manufacturers, who are understandably the stakeholders with the greatest burdens in terms of compliance, a wide array of parties along the supply chain, from importers⁴⁹ and distributors⁵⁰ to authorised representatives,⁵¹ must comply with specific rules.

Since it aligns with the NLF, the CRA imposes as a precondition for making PDEs available on the EU market, whereby PDEs must meet the essential requirements (ERs) set out in Part 1 of Annex I⁵² and the processes put in place by the manufacturer must comply with the ERs set out in Part 2 of Annex I.⁵³

For the purpose of complying with the abovementioned obligation, manufacturers have to carry out an assessment of the cybersecurity risks associated with the PDE.⁵⁴ In line with the context-based tradition of risk management theory, the cybersecurity risk assessment

⁴⁶ European Commission (n 11) 5–6.

⁴⁷ Judgment of the Court of Justice of 20 February 1979, Case 120/78, *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein*.

⁴⁸ European Commission (n 11) 8.

⁴⁹ Cyber Resilience Act, Article 19.

⁵⁰ Cyber Resilience Act, Article 20.

⁵¹ Cyber Resilience Act, Article 18.

⁵² PDEs shall be designed, developed and produced to ensure an appropriate level of cybersecurity based on the risks. On the basis of the risk assessment, PDEs shall be made available without any known exploitable vulnerabilities and with a secure by default configuration; shall ensure protection from unauthorised access by appropriate control mechanisms; shall protect the confidentiality of processed personal or other data by means of state-of-the-art encryption, etc.

⁵³ Manufacturers of PDE shall: identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product; mitigate vulnerabilities without delay, including by providing security updates; apply effective and regular tests and reviews of the security of the product; publicly disclose information about fixed vulnerabilities, once a security update has been made available, etc.

⁵⁴ Cyber Resilience Act, Article 13(2).

has to be “based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use.”⁵⁵ This obligation clearly exemplifies the complementarity between the risk-based and product safety approach.

Manufacturers of PDEs must comply with many more obligations. For instance, when integrating components from third parties (including FOSS), manufacturers must make sure that such components do not compromise the cybersecurity of the PDE.⁵⁶ Moreover, they have several documentation (as per Article 31 and Annex VII)⁵⁷ and information obligations, vulnerability handling obligations, in accordance with the ERs set out in Part 2 of Annex I,⁵⁸ as well as cooperation obligations.⁵⁹

Notably, manufacturers also have to comply with a twofold set of reporting obligations. In the first case, when a manufacturer identifies a vulnerability in a component integrated into the PDE, it reports the vulnerability to the person or entity manufacturing or maintaining the component, and if it develops a patch, it then has to share the relevant code with said party.⁶⁰ This provision was added later in the legislative process and is to be welcomed as it provides (legal) incentives for cooperation between stakeholders with a view to ensuring a high level of resilience.⁶¹ In the second case, manufacturers notify the competent national market surveillance authority and ENISA of the exploited vulnerabilities and severe incidents having an impact on the security of the PDE.⁶²

Importantly, CRA’s requirements and obligations combine a more traditional by-design approach,⁶³ now fully entrenched in EU cybersecurity regulation,⁶⁴ with a lifecycle approach, which is not a hallmark of EU product safety legislation⁶⁵: not only cybersecurity cannot be (anymore) an afterthought but it must be taken seriously throughout a product’s lifecycle.⁶⁶

⁵⁵ Cyber Resilience Act, Article 13(3).

⁵⁶ Cyber Resilience Act, Article 13(5) CRA. Also on the due diligence front, manufacturers must ensure that PDEs bear a type, batch or other element allowing identification (Article 13(15) CRA).

⁵⁷ The technical documentation has to include the cybersecurity risk assessment (Article 13(4) CRA). Moreover, they have to document relevant cybersecurity aspects regarding the PDE (eg, vulnerabilities and information provided by third parties).

⁵⁸ When placing the PDE on the market and after marketing, for the support period, manufacturers ensure that the vulnerabilities of the product, including its components, are handled effectively through appropriate policies and procedures, including coordinated vulnerability disclosure policies (Article 13(8) CRA).

