Cybersecurity of consumer products against the background of the EU model of cyberspace protection

Cezary Banasiński¹ and Marcin Rojszczak ²,*

¹Faculty of Law and Administration, University of Warsaw, Warsaw, Poland and ²Faculty of Administration and Social Sciences, Warsaw University of Technology, Warsaw, Poland

*Correspondence address: Faculty of Administration and Social Sciences, Warsaw University of Technology, pl. Politechniki 1, 00-661 Warsaw, Poland. E-mail: marcin.rojszczak@pw.edu.pl

Received 26 February 2020; revised 19 February 2021; accepted 6 April 2021

Abstract

The entry into force of Regulation 2019/881 heralded a new stage in the construction of the EU cybersecurity model. At present, at the level of both EU institutions and individual Member States, preparatory work is underway to create the first ICT certification programmes relating to the area of cybersecurity. To date, the role of national competition and consumer protection authorities in helping to build a coherent cybersecurity model has not been sufficiently highlighted. The problem of the cybersecurity of products intended for the consumer market is a pressing issue. Furthermore, its significance is growing due in no small part to the increasing number of so-called smart connected consumer products and the mass expansion of the IoT market. As a result, threats to security or privacy increasingly stem not from cyberattacks on leading providers of online services but from the exploitation of vulnerabilities in commonly-used consumer products. This article aims to discuss the possible role of competition and consumer protection authorities in shaping a future model of EU cybersecurity. We discuss the existing mechanisms in EU law that allow supervisory authorities to shape the consumer product safety market and consider whether these measures can also be considered adequate for cybersecurity purposes. Particular attention is paid to identifying what legislative steps would be necessary to effectively synthesize the new EU cybersecurity regulations (including the planned cybersecurity certification framework) with existing consumer product safety laws.

Key words cybersecurity; consumer protection; general product safety; certification framework; misleading commercial practices

Introduction

Building a coherent cybersecurity model is an important element of the EU’s single digital strategy. Work in this area parallels the reform of EU data protection regulations and the electronic communications framework. The issue of properly protecting IT systems and networks has gained greater importance over the years mainly due to the growing scale of cyber threats and the negative effects they cause. For years, this area has been outside the mainstream interest of the EU legislature—mainly as a result of insufficient interest from Member States in strengthening cooperation in this sphere and a lack of understanding that, due to the global reach of cyber threats, protective measures taken only at a national level are not an optimal solution.

The discussion of effective mechanisms for protecting cyberspace must encompass not only technical issues but also legal and geopolitical aspects. Cyberspace is an increasingly important element in the functioning of many economies which naturally raises questions about whether and how certain activities emerging in this space can
be regulated by public authorities. Individual states prioritize protecting critical infrastructure in order to ensure continuity of services to the public. For this reason, at the level of state cybersecurity, it is particularly important to define minimum security measures and to agree on common procedures (plans) for responding to the most serious incidents. On the other hand, from the viewpoint of individual entrepreneurs, it is equally important to ensure protection of the information they process, e.g., business secrets and customer data—especially against the threat of tampering or disclosure. The last level of this analysis relates to small businesses and individual users. They have the most limited possibilities for effective protection yet are being increasingly targeted by cybercriminals. This applies especially to home users who often not only lack adequate knowledge in the field of IT security but are also largely dependent on security mechanisms made available to them by the suppliers of the products and services they use.

It is not possible to separate the particular areas of the threats mentioned above; their negative impact on a state’s cyber infrastructure can certainly also have an adverse effect on the security of the systems and networks of individual entrepreneurs. Similarly, the negative consequences of attacks on the infrastructure of service providers often also affect individuals who have been using these services. As a result, when designing a legal regime intended to strengthen the cyberspace area, it is necessary to take into account not only the obligations required for given categories of obliged entities but also the relationships between particular cybersecurity levels. The regulations introduced thus far have been aimed mainly at increasing the degree of protection at the first two levels, i.e., of the state and entrepreneurs that have a critical infrastructure, possibly including operators of essential services and digital service providers. Of course, the enactment of these provisions also indirectly contributes to an increase in user security even if it is just a reduction in the risk of theft of data processed by these entrepreneurs.

