EJLT European Journal of Law and Technology

Under Attack: The Discrepancy between Cybersecurity Regulation and Vehicle Regulation

Nynke E Vellinga[*] and Trix Mulder[**]

Abstract

Attack surfaces are increasing as products become ever more connected. This has been acknowledged by the European Commission in its 'A Europe: fit for the digital age' strategy and in recent legislative proposals. Most importantly, the Cyber Resilience Act (CRA) sets minimum cybersecurity requirements for products with digital elements. These requirements range from effective and regular tests to the dissemination of free security updates in case of a cybersecurity breach. This should ensure a base level of cybersecurity throughout the product's lifetime. Unfortunately, there is a catch: not all products with digital elements fall within the scope of the CRA. For instance, vehicles are not subject to the Act. The exclusion of this category of products with digital elements seems to be based on the premise that 'the sectoral rules achieve the same level of protection as the one provided for by this Regulation' (recital 14). This article challenges this premise: it explores the level of cybersecurity as laid down in the CRA and compares it to the level of cybersecurity ensured by the sectoral rules in vehicle regulation. Could this mean that in the future your smartphone will be more cybersecure than your car?

Keywords: cybersecurity; automated vehicles; Internet of Things; Cyber Resilience Act

[*] Faculty of Law, University of Groningen, the Netherlands, n.e.vellinga@rug.nl.

[**] Marian van Os Centre of Expertise Ondernemen, Hanze University of Applied Sciences, Groningen, the Netherlands, tr.mulder@pl.hanze.nl.

1. Introduction

Products are increasingly more connected: apps can be used to control washing machines, window blinds and your home's lights when on holiday. The cost of such convenience is that these connections also increase the attack surfaces of the devices. Consequently, your washing machine, blinds and lights are left more vulnerable to malicious attacks. At first glance, the consequences of a cybersecurity breach might be manageable. It is annoying when a washing machine stops working or runs through many more wash cycles than necessary, but this does not lead to substantial harm. When it comes to controlling the lights in one's home, a hacker can do more damage: powerful or flickering lights can cause great distress.[1] In addition, personal data might be accessed and used, for instance data relating to a person's address, daily routines (closing the blinds at night, opening them when leaving for work), etc. It could even lead to clues in a criminal investigation – did a suspect use the washing machine shortly after the crime, perhaps in an attempt to destroy incriminating evidence?

The increased vulnerability of these Internet-of-Things (IoT) devices can, when vulnerabilities are exploited, lead to roughly two types of risks: risks relating to data protection infringements; and risks concerning physical harm. The latter risk is of especially great concern in the automotive field: because vehicles, too, are becoming increasingly connected, therefore increasing attack surfaces, physical harm as a consequence of a cybersecurity breach is a genuine risk. The hacking of cars has already made the headlines in recent years, highlighting the risks for road users.[2]

The European Commission (EC) has acknowledged the cybersecurity risks to which connected devices are exposed. In 2022, the Commission proposed the Cyber Resilience Act (CRA) to address these risks and to ensure a uniformly high level of cybersecurity of products with digital elements.[3] These products include the

---

[1] The Center for Victims of Torture, 'The Hidden Harm' (2017) <www.cvt.org/wp-content/uploads/2017_hidden_harm_v2_1.pdf> accessed 8 September 2024.

[2] See for instance Andy Greenberg, 'Hackers Remotely Kill a Jeep on the Highway—With Me in It' (*The Verge*, 21 July 2015) <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>; Ronan Glon, 'Researchers hack Tesla's infotainment system and get paid upgrades for free' (*AutoBlog*, 4 August 2023) <www.autoblog.com/2023/08/04/researchers-hack-teslas-infotainment-system-and-get-paid-upgrades-for-free>; Umar Shakir, 'Tesla hacker discovers secret 'Elon Mode' for hands-free Full Self-Driving' (*The Verge*, 20 June 2023). <www.theverge.com/2023/6/20/23767041/tesla-hacker-elon-mode-hands-free-full-self-driving-autopilot>; Ed Garsten, 'Advanced Cars May Face Greater Risk Of Hacking, Cybersecurity Experts Warn' (*Forbes*, 26 April 2023) <www.forbes.com/sites/edgarsten/2023/04/26/cybersecurity-vulnerability-in-vehicles-is-escalating-as-software-engineer-shortage-grows/?sh=65ea15808ab2> accessed 8 September 2024.

[3] European Parliament 'Legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))', Recitals 4 and 11. The legislative procedure is ongoing at the

examples listed above: the washing machine, blinds and lights, and the smartphone (apps) controlling them. However, the CRA does not apply to cars, even though (connected) vehicles could cause significant damage when hacked.

The legal framework for connected vehicles has only recently been developed, in what seems to be a response to the headlines on car hacking.[4] As this framework has been developed mainly on the level of the World Forum for Harmonization of Vehicle Regulations of the United Nations Economic Commission for Europe and not so much on a European Union (EU) level, discrepancies between the cybersecurity requirements for IoT devices and connected vehicles are likely to arise.

This paper will therefore discuss this possible dichotomy in regulation of IoT devices and of connected cars, and the consequences of the difference in regulation will be explored. To this end, the legal framework for cybersecurity in vehicles is compared to the CRA and the framework it sets for the cybersecurity of one very familiar IoT device: the smartphone. Hereby, we can assess whether different levels in cybersecurity exist for smartphones and connected vehicles. We will identify the cybersecurity obligations of manufacturers, thereby narrowing the scope of this contribution to a key stakeholder in both the IoT and the automotive sector. In doing so, we aim to answer the question of whether regulation offers IoT devices the same level of cybersecurity as connected vehicles: is a smartphone going to be more cybersecure than a car?