⁵⁹ Manufacturers keep the technical documentation and the EU declaration of conformity at disposal of the Market Surveillance Authorities for at least ten years after the marketing or for the support period – whichever is higher (Article 13(13) CRA).

⁶⁰ Cyber Resilience Act, Article 13(6).

⁶¹ M Taddeo, “Is Cybersecurity a Public Good?” (2019) 29 *Minds and Machines* 349, 351; R Brighi and PG Chiara, “La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell’Unione Europea” (2021) 21 *Federalismi* 17, 31.

⁶² Cyber Resilience Act, Article 14.

⁶³ The European Data Protection Supervisor, in its Opinion on the CRA proposal (EDPS, Opinion 23/2022), strongly recommended including the data protection by design (and by default) principle in the CRA’s ERs. However, these principles do not feature in the final text of the CRA. Instead, the principle of data minimisation appears as one of the ERs (Annex I, Part I, para. 2, letter g CRA).

⁶⁴ Lee A Bygrave, “Security by Design: Aspirations and Realities in a Regulatory Context” (2021) 8 *Oslo Law Review* 126, 126.

⁶⁵ PG Chiara (n 19) 126.

⁶⁶ C Ducuing, “Towards an Obligation to Secure Connected and Automated Vehicles ‘By Design?’” in A Vedder, J Schroers, C Ducuing and P Valcke (eds), *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Cambridge, Intersentia 2019) p 203; M Burri and Z Zihlmann, “The EU Cyber Resilience Act – An Appraisal and Contextualization” (2023) 2 *EuZ – Zeitschrift für Europarecht* B1 29; LA Bygrave, “Cyber Resilience versus Cybersecurity as Legal Aspiration” (14th International Conference on Cyber Conflict: Keep Moving, Tallinn 2022) 27.

In this respect, the CRA implicitly introduces a somewhat “principle of accountability,” as manufacturers have to determine themselves the support period of each PDE following several criteria and, if requested, they must be able to provide market authorities with the factors that were taken into account to determine such period.⁶⁷

The last step that manufacturers must take before marketing is demonstrating compliance with CRA essential requirements through a specific conformity assessment procedure. Finally, manufacturers draw up an EU declaration of conformity to state that the fulfillment of the ERs has been demonstrated⁶⁸ and affix the CE marking,⁶⁹ which indicates the conformity of a product.

Conformity assessment is one of the cornerstones of the NLF reform. In the specific context of the CRA, the risk-based taxonomy of PDEs (ie, default, important class I and II, critical, and FOSS) is mainly relevant as regards the different NLF procedures⁷⁰ manufacturers can or must follow to demonstrate compliance with the ERs. For the “default” category – which, according to the Commission, should cover the vast majority of PDEs,⁷¹ manufacturers can either opt for self-assessment (ie, internal control procedure, based on Module A of Decision No 768/2008/EC) or a stricter procedure involving a third party (eg, EU-type examination procedure, full quality assurance or, if available, an EU cybersecurity certification scheme).⁷²

As regards class I important PDEs, self-assessment is still allowed but additional safeguards are required⁷³: manufacturers need to apply, alternatively, harmonised technical standards,⁷⁴ common specifications⁷⁵ or European cybersecurity certification schemes. If not, the class I important PDE shall undergo third-party assessment. For class II important and critical PDEs self-assessment is excluded, even if the PDE complies with harmonised standards, technical specifications or EU cybersecurity certification schemes fully or in part.⁷⁶ The only exception is provided for important PDEs that qualify as FOSS: manufacturers can follow the internal control procedure based on Module A, provided that they make the technical documentation available to the public.⁷⁷ The rationale behind this regulatory choice lies in the transparency paradigm of the open source: anyone (tech-savvy enough) can verify the software’s degree of security.

III. The Cyber Resilience Act and fundamental rights protection: which tools in whose hands?

After examining the regulatory model of the CRA, combining a horizontal, risk-based and product safety approach, time is ripe to investigate the extent to which the Regulation enhances the protection of fundamental rights as claimed in the Explanatory

⁶⁷ Cyber Resilience Act, Article 13(8).

⁶⁸ Cyber Resilience Act, Article 28.

⁶⁹ Cyber Resilience Act, Article 30.