However, a separate issue is the problem of promoting the principles of so-called cyber hygiene which should be understood as “simple, routine measures that, where implemented and carried out regularly by citizens, organisations and businesses, minimise their exposure to risks from cyber threats” (recital 8 in [1]). Both ENISA publications [2] and international standards dedicated to the IT security area (see definition introduced in [3]) emphasize the importance of cyber hygiene in building a comprehensive cybersecurity model. Researchers have emphasized the importance of users’ knowledge and behaviour to mitigate cybersecurity risks [4]. But most cyber hygiene practices [see e.g. p. 38 in 5] cannot not be effective if the technologies that are used are not designed with IT security requirements in mind. Therefore, it should not come as a surprise that the implementation of cyber hygiene programmes may also affect consumer purchasing decisions.1

In recent years, the number of IoT devices used in households has risen dramatically [7]. These include not only typical computer devices (e.g. access routers, printers and IP cameras) but also home appliances (television sets, vacuum cleaners, refrigerators, etc.) and health care equipment (blood pressure monitors, glucose meters, insulin pumps, etc.). More and more often, experts are revealing attacks that are directly targeting the security of consumer devices (e.g. botnet networks, consisting of home Internet routers,3 or IP cameras4). The actual level of user cybersecurity depends not only on the measures taken by service providers and their overall adherence to cyber hygiene principles but also on the security of products operating in the end users’ home network. A single device, such as a printer with unresolved security vulnerabilities, can pose a threat to the security of the entire home network.

The mass ‘networking’ of various consumer devices results in a multiplication of possible risks affecting the user and the creation of dozens of new attack vectors [p. 719–20 in 12]. The question arises as to how it is possible for people who often do not understand modern technology well enough to properly configure the privacy settings on their social networking site account ensure the security of up to perhaps ten different types of devices they use on a daily basis. The scale of this problem only increases if one considers that, nowadays, hundreds of different technologies are used in the area of IoT device security [13]. Of course, this problem can simply be reduced to the issue of making sound purchase decisions. However, there are at least two reasons why it would be inappropriate to adopt such a solution. First, the user—even if familiar with the parameters of the purchased product or service—cannot predict errors that may show up later. Plenty of security vulnerabilities are discovered years after a given technology has been developed. Moreover, the occurrence of some vulnerabilities could not have been foreseen at the time of the product launch. Since assessment of the IT security level of a given technology can change over time, the consumer cannot simply choose a ‘secure product’. Secondly, the launch of products that do not offer basic types of security safeguards or for which the manufacturer does not provide regular security patches not only has a negative impact on the buyer of this product but, in the case of popular consumer products, it is also a threat to the operators of other systems and networks. Criminals can take advantage of easy access to a large number of vulnerable devices in order to create a new attack vector targeting, for instance, a critical infrastructure provider [13]. Therefore, it is impossible to create a complex cybersecurity model without proper regard for the security of products that are at home users’ disposal.

Unfortunately, the EU and national legislatures have thus far not made a comprehensive attempt to develop minimum IT security standards to be met by new products and services targeted at the consumer market. The first regulations of this type were adopted in California in the United States. Even though they are local in their reach, it is expected that, due to the importance of California’s economy, these requirements will eventually be applied to all products sold in America. Although the regulations that were adopted do not impose many detailed obligations, they require, for example, that connected consumer products be pre-programmed with an individual password that is unique for each of the items produced [14].

In the absence of specific regulations, the necessity to introduce obligations regarding minimum IT security standards in the field of consumer protection law has stimulated much debate. Such a

---

1 As was proposed in the roadmap presented by the Dutch Government: ‘The primary objective of awareness campaigns is to make consumers and SMEs aware of the digital security risks of IoT devices, how they can be addressed and which government measures can help them do so. Insights [... ] will also be used to ensure that users know what they must do (what their options are) to make the right purchase decisions and use hard- and software correctly’ [6].

2 In fact, cybersecurity of home medical appliances is one of most pressing aspects to be considered in discussion of the security of smart devices. See e.g. [8, 9].

3 ‘Gafgyt’ is an example of malicious malware that is made of hacked home routers. See [10].

4 An example could be ‘Persirai’, a botnet network made of hacked IP cameras. Trend Micro has detected about 120 000 cameras vulnerable to this type of attack. Details presented in [11].
concept is interesting for several reasons. First of all, it affords an opportunity to utilize a mature legal framework, complemented by extensive case law of both national consumer protection authorities and courts, including the ECJ. Secondly, it makes it possible to transfer, even partially, liability for the level of IT security of products to their manufacturers which, at the same time, would avoid involving individual users in complicated legal disputes. Thirdly, it increases the level of cybersecurity of all products on the market; in this way, the concept horizontally affects the entire market by shaping appropriate IT security norms and standards.