2. Cybersecurity Terminology

Before exploring the CRA and automotive regulation, it is important to clarify what 'cybersecurity' means. Many definitions of this term can be found in literature.[5] These definitions do not necessarily align. The *Oxford English Dictionary* (OED) teaches us that cybersecurity is:

> 'Security relating to computer systems or the internet, esp. that intended to protect against viruses or fraud.'[6]

The OED also provides us an answer to the question of what 'security' is:

time of writing <www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html> accessed 8 September 2024.

[4] Scott McLachlan, Burkhard Schafer, Kudakwashe Dube, Evangelia Kyrimi and Norman Fenton, 'Tempting the Fate of the furious: cyber security and autonomous cars' (2022) 36 *International Review of Law, Computers & Technology* 181, 182–83.

[5] Dan Craigen, Nadia Diakun-Thibault and Randy Purse, 'Defining Cybersecurity, Technology Innovation Management Review' (2014) 4 *Technology Innovation Management Review* 13.

[6] Oxford English Dictionary <www.oed.com> accessed 8 September 2024.

> 'Freedom from danger or threat. The state or condition of being protected from or not exposed to danger; safety.'[7]

If we then zoom in on the definitions of cybersecurity that can be found in the different legal instruments discussed in this contribution, we find that the EU seems to view cybersecurity more as a process as opposed to the state or condition we found in the OED. The EU Cybersecurity Act reads:

> '"[C]ybersecurity" means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.'[8]

This definition treats cybersecurity as a collection of activities, an effort made, not as a state. The CRA refers to this definition from the Cybersecurity Act.[9] The CRA also provides a definition of 'cybersecurity risk':

> '[T]he potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident.'[10]

For a definition of 'cybersecurity' the CRA refers back to the definition above from the Cybersecurity Act. Therefore, this definition of 'cybersecurity' as a collection of activities to protect networks, systems, users and persons from cyberthreats seems to be the leading definition in the EU legislative context. Subsequently, a cyber threat constitutes:

> '[A]ny potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.'[11]

The definition of 'cybersecurity' used in EU legal instruments is, however, not aligned with the definition of this term in the automotive context. The leading definition of 'cybersecurity' in the automotive context can be found in Article 2.2 of UN Regulation 155:

---

[7] ibid.
[8] 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), art 2(1).
[9] ibid, art 3(3).
[10] ibid, art 3(37).
[11] Cybersecurity Act, art 2(8).

> '"Cyber security" means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components.'

This definition focuses on cybersecurity as a state. This state of cybersecurity can be achieved through the processes mentioned in UN Regulation 155 as well as UN Regulation 156, as will be discussed below.

One could therefore argue that the 'activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats' that define 'cybersecurity' in the EU legislation can contribute to reaching the state of cybersecurity within the context of the automotive context. For this contribution, we will therefore focus on cybersecurity as a state, in line with the UN Regulations and the OED, that can be achieved by certain activities and processes as mentioned in the Cybersecurity Act. Therefore, we combine the 'cybersecurity' definitions from both the automotive and EU legislation as well as the definitions provided in the OED.

3. The Cyber Resilience Act

In light of the increasing cybersecurity threats,[12] the EU harbours ambitions to spearhead initiatives aimed at ensuring secure digitalisation. One such initiative is the CRA.[13] The CRA is of particular interest for this contribution, in assessing the requirements for smartphone cybersecurity.

According to the EU, the CRA would guarantee:

- 'harmonised rules when bringing to market products or software with a digital component;
- a framework of cybersecurity requirements governing the planning, design, development and maintenance of such products, with obligations to be met at every stage of the value chain;
- an obligation to provide duty of care for the entire lifecycle of such products.'[14]

---

[12] Enisa, 'Enisa Threat Landscape 2023' (October 2023). <www.enisa.europa.eu/publications/enisa-threat-landscape-2023> accessed 8 September 2024.
[13] European Parliament 'Legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))' <www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html> accessed 8 September 2024.
[14] European Commission, 'EU Cyber Resilience Act. New EU cybersecurity rules ensure safer hardware and software' (July 2024) <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act> accessed 8 September 2024.

The CRA is anticipated to decrease the number of cybersecurity incidents, consequently reducing the cost of incident management and reputational damage for companies.[15] This, in turn, is expected to boost the trust that consumers and business customers have in companies and products, leading to an increased demand for products with digital elements, both within and outside the EU.[16] At the same time, consumers and users are set to benefit from more information when choosing a product with digital elements and from clearer instructions about its use. As a result of the decrease in security risks and incidents, consumers and citizens will experience improved protection of fundamental rights, such as data protection and privacy protection.[17] The CRA is committed to nurturing a culture of openness and resilience in response to cyber threats, and one of the key strategies to achieve this is by ensuring that users are adequately informed and safeguarded.

The CRA is designed to protect consumers and businesses that purchase or utilise products with a digital element.[18] The CRA applies to products with digital elements that are intended or could reasonably be expected to have a direct or indirect data connection to a device or network.[19] According to Article 3(1) CRA a product with a digital element is:

> '[A] software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.'

Article 3(5) CRA defines hardware as:

> '[A] physical electronic information system, or parts thereof capable of processing, storing or transmitting of digital data.'

In line with this definition, a smartphone is identified as hardware. The operating system of the smartphone and the apps that are used on the smartphone are considered as software under Article 3(4) CRA:

> '[T]he part of an electronic information system which consists of computer code.'

This means that the physical smartphone, its operating system, and the apps used, all need to comply with the CRA.

The CRA, however, does not apply to all products with digital elements. For instance, products with digital elements that are already covered by Regulation (EU) 2019/2144, which pertains to type-approval requirements for motor vehicles and

---

[15] CRA, recital 1.
[16] ibid.
[17] ibid.
[18] CRA, recital 10.
[19] CRA, art 2(1).

their trailers, systems, components and separate technical units intended for such vehicles, do not fall within the scope of the CRA.[20]

Therefore, these products are not subject to the essential requirements and conformity assessment procedures set out in the CRA. Regulation (EU) 2019/2144 is generally considered to already sufficiently establish the cybersecurity and safety benchmarks in the EU's automotive industry, since it introduces specific cybersecurity requirements, including the operation of a certified cybersecurity management system and software updates. It covers the policies and processes of organisations for cyber risks throughout the entire life cycle of vehicles, equipment and services.