⁷⁰ Established in Decision No 768/2008/EC.

⁷¹ European Commission, Directorate-General for Communications Networks, Content and Technology, “Cyber Resilience Act: New EU Cybersecurity Rules Ensure More Secure Hardware and Software Products” (2022) available at <<https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products>> (last accessed 14 June 2024).

⁷² Cyber Resilience Act, Article 32(1).

⁷³ Cyber Resilience Act, Article 32(2).

⁷⁴ Cyber Resilience Act, Article 27(1).

⁷⁵ Cyber Resilience Act, Article 27(2).

⁷⁶ Cyber Resilience Act, Article 32(3) and (4). The Commission is empowered to determine, through delegated acts, which categories of critical PDEs are required to obtain a EU cybersecurity certificate to demonstrate conformity (Cyber Resilience Act, Article 8(1)).

⁷⁷ Cyber Resilience Act, Article 32(5).

Memorandum of the EU Commission to the CRA proposal. As seen, CRA obligations and essential requirements do not include mechanisms ensuring that PDEs respect fundamental rights, as opposed to the AI Act where the rights-based approach is clearly displayed throughout this atypical product safety instrument, starting from the legal basis added during the trilogue negotiations to regulate personal data protection under Article 16 TFEU, although it is not the first NLF regulation to embed fundamental rights protection.⁷⁸

In short, Article 1 AI Act clarifies from the outset that the Regulation aims, on the one hand, to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI) and, on the other hand, to ensure a high level of protection of health, safety, fundamental rights enshrined in the Charter. Then, the adverse impact on fundamental rights is one of the criteria to be followed by the Commission when modifying the taxonomy of high-risk AI systems listed in Annex III of the AI Act.⁷⁹ Furthermore, different essential requirements for high-risk AI systems take into account risks to fundamental rights,⁸⁰ and an obligation to conduct a fundamental rights impact assessment for high-risk AI systems is foreseen for specific deployers.⁸¹ Finally, the Commission may subject specific high-risk AI systems to third-party conformity assessment by taking into account the effectiveness of self-assessment (internal control procedure) in minimising the risks to fundamental rights.⁸²

The CRA, instead, barely contains any references to fundamental rights. And those few only relate to enforcement procedures. Products with digital elements might pose risks to fundamental rights, although compliant with CRA's essential requirements. For instance, the rights to privacy (Article 7, EU Charter of Fundamental Rights, CFR) and protection of personal data (Article 8 CFR) may be impacted by, say, Security Information and Event Management (SIEM) products, falling under CRA's Class I Important products, as they have to process large amounts of data, potentially including personal data, to detect anomalous situations and prevent attacks. Moreover, the parents' right to education (Article 14 CFR) might be impacted by value-laden AI-generated content of connected toys, falling in the scope of the CRA. All in all, given the broad horizontal scope of the CRA (Sect. II, 1), most commercial products, which are susceptible to being deployed in very diverse sectors, must comply with CRA's requirements. The implications for fundamental rights are significant. Thus, assessing which fundamental rights are impacted will eventually depend on the context in which these products are deployed and the specific application domain.

Against this backdrop, this section aims to unravel the enforcement mechanisms set out in Chapter V of the CRA with a view to assessing the degree of protection afforded by the CRA provisions to fundamental rights. In terms of private enforcement, the final version of the CRA improved consumer protection compared to the Commission's proposal, which was highly criticized in this regard.⁸³ If, on the one hand, market surveillance authorities have an obligation to inform consumers of where to submit complaints indicating non-compliance with the CRA,⁸⁴ on the other hand, the CRA does not foresee an autonomous

⁷⁸ See Regulation (EU) 2017/745 (medical devices regulation).

⁷⁹ Artificial Intelligence Act, Article 7. See also Article 6(3).

⁸⁰ Artificial Intelligence Act, Articles 9(2)(a); 10(2)(f); 13(3)(b)(iii); 14(2).

⁸¹ Artificial Intelligence Act, Article 27.

⁸² Artificial Intelligence Act, Article 43(6).