The purpose of this contribution is to discuss to what extent existing consumer protection regulations may be used to reduce threats that may potentially and adversely affect the users of smart connected products. Section 2.1 discusses the current EU cybersecurity framework with particular attention being paid to regulations that apply to the security of connected products. Section 2.2 considers the problem of protecting consumer products that cannot simply be handled by the proper application of data protection law. Without diminishing the importance of regulations already laid down in this area, the authors are of the opinion that these provisions do not allow for a comprehensive solution to the problem. Therefore, section 2.3 is an introduction to consumer protection law both from a horizontal perspective (the definition of general product safety and a defective product) and in terms of sector-specific regulations (radio equipment safety). These considerations are supplemented in the subsequent section (2.4) with reference to unfair market practices possibly relating to incomplete or misleading information provided by manufacturers about the features of their products, including cybersecurity aspects.

On the basis of the conclusions drawn from an analysis of the possible sources of requirements, Section 3 discusses extending the existing definition of product safety and synthesizing consumer protection regulations with the current EU framework for cybersecurity certification of ICT products. A challenging problem in the field of consumer product cybersecurity is ensuring an appropriate level of security throughout the products’ life cycle, including the maintenance stage; Section 4 discusses this issue. The article ends with a summary restating the most important conclusions and recommendations concerning further enhancement of the EU cybersecurity model.

**Sources of requirements for connected consumer products in EU law**

**The EU cybersecurity model**

The issue of cyberspace protection has been on the agenda of EU institutions for almost 20 years. Most of the work, however, has resulted simply in policy papers that establish a course of action and confirm the significance of the problem yet are devoid of binding force [15]. Although ENISA—an agency dedicated to providing expert assistance in the area of IT security—was established in 2004, until fairly recently, its competences did not allow it to take more active steps relating to the standardization of the cybersecurity area in the EU. This situation has changed significantly in recent years given the adoption of Directive 2016/1148 [16] (the so-called NIS Directive) and Regulation 2019/881 (the so-called Cybersecurity Regulation). In particular, the inclusion of the directive in national legal systems was an important stage in creating the EU cybersecurity model. In this way, the European Union has, for the first time, introduced a mechanism that allows for cross-border exchange of information on the most serious incidents in cyberspace and also makes it possible to coordinate protective activities and prevent similar threats in the future.

Regarding the construction of a cybersecurity system, the NIS Directive can be considered as an extension of previous regulations on the EU model of critical infrastructure protection. To a large extent, the obligations defined in both regimes are addressed to the same group of obliged entities, i.e. operators of essential services and operators of critical infrastructure. In the case of the NIS Directive, the list of these also includes operators of key digital infrastructure, in particular internet exchange points (IXP), DNS service providers, and TLD name register operators. In reality, however, the exact group of entities covered by the requirements of the directive arises from decisions issued by relevant national authorities. On the one hand, such a solution makes it possible to better adapt the protection model to the conditions of the local market; on the other hand, it creates the risk that entities with a similar profile (performing the same tasks on a comparable scale) will be treated differently depending on whether they are included in the catalogue of operators of essential services.

The NIS Directive is often presented as the foundation of the EU cybersecurity model [17]. It should be remembered, however, that the purpose of its adoption was mainly to enhance communication and to improve the exchange of knowledge and experience between Member States. The creation of national and sectoral security incident response teams (CSIRTs) and the establishment of communication channels between them are necessary but are not the only actions that must be taken to improve the level of cybersecurity in the EU. Undoubtedly, the directive will improve the process of responding to the most serious incidents and thus help to minimize their consequences as well as decrease the likelihood of their recurrence in the future. A significant number of the obligations defined in the directive are aimed at increasing the level of cybersecurity of the state and of key entities that influence the provision of services to the public. The issue of taking steps directly focused on the safety of users is treated somewhat indirectly—namely, as a consequence of increasing the cybersecurity level of critical services and major digital services. Moreover, hardware manufacturers and software developers have also been excluded from the scope of application of the directive which further reduces the practical importance of regulations arising therefrom for home users.