3.1 Categories of Products

When establishing the cybersecurity requirements for smartphones, it is necessary to determine the category of products to which smartphones belong according to the CRA, as this has consequences for the conformity assessment procedures they have to undergo. The CRA classifies products with digital elements into three categories: the general category, and the more stringent categories 'important products with digital elements', which are subdivided into Class I and Class II, and critical products with digital elements.[21] According to the CRA, all products within its scope fall into the general category unless they meet the requirements of important products with digital elements, which are divided into Class I or Class II products, or critical products with digital elements.[22] Class I and Class II products are listed in Annex III of the CRA. The Commission is empowered to adopt delegated acts in accordance with Article 61 CRA to amend Annex III by including new categories of important products with digital elements, specifying their definitions, moving categories from one class to another, or withdrawing existing categories from the list.[23] Additionally, the critical products with digital elements listed in Annex IV of the CRA must comply with the stricter conformity assessment regime outlined in Article 32(2) CRA, similar to Class I important products with digital elements, provided they are not already regulated by the Cybersecurity Act.[24]

Important products with digital elements are those products where

> 'the negative impact of the exploitation of potential vulnerabilities in the product can be severe due to, amongst others, the cybersecurity-related functionality or a function carrying a significant risk of adverse effects in terms

[20] ibid, art 2(2).
[21] ibid, art 7, Annex III and Annex IV.
[22] ibid, art 3(1) in conjunction with art 7(1) (2).
[23] ibid, art 7(3).
[24] ibid, art 8 and recitals 44–46. Just as with Class II products, the products listed in Annex IV have a cybersecurity-related functionality and primarily perform a central system function or a function having the potential to disrupt, control or damage a large number of other products with digital elements through direct manipulation. However, these products are also covered by the Cybersecurity Act and are, therefore, mentioned separately in the CRA.

> of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data.'[25]

The products that meet these requirements are listed in Annex III, and are divided into Class I and Class II products, based on the criteria of Article 7 CRA. Important products meet one of the following criteria:

> (a) a digital product that primarily performs functions essential to the cybersecurity of other products, networks, or services;[26] or
>
> (b) a product that has the potential to disrupt, regulate, or inflict damage on a multitude of other products or can endanger the health and safety of a large number of individuals through direct interference, such as a central system function.[27]

Class I and Class II products require a more stringent assessment procedure compared to the general category of products with digital elements. The CRA employs the modules of Annex II of Decision 768/2008/EC[28] for the distribution of conformity assessment procedures within the CRA. The CRA thereby aligns with the cross-sectoral 'coherent basis' provided for product assessment procedure as laid down in this Decision.[29] The Decision provides for multiple different modules for different procedures of assessment, ranging from internal production control (Module A), to full quality assurance (Module H).[30] While the general category of product with digital elements can comply with an internal control procedure as provided for in Module A based on module A of the Decision as set out in Annex VIII of the CRA,[31] Class I and Class II products must adhere to stricter requirements.[32] For each category, the manufacturer may choose one of the prescribed assessment procedures. It is permissible to select the simplest assessment procedure, but the manufacturer is also free to opt for more stringent procedures. See Table 1 for a comprehensive overview of the different assessment procedures for the different categories of products with digital elements out of which the manufacturer must choose one. For critical products

---

[25] CRA, recital 43.
[26] CRA, art 7(2)(a).
[27] ibid, art 7(2)(b).
[28] Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC [2008] OJ L218/82.
[29] ibid, recitals 1–2.
[30] ibid, Annex II.
[31] CRA, art 32(1).
[32] ibid, art 7(1).

with digital elements, an option is available only if the requirements of Article 32(4)(a) are not fulfilled. This option is therefore indicated with an asterisk (*) in Table 1.

Procedure	Category
The internal control procedure (based on module A) set out in Annex VIII	General category
Where available and applicable, a European cybersecurity certification scheme as specified in Article 27(9) CRA	General category
The EU-type examination procedure (based on module B) set out in Annex VIII, followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII	General category, Important products (both Class I and Class II), Critical products
Conformity assessment based on full quality assurance (based on module H) set out in Annex VIII	General category, Important products (both Class I and Class II), Critical products
Where available and applicable, a European cybersecurity certification scheme pursuant to Article 27(9) CRA at assurance level at least 'substantial' pursuant to the Cybersecurity Act (Regulation (EU) 2019/881)	Important products in Class II, Critical products*
A European cybersecurity certification scheme in accordance with Article 8(1)	Critical products

Table 1: Procedures to demonstrate compliance.[33]

Compliance for Class II products must always be demonstrated through one of the three procedures listed for their category in Table 1.[34] Manufacturers of Class I products only have to demonstrate compliance through their two procedures when the manufacturer has 'not applied, or has only partially applied, harmonised standards, common specifications, or European cybersecurity certification schemes at assurance level at least "substantial" as referred to in Article 27, or where such standards, specifications, or schemes do not exist'.[35]

[33] ibid, art 31(1)–(4).
[34] ibid, art 32(3).
[35] ibid, art 32(2).

3.2 Smartphones

Annex III CRA provides a list of the categories of important products with digital elements that are classified either as Class I or Class II. Smartphones as such are not mentioned in Annex III. However, operating systems are considered to be a Class I category according to Annex III point 10 and fulfil the criterium specified under Article 7(2)(b) CRA. Consequently, one might anticipate that a smartphone, which possesses an operating system, would be classified as a Class I product. It should, however, be noted that most products with digital elements will incorporate some form of operating system.[36] In the previous version of the CRA, 'Operating systems for servers, desktops, and mobile devices' were considered to be Class II products. The legislator then renamed this category 'General purpose operating systems' and moved it to Class I. In the current version the category is renamed again to 'Operating systems'.