⁸³ H-W Micklitz, "The Role of Standards in Future EU Digital Policy Legislation: A Consumer Perspective" (2023) Report commissioned by BEUC and ANEC, pp 79–80 available at <<https://www.anec.eu/images/Publications/other-publications/2023/ANEC-DIGITAL-2023-G-138.pdf>> (last accessed 12 July 2024); BEUC, "The Cyber Resilience Act Proposal – BEUC Position Paper" (2023) p 23 available at <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-006_The_Cyber_Resilience_Act_Proposal.pdf> (last accessed 12 July 2024).

⁸⁴ Cyber Resilience Act, Article 52(11). Market surveillance authorities are also tasked to set up mechanisms to facilitate reporting of vulnerabilities, incidents and cyber threats that may affect PDEs.

individual right to lodge a complaint to said authorities, like in the case of Article 85 of the AI Act. Moreover, the final version of the Regulation includes an amendment to Directive (EU) 2020/1828 on representative actions (RAD).⁸⁵ Accordingly, the RAD is applicable to collective redress mechanisms concerning infringements of the CRA that can harm consumers' collective interests.⁸⁶

Besides, it is worth taking into account the interplay between the revised Product Liability Directive (PLD)⁸⁷ and the CRA. The former will consider a product to be defective if it does not provide – among others – safety-relevant cybersecurity requirements.⁸⁸ Such requirements are to be found in the CRA.⁸⁹ In other words, where damages occur as a result of a lack of safety in a PDE, and where such lack of safety consists of a lack of security updates, consumers can hold manufacturers liable pursuant to the revised PLD. That being said, consumers are not awarded with legal means of redress to claim an infringement of their fundamental rights resulting from an infringement of the CRA.

In terms of public enforcement, the CRA aligns with the NLF, in particular, Regulation (EU) 2019/1020 on market surveillance. National market surveillance authorities carry out an evaluation of a PDE with respect to its compliance with CRA's requirements, if they have sufficient reason to consider (for example, through consumers' complaints) that it presents a significant cybersecurity risk, the determination of which shall also consider non-technical risk factors.⁹⁰

If the PDE does not comply with the relevant requirements, the authority can prescribe corrective or restrictive measures, including bringing the PDE into compliance with those requirements and withdrawing or recalling it from the market. In such cases, the authority informs the Commission and the other national market surveillance authorities, which can object to those measures. If no objections are raised, the measures are deemed justified; otherwise, a specific Union safeguard procedure is triggered.⁹¹ In terms of cooperation, market surveillance authorities can carry out joint activities with regard to specific PDEs⁹² and can conduct simultaneous coordinated control actions ("sweeps") to check compliance with the CRA.⁹³

Importantly, the Commission is empowered to activate the enforcement process by informing the relevant authority that a PDE is likely not to comply with CRA requirements.⁹⁴ If the relevant authority does not take effective measures, and if the Commission has reason to consider that the PDE remains non-complaint, only in cases that justify an immediate intervention to preserve the proper functioning of the internal market, the Commission carries out an evaluation of compliance, with the support of ENISA, if requested.⁹⁵ Following such evaluation, corrective or restrictive measures can be imposed by the Commission at the Union level after consultation with the Member States and the economic operators concerned.

Although compliant with the CRA, a product with digital elements can nonetheless pose a significant cybersecurity risk, or other risks such as: (i) to the health or safety of persons; (ii) to compliance with obligations under Union or Member States law intended to protect fundamental rights [emphasis added]; (iii) availability, authenticity, integrity or

⁸⁵ Cyber Resilience Act, Article 67.

⁸⁶ Cyber Resilience Act, recital 125; Article 65.

⁸⁷ Directive (EU) 2024/2853 on liability for defective products and repealing Council Directive 85/374/EEC.

⁸⁸ New Product Liability Directive, Article 7(2)(f).

⁸⁹ Cyber Resilience Act, recital 31.

⁹⁰ Cyber Resilience Act, Article 54.

⁹¹ Cyber Resilience Act, Article 55.

⁹² Cyber Resilience Act, Article 59.

⁹³ Cyber Resilience Act, Article 60.

⁹⁴ Cyber Resilience Act, Article 56.