Established under Regulation 2019/881, the European cybersecurity certification framework has made it possible to create programmes for the certification of IT products and services offered in the internal market [18]. Owing to the adoption of a hierarchical model, programmes of this type can be implemented at both EU and national levels. A new concept of the European cybersecurity certificate has also been introduced; it confirms that the product that has been examined has been positively evaluated at one of three assurance levels (basic, substantial or high). Without a doubt, the enactment of a certification framework for products and services will significantly improve the safety of products, including those offered to consumers. However, because the regulation only recently entered into force, it is still impossible to assess the actual impact of product certification on the coherence of the cybersecurity model applicable in the Union.

Whereas the entry into force of the NIS Directive and the Cybersecurity Regulation may have gone unnoticed from the users’ point of view, most of society is aware of the effects relating to the reform of data protection laws, the key element of which was the adoption of Regulation 2016/679 (GDPR) [19]. One of the crucial elements of the GDPR is increasing the control that data subjects have over information processed about them; another is the
introduction of mechanisms for quick notification of data leaks [20]. Owing to this, users can more effectively counteract the negative effects of disclosed violations such as identity theft. Undoubtedly, the granting of powers to supervisory authorities to impose high administrative penalties has also resulted in a significant increase in the attention paid by entrepreneurs to user data security issues.

The EU cybersecurity model is also being developed in alignment with regulations established in the area of the electronic communications market. In this regard, it should be borne in mind that telecommunications service providers are, in principle, excluded from the application of the NIS Directive. Requirements related to the security of systems and networks for these sectors were defined in the EU telecommunications regulations (in particular, Directive 2002/21 [21]). Directive 2018/1972 that established the European Electronic Communications Code (EECC Directive) [22], a new legal act adopted in 2018, will form the basis for EU regulations in the electronic communications sector after its implementation into national legal systems is completed in December 2020. The EECC Directive will also replace Directive 2002/21 and, as a result, will become the primary source of cybersecurity regulation for the providers of infrastructure and telecommunications services. An important change relating to the entry into force of the EECC Directive will also be an extension of the scope of the EU electronic communications sector framework that stems from changes to the definitions of key terms such as ‘electronic communications network’ or ‘electronic communications service’ [23].

In order to understand the direction of the development of the EU cybersecurity model and its potential for effective protection against the growing wave of threats in cyberspace, it is necessary to take a wider look at the activity of the EU legislature. Strictly speaking, the cybersecurity model results from the application of the NIS Directive and the Cybersecurity Regulation. In a broader context it has also been built with the use of legal mechanisms arising from other areas of law, including data protection and electronic communications laws. It seems obvious that, when referring to the protection of consumer rights and the safety of products offered to this group of customers, cybersecurity mechanisms should follow from or at least correlate with the measures applied in consumer protection law and, supplementarily, in competition law.

However, it would be a mistake to define the scope of regulations relevant to the cybersecurity of consumer products too broadly. The breadth of the term ‘cybersecurity’ means that this area may be associated with almost any provisions governing activities undertaken online. In this way, the above term can be connected with sector-specific regulations on e-commerce, provision of financial services, or any distantly concluded or implemented contracts. Such a broad definition of cybersecurity—in isolation from the context of research—makes it impossible to set boundaries for the analysis. In the third decade of the 21st century, everything can be ‘cyber’. Tom Gerety [24] noted that ‘a legal concept will do us little good if it expands like a gas to fill up the available space’. Gerety was referring to the conceptualization of privacy, but his remark also aptly describes today’s difficulties with definition of cybersecurity.

Hence, when isolating the most important areas that affect the cybersecurity of products from the end-user’s perspective (Fig. 1), it is necessary to make certain preliminary assumptions to limit the scope of legal regulations considered in the further analysis. First, it seems reasonable to omit provisions that de facto do not pertain directly to the cybersecurity of products but are closely related to the security of online services (e.g. PSD2 or eIDAS regulations). Next, due to the specificity of connected products, the issue of detailed obligations imposed on online content providers (information society services) may also be regarded as secondary. As a result, the regulations presented in Fig. 1 are limited to those that have a real impact on setting standards for the market of connected products, i.e. provisions relating to data protection law, electronic communications law, as well as product safety and consumer protection.