Unfortunately, the CRA does not define what is considered an operating system, although Recitals 43, 44 and 45 CRA provide clarification on this matter. The categories of products with digital elements, as referred to in Annex III CRA, should be interpreted as products that possess the core functionality of their respective types. The categories of products with digital elements listed in Class I of Annex III CRA either have a cybersecurity-related functionality or a function that carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements through direct manipulation, such as a central system function.[37] From this, we deduce that an operating system, as such, falls under Class I. Nevertheless, the operating system as a component of a singular smartphone fails to satisfy the prerequisites for this classification. Therefore, a smartphone is part of the general category of products with digital elements. As a result, we will concentrate on the requirements outlined in Article 6 CRA concerning the general category of products with digital elements as we examine the cybersecurity aspects for smartphones.

3.3 The Manufacturers

The CRA sets the implementation of compulsory cybersecurity requirements for manufacturers, importers and distributors of smartphones, and thus enables a base level of cybersecurity. These requirements range from effective and regular tests to the dissemination of free security updates in case of a cybersecurity breach.[38] The manufacturer is the entity responsible for developing, manufacturing or commissioning products with digital elements, and marketing them under their own name or trademark, either free of charge, for a fee or subject to monetisation.[39] Users of the product with digital elements that make substantial changes to the product with digital elements are also considered to be a manufacturer. Substantial changes

[36] CRA, recital 10.
[37] ibid, recital 43.
[38] CRA, annex 1, Part I, point 2(b) and Part II point 3.
[39] CRA, art 3(13).

are made when the changes affect 'the compliance of the product with digital elements with the essential requirements set out in Annex I, Part I, or which results in a modification to the intended purpose for which the product with digital elements has been assessed'.[40] Additionally, the CRA also refers to distributors[41] and importers.[42] These entities are responsible for introducing the smartphones into the internal market.

The CRA introduces two categories of obligations to manufacturers: a set of *ex ante* obligations that providers of products with digital elements must comply with before these products may be placed on the market;[43] and a set of *ex post* obligations that apply after the products have been placed on the market.[44]

3.4 Obligations for Manufacturers

As indicated in the introduction to this article, we will direct our attention towards the manufacturer of smartphones. This is attributed to the manufacturer's considerable impact in both the spheres of the IoT and the automotive industry. Here, we will discuss the obligations of the manufacturer of smartphones before these smartphones are placed on the market (*ex ante* obligations) and their obligations once the smartphones have been introduced onto the market (*ex post* obligations).

3.4.1 Ex Ante Obligations

Under the *ex ante* obligations, manufacturers of smartphones must ensure that their products comply with the essential requirements set out in Annex I CRA.[45] Smartphones should be designed, developed and produced in a manner that provides the necessary conditions for an appropriate level of cybersecurity, based on the risks involved.[46] Furthermore, the manufacturer must undertake an internal assessment of the cybersecurity risks associated with the product to demonstrate that the product meets the essential requirements in Annex I before it may be placed on the internal market.[47] See Table 1 for an overview of the assessment procedures concerning the different categories of products with digital elements. Based on this cybersecurity risk assessment, smartphones are required to be inherently secure when they are introduced to the market. For example, they should be free of any known

[40] ibid, art 3(30).
[41] ibid, art 3(17): 'a natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties'.
[42] ibid, art 3(16): 'a natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union'.
[43] eg CRA, art 13(1), (2), (12), (15), (18).
[44] eg CRA, art 13(4), (6), (9), (10).
[45] ibid, art 10(1).
[46] CRA, Annex I, Part I, point 1.
[47] CRA, art 13(1)–(2), Annex I, Part I, point 2.

vulnerabilities that could be exploited and they should have a pre-configured setting where security updates are automatically installed within a predetermined time frame.[48] This pre-configured setting needs a simple and intuitive opt-out mechanism to allow users to maintain control.[49] Furthermore, a provision should be incorporated that enables the product to be restored to its original state.[50]

These options bear resemblance to the responsibilities pertaining to data protection by design and by default, as stipulated by the General Data Protection Regulation (GDPR).[51] Data protection by design requires organisations to incorporate technical and organisational measures at the earliest stages of designing processing operations to ensure that privacy and data protection principles are safeguarded from the outset. Data protection by default mandates that organisations process personal data with the highest level of privacy protection.[52] This includes, for example, processing only the necessary data, maintaining short storage periods, and limiting accessibility, thereby ensuring that personal data is not made accessible to an indefinite number of individuals.[53] And, similar to the GDPR, the CRA states that these requirements must be proportionate to the level of risk posed by the products and software, and must reflect the state of the art.[54] For the CRA this necessitates that products with digital elements must undergo regular updates.[55]

Additionally, manufacturers are obligated to prepare an EU declaration of conformity in accordance with Article 13(12). When preparing this declaration, the manufacturer acknowledges his responsibility to make sure their product meets all the necessary standards outlined in Annex I CRA.[56] The manufacturer has the authority to evaluate its own products' compliance with the CRA.[57]

---

[48] ibid, Annex I art 1, Part I, point 2(a), (c).
[49] ibid.
[50] ibid, point 2(b).
[51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, art 25.
[52] Ari Ezra Waldman, 'Data Protection by Design? A Critique of Article 25 of the GDPR' (2021) 53 *Cornell International Law Journal*, Northeastern University School of Law Research Paper No 411-2021.
[53] GDPR, art 5.
[54] ibid, art 25(1) and CRA, art 6, Annex I, Part I, point 1, 2(a), (k), Part II point 7.
[55] CRA, art 6, Annex I, Part I, point 1, 2(a), (k), Part II point 7.
[56] ibid, art 28(1).
[57] CRA, recital 92: 'Conformity assessment of products with digital elements that are not listed as important or critical products with digital elements in this Regulation can be carried out by the manufacturer under its own responsibility… (...) The manufacturer retains the flexibility to choose a stricter conformity assessment procedure involving a third party.'