⁹⁵ Cyber Resilience Act, Article 56(3).

confidentiality of services offered using an electronic information system by NIS2 essential entities; or (iv) other aspects of public interest protection.⁹⁶

Should a national Market Surveillance Authority conclude after an evaluation (see above) that this is the case, it requires the manufacturer to take all appropriate measures to ensure that the product no longer presents said risks or to withdraw or recall the product from the market. As in the “standard” procedure at the national level, the authority immediately informs the Commission and the other Member States of the measures adopted. The Commission then consults with the Member States and the relevant operator to decide whether the measure is justified.

As in the procedure at the Union level, the Commission may trigger the evaluation of the relevant market surveillance authority if it considers that a PDE poses the abovementioned risks.⁹⁷ Also this procedure envisages the possibility for the Commission to take over the risk assessment from national authorities, with the support of ENISA, provided that: (a) exceptional circumstances justify an immediate intervention to preserve the proper functioning of the EU market; (b) no effective measures have been taken by the relevant national authority; (c) the Commission has sufficient reason to consider that the PDE still presents the risks to those fundamental values; (d) it informs the relevant market surveillance authorities accordingly.⁹⁸ The Commission may then impose a corrective or restrictive measure at the Union level.⁹⁹

I. Procedural challenges

To get an understanding of the fundamental rights relevance in the CRA’s enforcement mechanisms, the analysis needs to focus on the procedure of Article 57 CRA described above, ie, complaint PDEs that nonetheless present significant risks. From a procedural standpoint, the CRA is surprisingly concise. This opens up a number of significant questions. How much time has to pass between the Commission’s notification to the relevant market surveillance authority and its inaction before the Commission’s takeover? What are the exceptional circumstances that justify the immediate intervention of the Commission?

It is thus not clear when the Commission can effectively take over from national Market Surveillance Authorities in situations where PDEs do not comply with the CRA or do comply but present nevertheless a significant cybersecurity risk or other risks to fundamental values. Against the background of a widespread lack of staff and financial resources of market surveillance authorities at the Union level,¹⁰⁰ it is not unreasonable to imagine that slow enforcement risks becoming the rule rather than the exception. The lack of deadlines leaves even more astonished if those procedures are compared with the Union safeguard procedure under Article 55 CRA. In that case, the Commission decides whether corrective or restrictive measures taken by national authorities are justified or not within a specific timeframe (ie, nine months from the notification from the relevant authority).

Moreover, other legal acts in EU “digital law” contemplate scenarios where subject to specific conditions, there is a transfer of enforcement powers from the national to the Commission level. However, Regulation (EU) 2022/2065 (Digital Services Act), for instance,

⁹⁶ Cyber Resilience Act, Article 57(1).

⁹⁷ Cyber Resilience Act, Article 57(6).

⁹⁸ Cyber Resilience Act, Article 57(7).

⁹⁹ Cyber Resilience Act, Article 57(8).

¹⁰⁰ European Commission, “Study for the Preparation of an Implementation Report of the General Product Safety Directive – Final Report” (2020) p 91 available at <https://commission.europa.eu/system/files/2021-09/final_report-gpsd-part1-main_report-final-corrected2.pdf> (last accessed 23 July 2024). See also TUV Verband, “Market Surveillance – Rreport” available at <<https://www.tuev-verband.de/en/products/product-safety-legislation/market-surveillance>> (last accessed 23 July 2024).

sets precise deadlines for this referral.¹⁰¹ All in all, the vague formula of the CRA would potentially leave in the hands of the Commission a blank cheque for choosing which PDEs to bring to the scrutiny of its offices, alleging the exceptional nature of the circumstances.

Related to that, whereas Recital 113 CRA sheds light on the meaning of “exceptional circumstances,” it only makes reference to seemingly less problematic situations of emergency where non-compliant products are widely made available by the manufacturer throughout several Member States or used in key sectors by NIS2 entities while containing known vulnerabilities that are being exploited by malicious actors and for which the manufacturer does not provide available patches. This notwithstanding, there is no indication in Article 57, nor in the corresponding recitals, as to the criteria for determining what an exceptional circumstance might amount to in the case of complaint PDEs.

A possible solution to the question of which criteria should be taken into account in determining the exceptionality of circumstances could look at the gravity of the risk posed by the (compliant) product. This argument follows from the interpretation of Recital 113 CRA, whereby exceptionality is linked to a cross-border effect or the critical context in which the product is used.