It is worth noting that an important element of the scheme that is presented is the distinction between ‘data security’ and ‘device security’. Although both areas are intertwined and equally important from the user’s perspective, in practice, they are affected by different risks and shaped by different legal provisions. Data security is closely related to the security of an online service that is used for data processing. For each networked device, it is possible to identify at least one online service that usually allows remote configuration or control of the product. Of course, there can be more services and what is more is that distinct providers may be responsible for their proper functioning. This subsequently leads to the conclusion that several entities may be liable for the security of a connected product (e.g. an IP camera) with the liability of each of them arising from different legal provisions.

Data protection law

With the adoption of the GDPR, requirements relating to the security of personal data processing have been significantly strengthened and clarified. Pursuant to Regulation 2016/679, both the data controller and the processor are required to take appropriate technical measures that are adequate to address the risks that are identified. In the catalogue of examples of such technical measures, the legislature included pseudonymization and encryption of personal data as well as regular evaluation of the effectiveness of the technical safeguards that are implemented. Furthermore, one of the innovations introduced in the GDPR was the stipulation that requirements relating to the protection of personal data should be taken into account at the design stage (privacy by design) [25]. In practice, the concept of ‘privacy by design’ should result in the selection of safeguards that, in the opinion of the manufacturer (data controller), will lead to a minimization of the risks that may adversely affect the security of processed data. The reference of ‘privacy by design’ to the segment of connected consumer products, therefore, should result in the consideration of privacy and data protection requirements as early as the design stage of a specific solution. Moreover, it should lead to data protection being treated as a holistic process which requires proactive prevention of incidents rather than only responding to the effects of their occurrence (cf. p. 103 in [26]). At the same time, it should be borne in mind that privacy by design is a more general concept intended to help increase the security of processed personal data rather than a detailed list of specific security measures that have to be taken by the data controller. Bert-Jaap Koops and Ronald Leenes aptly note that ‘privacy by design’ should not be interpreted as a general requirement for system developers to embed as many data protection requirements as possible into the design of the system [p. 147 in 27]. Privacy by design is not an exhaustive list can take advantage of in the form of a separate online service, the data controller will be the provider of the optional service.
(security checklist) that can become the basis for controlling or assessing the security of certain products.

However, the GDPR cannot be an effective solution to the problem of adequate protection of connected consumer products. First, GDPR’s scope is the processing of personal data. If the manufacturer does not intend to collect personal data, the regulation’s provisions do not apply.

In addition, the GDPR, in principle, covers only the area of data protection—and not all abuses that may relate to connected consumer products. As shown in Fig. 1, not all functions that a given device performs are related to the processing of personal data. Consider the simple example of when an attacker uses a known vulnerability that has existed in a communication protocols for years to breach its security measures and install malware on a home printer device. This device—as the so-called ‘zombie’—becomes part of a remotely managed botnet. In fact, it is currently quite a common attack vector. However, if the perpetrator’s action was not intending to violate the user’s privacy (e.g. by intercepting the content of printed documents) and was ‘only’ aimed at using the printer device as part of a botnet performing other tasks (e.g. spam distribution, DDoS attacks, etc.), it is doubtful that an incident of this sort leads to a violation of GDPR provisions. Undoubtedly, the perpetrator’s behaviour can be prosecuted under criminal law, however, possible criminal liability does not equate to the manufacturer’s obligation to properly secure networked devices against this type of threat. In practice, a significant number of attacks on IoT devices are not privacy violations or personal data theft [28]. Rolf Weber even claims that, in the case of IoT device security incidents, data protection law has limited application in general which is due to the fact that ‘IoT raw data are not personal on its face as it does not identify an individual’ [p. 619 in 29].

A cybercriminal does not have to breach the security of personal data for his behaviour to have negative effects on the user. The GDPR is undoubtedly an important source of requirements in the area of data protection, however, data protection is not the entire cybersecurity. When thinking about the cybersecurity of networked devices, it is worth visualizing violations other than those related to privacy. A simple example is an electronic lock that makes it possible to remotely open the door to our house. An attacker who has blocked the operation of this lock, as a result of which we were not able to get inside, would undoubtedly reduce our confidence in the security of the technology that we use. Therefore, when looking for effective protection standards for smart devices, it is necessary to go beyond the data protection law.