Furthermore, the manufacturer shall ensure that the smartphone is accompanied by the information and instructions set out in Annex II, in an electronic or physical form.[58] These requirements vary from information regarding a singular contact point for reporting cybersecurity vulnerabilities of the product, to details about the technical security support offered by the manufacturer. The latter includes the anticipated lifespan of the product, the end-date of technical security support, including the minimum duration during which users can expect to receive security updates.[59]

3.4.2 Ex Post Obligations

In compliance with the *ex post* obligations, the smartphone manufacturer is required to ensure that, following the cybersecurity risk assessment as stipulated in Article 13(8) CRA, any inherent vulnerabilities in the product are effectively mitigated throughout the manufacturer's predetermined support period. The support period should be a minimum of five years, unless the expected lifespan of the product is less than five years. However, such exceptions usually occur only in specific circumstances.[60] For instance, the CRA cites the example of a contact-tracing app designed for use during a pandemic, where its lifespan may be limited to the duration of the pandemic.[61] The manufacturer determines the support period based on the reasonable time during which a user is expected to utilise the product, considering its functionality and intended purpose, and during which users can expect to receive security updates.[62]

The protection the CRA offers is not limited to the development phase of a smartphone as it extends into the expected lifetime of the product via the support period determined by the manufacturer.[63] When it comes to the smartphone's operating system and the apps, the manufacturers are allowed, in instances where they have introduced successive iterations of a software product on the market, to furnish security updates exclusively for the most recent version of the software product. However, they may only do so if the users of preceding versions of the software product are able to access the latest version at no additional cost, and are not subjected to substantial supplementary expenses in order to modify the hardware and software environment in which they use the original version of that product.[64]

---

[58] CRA, art 13(18).
[59] CRA, Annex II points 2 and 7.
[60] CRA, art 13(8) and recital 61.
[61] CRA, recital 61.
[62] CRA, art 13(8).
[63] CRA, art 13(8) states: 'Manufacturers shall determine the support period so that it reflects the length of time during which the product is expected to be in use, taking into account, in particular, reasonable user expectations, the nature of the product, including its intended purpose, as well as relevant Union law determining the lifetime of products with digital elements.'
[64] CRA, art 13(10).

Additionally, manufacturers are obligated to promptly report any vulnerabilities in their digital products that are being exploited, as soon as they become aware of such issues.[65] These notifications should be directed to the national Cyber Security Incident Response Team (CSIRT), designated as coordinator in accordance with the NIS2 Directive[66] and to the European Union Agency for Cybersecurity (ENISA).[67] According to Article 12(1) NIS2 Directive a CSIRT will serve as a trusted intermediary, facilitating necessary interactions between the individual or entity reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or services. ENISA shall set up a single reporting platform to make reporting vulnerabilities easily accessible. ENISA will manage and maintain the day-to-day operations of this platform. The design of this platform will let Member States and ENISA create their own electronic points for sending messages.[68]

Now that we have established the legal framework of cybersecurity in relation to smartphones, it is appropriate to shift our focus towards exploring the concept of cybersecurity within the context of motor vehicles.

4. The Regulation of Cybersecurity in Motor Vehicles

When it comes to safety and security of vehicles that drive on the public roads of the EU, intertwining requirements can be found in legislative instruments at the EU and UNECE level. These instruments concern specific (cyber) security and safety requirements that need to be fulfilled in order to have a (type) of vehicle approval granted by the approval authority under the EU Type-approval Regulation.[69] Only with such an approval are vehicles allowed to be used on the EU's public roads.

[65] ibid, art 14(1).
[66] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2019] OJ L333/80.
[67] CRA, art 3(51) and Directive (EU) 2022/2555.
[68] CRA, art 16(1).
[69] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC [2018] OJ L151/1.

The EU General Safety Regulation (GSR)[70] sets out technical requirements for the type-approval of all new motor vehicles as of 6 July 2022.[71] These include requirements on an event data recorder, intelligent speed assistance, emergency stop signal, and specific requirements for (fully) automated vehicles.[72] The GSR itself does not contain any substantive cybersecurity requirements. It does, however, state that:

> 'The connectivity and automation of vehicles increase the possibility for unauthorised remote access to in-vehicle data and the illegal modification of software over the air. In order to take into account such risks, UN Regulations or other regulatory acts on cyber security should be applied on a mandatory basis as soon as possible after their entry into force.'[73]

The UN Regulations referred to here are UN Regulation 155 (R155)[74] and UN Regulation 156 (R156).[75] R155 requires the manufacturer of the (type of) vehicle for which approval is requested to have a cybersecurity management system, whereas R156 requires a software update management system (SUMS).

The SUMS should ensure the safe and secure updating of the software of the vehicle. It entails 'a systematic approach defining organisational processes and procedures' in order to comply with R156.[76] R156 requires several processes to be in place, including a process to inform the vehicle user about the update (Article 7.1.1.11), and a process by which the manufacturer ensures that software updates are 'protected to reasonably prevent manipulation before the update process is initiated' (Article 7.1.3.1). The update processes have to be protected so as to 'reasonably prevent them being compromised, including development of the update delivery system'.[77]

---

[70] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (hereinafter GSR) [2019] OJ L325/1.

[71] GSR, art 19.

[72] ibid, arts 6 and 11.

[73] GSR, recital 26.

[74] UN Regulation No 155: Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. ECE/TRANS/WP.29/2020/79 (UN R155).

[75] UN Regulation No 156: Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system. ECE/TRANS/WP.29/2020/80 (UN R156).

[76] ibid, art 2.5.

[77] ibid, art 7.1.3.2.

This way, the cybersecurity of the vehicle during the update process should be safeguarded.