From a comparative perspective, it is possible to resort to the AI Act, with a view to critically reflecting on relevant “regulatory siblings,” that is, “legal rules which bear a striking terminological resemblance, if not sometimes an identical form.”¹⁰² In particular, Article 82 AI Act, laying down (procedural) enforcement rules for compliant AI systems that present a risk, is the regulatory sibling of Article 57 CRA. In the case of the AI Act, however, the Commission does not have the power to request the relevant authority to evaluate a compliant AI system or to carry out an evaluation, as in the CRA.

The ambiguities addressed above reveal a picture of legal uncertainty, which eventually leaves considerable power in the hands of the Commission. In this regard, recent developments in EU product safety *acquis*, notably the CRA, the AI Act,¹⁰³ and the General Product Safety Regulation,¹⁰⁴ or in the Digital Single Market (eg, Digital Services Act¹⁰⁵ and Digital Markets Act¹⁰⁶), can be seen as significant steps in the ongoing paradigm shift where enforcement powers, once the exclusive prerogative of national authorities, increasingly assume Union relevance through a centralisation on the Commission.

2. Substantive challenges

As seen above, Article 57 lists, besides significant cybersecurity risks, several other risks that shall be managed by economic operators if posed by their products. Whereas the risk to the health or safety of persons is the bread and butter of EU product safety legislation, the remaining three categories, ie, (i) the risk to compliance with obligations intended to protect fundamental rights; (ii) availability, authenticity, integrity or confidentiality of services offered by NIS2 entities or, (iii) other aspects of public interest protection deserve more attention. If the last risk-category has already been criticised for being ultimately a too vague and broad open clause,¹⁰⁷ for the purpose of this paper, the analysis focuses only on the risk to compliance with fundamental rights obligations.

¹⁰¹ Digital Services Act, Article 59(1).

¹⁰² C Goanta, “Regulatory Siblings: The Unfair Commercial Practices Directive Roots and the AI Act” in I Graef and B van Der Sloot (eds), *The Legal Consistency of Technology Regulation in Europe* (London, Hart Publishing 2024) 84.

¹⁰³ Artificial Intelligence Act, Article 75: the AI Office, within the Commission, is tasked to monitor and supervise compliance of AI systems based on general-purpose AI models with the obligations of the AI Act.

¹⁰⁴ See Chapter VII of Regulation (EU) 2023/988 (General Product Safety Regulation).

¹⁰⁵ Digital Services Act, Article 56.

¹⁰⁶ See Chapter V of the Digital Markets Act.

¹⁰⁷ M Burri and Z Zihlmann (n 67) 41.

The main research question underlying the legal analysis was to what extent the CRA could enhance the protection of fundamental rights. A closer look at the abovementioned provision reveals how the CRA upholds fundamental rights and, consequently, how the “risk to rights” is operationalised in this piece of EU law. The risk is not to fundamental rights¹⁰⁸ *per se*, but to the compliance with obligations intended to protect fundamental rights. In the first scenario, the emphasis is more on the violation of the essence of the right; in the second scenario, on the other hand, the risk is somewhat more specific, ie, with respect to compliance with a second-level norm implementing a fundamental right. The question that must be asked is whether the difference between the two approaches is merely semantic or, however subtle, substantial. In other words, does the assessment that the law requires change completely?

This is a major difference from the “regulatory sibling” of the AI Act. Article 82 AI Act mandates market surveillance authorities to require the relevant economic operator to take all appropriate measures to ensure that the high-risk AI system, although compliant with the Act, no longer presents a risk to fundamental rights. And not to the compliance with fundamental rights obligations. Such an approach is coherent with the rights-based regulatory foundation of the AI Act, even if the choice to achieve fundamental rights protection ends in the context of AI by recourse to product safety means has attracted a lot of criticism.¹⁰⁹

Here lies the crux of the CRA. Thus, the Commission’s CRA proposal was more ambiguous, as Recital 59 referred to risks to fundamental rights (like the AI Act), whereas Article 46 was already in its final form, ie, risks to the compliance with obligations under Union or national law intended to protect fundamental rights.