Product safety and consumer protection

Horizontal regulations: the definition of a(n) (un)safe and a defective product

In the context of the ongoing digitization of the internal market, the need to ensure consumer safety is obvious; it is somehow a consequence of EU policy activities focused on the digitization of not only states but also the economy. In the Digital Agenda for Europe [30], part of the ‘Europe 2020’ programme [31], it is assumed that information and communication technologies should serve an elementary development function. At the same time, the need to popularize broadband Internet is emphasized in order to promote social inclusion and the competitiveness of the EU economy, especially through the 2025 implementation of 5 G and gigabit Internet access in all key areas of socio-economic development. Objectives defined in the Digital Agenda for Europe were outlined in the Digital Single Market Strategy for Europe [32, 33] for which the aim is to create a uniform legal framework for the EU digital market. It proposes a far-reaching harmonization of law that is aimed at removing regulatory barriers to cross-border e-commerce. This recommendation has led to, among others, Regulation 2018/302 on unjustified geo-blocking and other forms of discrimination against customers [34].

However, these declarations have not been accompanied by regulations that have strengthened consumer protection in the event of external attacks preventing them from the normal use of digital devices. Due to the above-mentioned scope of the NIS Directive, the CSIRTs’ tasks prescribed therein are centred around responding to incidents related to threats in public networks and, if an attack occurs, taking the necessary steps in cooperation with national and foreign centres to analyse the nature, manner, and extent of the incident as well as to exchange information in order to alert key sectors and institutions. Therefore, CSIRTs’ responses are mainly of an ex post nature which does not guarantee the necessary consumer safety in the use of digital devices.

The application of the provisions of Directive 2001/95 on general product safety (GPSD) seems to be difficult in this situation [35]. The directive defines a product as any product—including providing a service—that is intended for consumers or likely, under reasonably foreseeable conditions, to be used by consumers even if not primarily intended for them. However, a dangerous product is only a product that presents a risk to the safety and health of persons greater than the minimum risks associated with the product’s use under normal or reasonably foreseeable conditions of use. A product shall be deemed safe when it conforms to the national laws of the member state that are drawn up in conformity with the TFEU, in
particular Articles 28 and 30, in the territory where the product is marketed.

Hence, the directive applies to products used by consumers that do not meet the requirement of health and safety protection but without defining the concept of safety. There is no doubt that safety should be understood as the life and health of consumers as product users. This is also confirmed by the legislation of the Member States transposing the directive into national law. For example, the Polish Act of 12 December 2003 on general product safety [36] simply states that a safe product is a product that, under ordinary or other reasonably foreseeable conditions of use, does not present any risk to consumers or creates a negligible risk reconcilable with its normal use. In turn, while the German Gesetz über die Bereitstellung von Produkten auf dem Markt [37] adheres to both concepts expressed in Directive 2001/95, i.e., health and safety, it associates safety itself with health protection as an element of public safety.

Private law protection is also questionable. Whereas Recital 50 in the preamble to the NIS Directive states that hardware manufacturers and software developers are not operators of essential services or digital service providers, their products increase the security of IT systems and networks. ‘Therefore, they play an important role in enabling operators of essential services and digital service providers to secure their network and information systems. Such hardware and software products are already subject to existing rules on product liability.’ This statement, however, is not substantiated. Directive 85/374 of 25 July 1985 concerning liability for defective products [38] states in Article 6 that a product is defective when it does not provide the safety that a person is entitled to expect. This takes all circumstances into account including the presentation of the product, the use to which it could reasonably be expected that the product would be put and the time when the product was put into circulation. However, for the manufacturer to be liable in law, a causal link must be established between the product defect and the damage that has occurred. The manufacturer’s liability as understood in this context does not fully accord with the problem of cybersecurity being analysed here [p. 109–11 in 39].

The importance of sector-specific regulations

The general product safety directive is of a horizontal and, at the same time, supplementary nature which means that it applies when there is no relevant sector-specific regulation pertaining to certain product categories. If there is sector-specific regulation in place, the assessment of cybersecurity of consumers should be analysed from the perspective of the principles of the EU conformity assessment and market surveillance systems.

The primary purpose of the EU conformity assessment system is to harmonize technical requirements for products which is important primarily for the free movement of goods within the single market. The harmonization of conformity assessment rules within the EU apply to products and consist of the enactment by Member States of provisions defining the essential requirements for products. This is achieved through the implementation of mandatory provisions of technical harmonization directives and optional European harmonized standards that contain detailed technical requirements.

The technical harmonization directives introduce the obligation to assess the conformity of products; however, they only apply to products introduced for the first time into the EU market or placed on the EU market for the first time, i.e., new products manufactured in the EU as well as new and used products from third countries [42].