R155 also requires processes safeguarding the cybersecurity of vehicles. The type-approval required as cyber security management system (CSMS) is defined as:

> '[A] systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyberattacks.'[78]

These processes are very strongly geared towards preventing unauthorised access to the vehicle's systems.[79] They include processes to manage the manufacturer's cybersecurity (Article 7.2.2.2(a)), processes for the treatment of risks (Article 7.2.2.2(c)−(d)), and processes for the testing of the cybersecurity of a vehicle type (Article 7.2.2.2(e)).There should also be processes in place to 'monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cybersecurity measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified'.[80] The manufacturer must have these processes in place during the 'post-production phase'.[81] This phase ends when there are no longer any operational vehicles of the specific type.[82] The approval authority can audit the conformity of production with both the SUMS and CSMS and has a strong tool available to enforce the rules on the SUMS and CSMS: non-conformity can lead to withdrawal of the granted approval.[83]

In addition to the binding legal framework of the GSR and the UN regulations, non-binding standards can contribute to the cybersecurity of vehicles. ISO/SAE standard 21434:2021 should be mentioned here, as it 'specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces'.[84] Although this standard is not legally binding, it can nevertheless have a substantial impact on the vehicle's cybersecurity as industry can decide to adhere to this standard. This could be a sensible approach to managing liability risks. It should be noted that the vehicle approval authority has the competence to refuse approval of a vehicle type when, despite meeting all mandatory requirements, it is deemed unsafe for use on

---

[78] UN R155, art 2.3.
[79] It could be argued that this is not enough of a protection offered by the CSMS. See more extensively: Nynke Vellinga, 'Connected and vulnerable: cybersecurity in vehicles' (2022) 36(2) *International Review of Law, Computers & Technology* 161.
[80] UN R155, art 7.2.2.2(g).
[81] ibid, art 7.2.2.1. UN R156 implies the same regarding the SUMS processes.
[82] ibid, art 2.7.
[83] ibid, art 10 and UN R156, art 10.
[84] ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering.

public roads.[85] In light of this, compliance with a non-binding standard could therefore also prove to be important in the context of the type approval.

5. The Role of Regulation in an Open Cybersecurity Culture

The CRA is structured to enhance the digital environment's security for all parties involved. This includes users, as IoT devices have become part of everyday life.[86] The CRA primarily tackles two significant issues that add extra costs for users and society[87] – not only financially, but also in terms of violating human rights, such as privacy and data protection.[88] The first issue raising these costs is the widespread low level of how many vulnerabilities arise, and the inconsistent and insufficient provision of security updates to address them.[89] The second issue is the users' limited understanding and access to information, which obstructs their ability to choose products based on their cybersecurity features.[90] Both issues can lead to, for instance, personal data breaches. The CRA aims to correct the second issue by requiring manufacturers to reveal cybersecurity aspects that are relevant to customers, and the first via the essential cybersecurity requirements for products with digital elements as listed in Annex I CRA, thereby ensuring a base level of cybersecurity for these products. In addition, mandatory vulnerability reports combined with providing manufacturers with the option to report vulnerabilities voluntarily to CSIRT or ENISA can enhance the future cybersecurity of products with digital elements, even when misuse has not been proven.[91] It could be argued that this contributes to a more open cybersecurity culture. ENISA describes how, among other legal instruments, the CRA encourages the development of Information Sharing and Analysis Centers (ISACs).[92] These centres collect data on cyberthreats and provide for a 'two-way sharing of information between the private and the public sector about root causes, incidents and threats,

[85] Regulation (EU) 2018/858, art 26(5).
[86] Waleed Ejaz, Alagan Anpalagan, Muhammad Ali Imran, Minho Jo, Muhammad Naeem, Saad Bin Qaisar and Wei Wang, 'Internet of Things (IoT) in 5G Wireless Communications' (2016) 4 *IEEE Access* 10310.
[87] CRA, recital 1.
[88] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore and Stefan Savage, 'Measuring the cost of cybercrime' (2013) *The economics of information security and privacy* 265; Cristina Cocito and Paul De Hert, 'The Transformative Nature of the EU Declaration on Digital Rights and Principles: Replacing the Old Paradigm (Normative Equivalency of Rights)' (2023) 50 *Computer Law & Security Review* 3.
[89] CRA, recital 1 and Enisa Threat Landscape 2023 <www.enisa.europa.eu/publications/enisa-threat-landscape-2023> accessed 8 September 2024.
[90] CRA, recital 1.
[91] CRA, art 15.
[92] ENISA, Information Sharing and Analysis Centers (ISACs) <https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/information-sharing-and> accessed 9 June 2024.

as well as sharing experience, knowledge and analysis'.[93] ISACs can thereby foster an open cybersecurity culture. The automotive field is also familiar with ISACs.

Although, in line with their nature as vehicle safety requirements, the UN R155, UN R157 and the GSR do not explicitly foster an open cybersecurity culture, the automotive sector has developed several cybersecurity initiatives, including the an ISAC: the Auto-ISAC. This initiative is described as 'an industry-driven community to share and analyse intelligence about emerging cybersecurity risks to the vehicle, and to collectively enhance vehicle cybersecurity capabilities across the global automotive industry, including light- and heavy-duty vehicle OEMs, suppliers and the commercial vehicle sector'.[94] Lucid, Mazda and Ford are among its members.[95] In 2016, Auto-ISAC published its Best Practice Executive Summary on cybersecurity.[96] The European Automobile Manufacturers Association (ACEA), representing 15 major Europe-based automobile manufacturers,[97] is also taking initiative on cybersecurity; it published its Principles of Automobile Cybersecurity in 2017.[98]

6. Regulation of Motor Vehicles and Protection under the CRA: how Cybersecure are Smartphones and Motor Vehicles?

Our overview of some of the key aspects of both the CRA and the UNECE vehicle regulations shows that the EU and UN legislators acknowledge the importance of the regulation of cybersecurity. However, the routes chosen by the legislators to ensure the cybersecurity of IoT devices and motor vehicles are different. A clear difference lies, for instance, in the requirement for a CSMS in the automotive field, whereas the CRA does not refer to such a CSMS. In this section, we will explore these differences in approach further, to assess whether the cybersecurity protection in the IoT field and the automotive field differ from one another.