In the first scenario seen above, the relevant authority, or the Commission, would have to carry out a contextual and expert-based fundamental rights impact assessment to determine whether a specific PDE entails a risk to specific rights and freedoms. As rights and freedoms are not easily quantified,¹¹⁰ these evaluations usually imply ascribing values to them.¹¹¹ This activity requires complex interpretative reasoning, a good knowledge of the relevant legal sources and case law, and, finally, normative judgments.¹¹²

In the second scenario, on the other hand, the relevant authority – or the Commission – “only” has to verify whether a specific PDE complies with a set of obligations aiming to safeguard fundamental rights. At first glance, the outcome of such an assessment could be binary: an obligation is either respected or violated. Yet, such a non-flexible understanding of compliance seems to be at odds with the very rationale of risk, which is inherently scalable and granular. In the field of data protection, Gellert proposed that the GDPR’s “risk to fundamental rights” should be considered in terms of “risk of non-compliance with the GDPR”: “the lower the compliance, the higher the potential violations of the data subjects’ fundamental rights. Inversely, just as a low level of compliance signals the likely infringement of the data subject’s rights and freedoms, ensuring in turn that the rights and

¹⁰⁸ The primary point of reference for the protection of FR should be the Charter, predominant over the other two sources of fundamental rights recognised by Article 6 TEU, namely ECHR and the constitutional traditions common to the Member States. See T Tridimas, “Fundamental Rights, General Principles of EU Law, and the Charter” (2014) 16 *Cambridge Yearbook of European Legal Studies* 361, 377.

¹⁰⁹ M Almada and N Petit (n 12) 18 and ff.

¹¹⁰ AJ Rosga and ML Satterthwaite, “The Trust in Indicators: Measuring Human Rights” (2009) 27 *Berkeley Journal of International Law* 253; see also JS Sampaio, “Proportionality in Its Narrow Sense and Measuring the Intensity of Restrictions on Fundamental Rights” in D Duarte and JS Sampaio (eds), *Proportionality in Law* (Cham, Springer 2018) 71–110.

¹¹¹ For example, Mantelero proposes a methodology to quantify impacts to fundamental and human rights in his *Human Rights, Ethical, and Social Impact Assessment (HRESIA): A Mantelero, Beyond Data: Human Rights, Ethical, and Social Impact Assessment in AI* (The Hague, Springer 2022); See also G Sartor, “The Logic of Proportionality: Reasoning with Non-Numerical Magnitudes” (2013) 14 *German Law Journal* 1419.

¹¹² PG Chiara and F Galli (n 13) 98–9.

freedoms are not violated by the processing operation contributing to higher levels of compliance.”¹¹³

In light of the above, also the compliance check will entail normative, qualitative and/or quantitative, context-based evaluations depending on the specific obligation scrutinised.¹¹⁴ Products with digital elements of everyday use, falling in the scope of the CRA, like smart cameras, alarm systems, fitness trackers, headsets, etc. collect, process, and share a significant amount of users’ personal and sensitive data over time (eg, position, temperature, blood pressure, heart rate). Under the CRA, a PDE will be assessed against its degree of compliance with, eg, GDPR’s principles relating to personal data processing, such as data minimisation¹¹⁵ – which, not surprisingly, is the only data protection-related essential requirements of the CRA, as well as data subject rights, eg, right to erasure,¹¹⁶ which might be at risk of not-be-complied with if the PDE does not afford the end-user the possibility of deleting all personal data concerning him/her from the device.

Yet, does Article 57 CRA really enhance and complement existing EU or national legislation safeguarding fundamental rights and liberties, such as Regulation (EU) 2016/679 (GDPR)? The answer is in the affirmative. Data Protection Supervisory Authorities do not have the *same* enforcement powers of Market Surveillance Authorities for infringements of the GDPR, although some may argue that the corrective measure of a definitive limitation on processing under Article 58(2)(f) GDPR, essentially amounting to a ban, has effects similar to the most severe corrective powers of MSAs under EU product safety legislation. As a result of the interplay between the GDPR and the CRA, however, where a PDE, although compliant with the CRA, poses nonetheless a risk to the compliance of GDPR obligations, national Market Surveillance Authorities or the Commission will be able to take the same measures that the authority can enforce vis-à-vis non-compliant products. It might even go so far as to demand the withdrawal of the PDE from the Single Market. In other words, if a PDE in CRA’s scope fails to provide safeguards to protect users’ privacy and personal data protection can be subject to the Commission (or national authorities) product safety enforcement powers.