One of the differences in approach that stands out is the phrasing of cybersecurity obligations and requirements in UN R155, UN R156 and in the CRA. Whereas the CRA sets out requirements for the (IoT) product itself, UN R155 and UN R156 are focused on obligations for the manufacturer that should ensure a cybersecure vehicle. In relation to both the cybersecurity of smartphones and the cybersecurity of automated vehicles, the legislator has placed the onus of ensuring the cybersecurity on the manufacturer of IoT devices and cars respectively. This underlines cybersecurity as an essential element of product safety: in product safety regulation

[93] ibid.
[94] <https://automotiveisac.com> accessed 8 September 2024.
[95] ibid.
[96] Best Practices <https://automotiveisac.com/best-practice-guides> accessed 10 June 2025.
[97] ACEA Members, <www.acea.auto/acea-members> accessed 8 September 2024.
[98] ACEA Principles of Automobile Cybersecurity (September 2017) <www.acea.auto/files/ACEA_Principles_of_Automobile_Cybersecurity.pdf> accessed 8 September 2024.

the safety of a product is also mainly an obligation of manufacturers.[99] The cybersecurity obligations of manufacturers of smartphones and vehicles do not end when their products have left the manufacturing process. These obligations stretch into the lifetime of the products. This again aligns with the revised Product Liability Directive, which no longer takes the moment a product was put into circulation as the moment at which to assess whether the product was defective, leading to liability of the manufacturer.[100] Instead, it takes the moment the manufacturer loses control over the product as the moment at which it should be assessed whether the product was defective and liability can be established.[101] This shows, together with the CRA and the vehicle cybersecurity framework, that the EU legislator is adapting to a new digital age in which a producer can ensure its product's safety – whether smartphone or car –well beyond the moment it has left production. It is therefore reasonable to extend the cybersecurity obligations of manufacturers beyond the manufacturing stages of a product's lifetime.

It should be noted, however, that the obligations of manufacturers of smartphones and manufacturers of cars do not stretch necessarily to the same amount. The manufacturers of smartphones will have to determine their support period, during which they will have to fulfil their cybersecurity obligations.[102] This support period has to reflect the duration for which the product is anticipated to be utilised, considering reasonable user expectations, the nature of the product, including its intended purpose, as well as pertinent EU legislation determining the lifespan of products with digital elements.[103] For smartphones with an expected lifetime of five years or more, the support period must be at least five years.[104] The support period is a subjective standard, and the actual lifetime of a product could extend well beyond it. Besides, the manufacturer of a smartphone could find itself incentivised to limit expectations

[99] See for instance 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 (General Product Safety Regulation) [2023] OJ L135/1, art 9.

[100] Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM/2022/495 final, art 6(1)(e).

[101] Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM/2022/495 final, recital 37: 'However, since digital technologies allow manufacturers to exercise control beyond the moment of placing the product on the market or putting into service, manufacturers should remain liable for defectiveness that comes into being after that moment as a result of software or related services within their control, be it in the form of upgrades or updates or machine-learning algorithms. Such software or related services should be considered within the manufacturer's control where they are supplied by that manufacturer or where that manufacturer authorises them or otherwise influences their supply by a third party.'

[102] CRA, art.13(8).

[103] ibid.

[104] ibid and recital 61.

on the support period to the legal obligation of five years so as to ensure it only briefly has to fulfil its cybersecurity obligations. Manufacturers of automated vehicles, however, have to fulfil their obligations during a timeframe for which an objective standard is used: their cybersecurity obligations only end when there are no operational vehicles of that specific type left.[105] Consequently, cars could be required to be protected from the exploitation of cybersecurity vulnerabilities significantly longer than smartphones. It should be noted, however, that both in relation to smartphones and AVs, cybersecurity and the availability of regular security updates could be used as a marketing strategy to stand out from the competition.

There are more noteworthy differences in the cybersecurity regulation of IoT devices and of automated vehicles. Whereas for the vehicle cybersecurity framework all cars are the same, which can be explained from the same risks they pose, the CRA categorises the IoT devices based on the risks they pose. Smartphones are not seen as posing a particularly high risk, therefore they fall within the scope of the general category of products with digital elements. Products posing a higher risk fall within the scope of important and critical products with digital elements. To ensure their cybersecurity, these important and critical products are subject to more stringent assessment procedures. This risk-based approach is similar to the risk-based approach applied in the categorisation of AI systems in the AI Act.[106] Similarly, the AI Act qualifies automated vehicles as high-risk AI systems.[107] It requires these high-risk AI systems to undergo third-party assessment, in line with the third-party assessment that automated vehicles have to undergo to acquire type approval.[108]

Nevertheless, vehicles fall outside of the scope of the CRA and AI Act.[109] The regulation of vehicle safety, including vehicle cybersecurity, is considered to be part of the 'old legislative framework', which is characterised by product-specific, very detailed legislation. For example, the specifics of crash test dummies are regulated.[110] The 'new legislative framework', on the other hand, allows for a less technically detailed, less product-specific approach.[111] The AI Act and CRA are both considered

[105] UN R155, art 2.7.
[106] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] OJ L2024/1689.
[107] ibid, arts 3(1) and 6(1), and Annex I.
[108] ibid, art 16(f), art 43 and Type-approval Regulation.
[109] ibid, art 2(2). Annex I Section B.
[110] See, eg, UN R94.
[111] Council Resolution of 10 November 2003 on the Communication of the European Commission 'Enhancing the Implementation of the New Approach Directives' OJ C 282, 25.11.2003, p 3–4; Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC.

to be part of this new legislative framework.[112] Legal instruments from the new and the old legislative frameworks could potentially collide or overlap. Therefore, vehicle safety has been left out of the scope of the new legislative framework.[113] Moreover, vehicle safety has traditionally been regulated at a United Nations (UN) level, through the aforementioned UN R155, for instance. It is not only the EU legislator that shapes the vehicle safety framework.