This notwithstanding, market surveillance authorities do not seem well-suited to carry out these value-based regulatory assessments due to the long-standing experience of data protection authorities in this field. Also, in the light of the chronic understaffing and underfunding issues, coupled with an unclear procedure, it is likely that an authority’s lack of readiness to initiate an enforcement procedure may give the Commission the opportunity to take severe restrictive and corrective measures on the grounds of eminently qualitative assessments. Against the backdrop of the relevance of non-technical factors (geopolitical factors, such as undue influence by a third country on suppliers) to determine the significance of cybersecurity risk,¹¹⁷ the underlying risk is “to weaponize” fundamental rights to achieve political ends.

IV. Conclusion

Despite receiving scant exposure in the literature, especially compared to the AI Act – which has nevertheless a significantly narrower scope, the CRA has everything it needs to

¹¹³ R Gellert, “Understanding the Notion of Risk in the General Data Protection Regulation” (2018) 34 Computer Law & Security Review 279, 284.

¹¹⁴ See *inter alia* G Malgieri and C Santos, “Assessing the (Severity of) Impacts on Fundamental Rights” (2024) SSRN available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4875937> (last accessed 29 July 2024). The authors propose three factors to measure the severity of infringements of positive rules established by law intended to protect fundamental rights.

¹¹⁵ General Data Protection Regulation, Art 5(1)(c).

¹¹⁶ General Data Protection Regulation, Art 17.

¹¹⁷ Cyber Resilience Act, Arts 54(2); 56(2).

be the new “GDPR” in terms of the potential to impact and “revolutionise” the market it regulates.¹¹⁸ Against this backdrop, this article dealt with the regulatory framework of the CRA, in particular, with a view to ascertaining to what extent this piece of EU product safety legislation would enhance the protection of fundamental rights, as claimed by the Commission in the Explanatory Memorandum to the proposal.

The legal analysis highlighted the regulatory approaches underlying the CRA (ie, horizontal, risk-based, and product safety approach) and compared the identified foundational choices with the ones operating in the AI Act. For both regulations rely on EU product safety law principles and aim to safeguard fundamental rights, albeit through different mechanisms and, as demonstrated, with varying outcomes. Thus, the most striking divergence between the two lies in implementing fundamental rights protection institutions. Whereas the AI Act explicitly relies on a rights-based approach, also evidenced by its legal grounding in Article 16 TFEU, the CRA deploys specific mechanisms, especially with respect to enforcement procedures, which enable the EU Commission, under certain conditions, to leverage this piece of legislation to strengthen the enforcement of other EU legal acts intended to protect fundamental rights, such as *inter alia* the GDPR. A further and more hidden impact of the enforcement procedure analysed above is the potential “weaponization” of fundamental rights by the Commission to regulate the market thereby achieving “political” goals, as recent developments in EU cybersecurity law illustrate how non-technical risk factors are increasingly relevant in assessing the cybersecurity risk.¹¹⁹

Acknowledgments. This work was supported by the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU – Mission 4 Component 2, Investment 1.3 “Partenariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca”, MUR notice n. 341 del 15/03/2022, Project SERICS - SEcurity and RIghts in the CyberSpace, proposal: PE00000014, CUP: J33C22002810001, funded by MUR decree n. 1556 of 11/10/2022.

Competing interest. The author(s) declare that they have no conflict of interest.

¹¹⁸ The extra-territorial application of the CRA is likely to be a major factor in this sense. See on the so-called “Brussels effect” A Bradford, *The Brussels Effect: How the European Union Rules the World* (New York, Oxford University Press 2020). With specific regard to the success of the Brussels effect model within EU product safety legislation, notably the AI Act, see M Almada and A Radu, “The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy” (2024) *German Law Journal* 1.

¹¹⁹ See NIS2 Directive, Article 22; Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, point (3); Cyber Resilience Act, Articles 19(3); 54(2); 56(2).