A possible negative consequence of this is that the IoT cybersecurity framework and the vehicle safety framework develop differently, which could lead to divergent cybersecurity requirements and potentially a lower level of cybersecurity required from vehicles than from smartphones. The EU, through the Member States present at the UN forum deciding on vehicle safety, should prevent this from happening. If necessary, the EU could decide to step in and lay down additional cybersecurity requirements in an instrument like the GSR.

When taken at face-value, the CRA and the vehicle cybersecurity framework might appear not much more than safety requirements. This, however, is too limited of a view: both the CRA and the vehicle cybersecurity framework contribute to upholding fundamental values. This includes the right to privacy (CRA) and the right to life (vehicle cybersecurity). The importance of the CRA and the vehicle cybersecurity legislation should therefore not be underestimated. It is important to note that other legal instruments also have the potential to contribute to the cybersecurity of smartphones and cars alike.

7. Beyond CRA, UNECE R155 and R156

So far in this article, the CRA and the two UNECE regulations have been given centre stage. However, the cybersecurity of IoT devices and motor vehicles is also influenced by other legislative instruments. This mainly concerns instruments that provide some form of consumer protection. For instance, in an indirect manner, the Product Liability Directive can provide an incentive to manufacturers and programmers alike to only bring cybersecure products on the market.[114] This becomes even more apparent in the proposal of the European Commission on a revision of the product

---

[112] Mohammed Raiz Shaffique, 'Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark?' (2024) 54 *Computer Law & Security Review* 1, 8.

[113] See the original EC proposal under 1.2: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final. See also Martin Ebers, Veronica Hoch, Frank Rosenkranz, Hannah Ruschemeier and Bjorn Steinrötter, 'The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' (2021) *MPDI* 589.

[114] 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 L210/29.

liability regime.[115] The proposal, which has now entered into force as Directive 2024/2853, includes explicit reference to 'safety-relevant cybersecurity requirements' as a factor that should be taken into consideration when assessing the defectiveness of a product.[116] Therefore, this tort law incentive is relevant to both smartphone manufacturers as well as motor vehicle manufacturers.

Two consumer protection instruments, Directives 2019/771 and 2019/770, contribute to maintaining a cybersecure state of vehicles and smartphones alike. Just as in the CRA, which offers protection for products with digital elements during the support period,[117] these Directives require sellers to provide security updates for products necessary to keep consumer products in conformity with the initial purchase contract.[118]

The General Product Safety Regulation came into effect on 13 December 2024.[119] This successor to the General Product Safety Directive specifically mentions that 'when required by the nature of the product, the appropriate cybersecurity features necessary to protect the product against external influences, including malicious third parties, where such an influence might have an impact on the safety of the product, including the possible loss of interconnection' should be taken into account when assessing the safety of a product.[120] This, too, is relevant for the cybersecurity of both smartphones and automated consumer vehicles.

As mentioned above, the AI Act does not apply directly to automated vehicles. Even though these vehicles will likely depend on AI, and automated vehicles could be classified as high-risk AI systems,[121] only new delegated acts to the Type-approval Regulation[122] and new implementing acts to the GSR[123] will have to align with the

---

[115] Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final.
[116] ibid, art 6(1)(f).
[117] CRA, art 13(8) states: 'Manufacturers shall ensure, when placing a product with digital elements on the market, and for the support period, that vulnerabilities of that product, including its components, are handled effectively'.
[118] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28, art. 7(3) and Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1, art 7.
[119] 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 (General Product Safety Regulation) [2023] OJ L135/1.
[120] ibid, art 6(1)(g).
[121] AI Act, art 2(2) jo. Annex II, Section B under 18−19.
[122] ibid, art 107.
[123] ibid, art 109.

high-risk AI system requirements of Chapter III, section 2 AI Act. This includes requirements on cybersecurity.[124]

Additionally, the NIS 2 Directive[125] as well as the ITS Directive[126] contain rules on the security of the networks used for vehicles to operate, including matters related to cybersecurity. As neither instrument specifically addresses the cybersecurity of the vehicle itself, focusing rather on the networks used, it suffices here to simply mention these Directives.

8. Conclusion

In this contribution, we have set out to answer the question whether an IoT device, in this case a smartphone, offers a higher level of cybersecurity than an automated vehicle. On the basis of the regulatory instruments studied here, this question cannot be answered fully. Whether the cybersecurity of a smartphone is better than that of an automated vehicle highly depends on how the CRA, UN R155 and UN R156 are interpreted by the parties involved. However, the CRA and the automated vehicle cybersecurity regulations clearly offer a level of cybersecurity for both smartphones and automated vehicles. This is a significant step forward in bringing only cybersecure products to the market and cybersecure vehicles on the road, as until recently cybersecurity of both IoT devices and automated vehicles were not, or only minimally, regulated. However, there is no guarantee that IoT devices and automated vehicles are completely cybersecure. This is, for instance, the case when a smartphone is connected to the vehicle's entertainment system, as there is no isolation of safety-critical systems from non-safety-critical systems in a vehicle. This could unlock the possibility for hackers to make their way via the smartphone into, for instance, the vehicle's steering system. The cybersecurity of the automated vehicle, which requires third-party assessment, is thereby potentially compromised by the smartphone that has undergone self-assessment by its manufacturer. Therefore, the legislator should remain vigilant to avoid vulnerabilities that could ultimately compromise the right to life and right to privacy.

---

[124] ibid, art 15.

[125] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

[126] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.