The technical requirements contained in the harmonized law are limited to essential requirements that entail the obligation of entrepreneurs to solely market products compliant with these requirements. A presumption of conformity with the essential requirements is also assigned to products that are manufactured in accordance with harmonized standards [43] for which the use is voluntary, so the manufacturer may apply other technical specifications to meet the essential requirements. There are currently approximately 5000 harmonized technical standards introduced in the implementation of individual harmonization directives [44].

The EU model for product safety assessment was supplemented in 1989 with common principles of conformity assessment that referred to the development of uniform components of this assessment, covering design and production phases, and encompassed the principles of CE conformity marking. The concept of such an assessment was introduced by Council Decision 93/465 of 22 July 1993 that provided for so-called ‘modules’ that were intended for use in various phases of conformity assessment procedures. The scope of the products covered by particular directives results primarily from the definition of specific products referred to in the technical directives [45].

The conformity assessment system in respect of market surveillance contains 70 acts of EU harmonization legislation. Regarding domestic electrical equipment, an important instrument is Directive 2014/35 on the harmonization of the laws of the Member States relating to making available on the market electrical equipment designed for use within certain voltage limits (Low Voltage Directive, LVD). Among other matters, the directive refers to electrical household appliances. Although it stipulates a protection mechanism against hazards that may arise from electrical equipment being affected by external factors, they are limited to, among others, resistance to non-mechanical influences in expected environmental conditions or foreseeable conditions of overload.

However, the LVD does not contain provisions that refer to regulations relating to broadly understood cybersecurity. This is understandable considering the fact that the harmonization directives concern product properties but not specific applications; the basic requirements are those relating to the main functions of the products that should be safe with regard to people’s health, lives, property, and the environment. Hence, in Directive 2009/48 [46] that concerns toy safety, terms such as ‘aquatic toy’, ‘chemical toy’, ‘activity toy’, or ‘cosmetic kit’ were defined in detail that made it possible to specify the requirements related to the protection of children’s health and life. At the same time, the directive fails to mention the possible risks that arise when a child gains access to content that is not intended for him or her through a toy or otherwise falls victim to cyberbullying. This problem was noted during a review of the effectiveness of the directive that was carried out by the European Commission in 2018. In their comments, NGOs pointed out the need to include a reference to cybersecurity risks in the requirements.

6 A lack of harmonization of requirements could actually have the effect of restricting trade between Member States. Initially, the so-called Old Approach model prevailed in EU law. It preferred ‘complete’ or ‘total’ harmonization, the aim of which was to eliminate any differences in product conformity that might occur at the level of national law of Member States. This concept evolved over time into the so-called New Approach according to which the role of EU law was to define ‘essential requirements’ for products while affording manufacturers freedom in terms of less vital product features [p. 571–78 in 40]. The New Approach to technical harmonization and standardization was introduced by the 1985 Council Resolution [41].

7 In EU terminology that means countries that are not parties of EEA.
for toy manufacturers [47], particular attention needs to be paid to the statistics presented by the EPIC according to which, in 2017, a total of 227 million smart toys were produced worldwide [p. 3 in 48]. Therefore, it is difficult to consider the segment of these types of products as negligible or insignificant from the perspective of consumer safety.

References to broadly understood cybersecurity are also missing from the so-called new ‘Goods Package’ that aims at ensuring better functioning of the single market for goods and improving the existing conformity assessment system in respect of market surveillance. This package contains two regulations from the European Parliament and the Council of the EU. The first, Regulation 2019/1020 [49], which will apply from 16 July 2021, is intended to increase compliance with and enforcement of EU product-related legislation. The purpose of the second one, Regulation 2019/515 [50], is to enhance and facilitate the application of the principle of mutual recognition in the single market.8

Essential requirements for radio equipment

Although the provisions on general product safety seem insufficient for establishing standards for the protection of networked devices against cyber threats, there are provisions in the EU legal model that can be used to achieve this objective, at least partially. This refers to Directive 2014/53 (Radio Equipment Directive, RED) [51], one of the harmonization directives that aims to approximate national regulations regarding the essential safety requirements for radio equipment.

In accordance with Article 10(1) of the RED, manufacturers placing their equipment on the EU market must ensure that it is designed and manufactured in compliance with essential technical requirements. Among these requirements, the EU legislature took into account the need to incorporate safeguards that aim to ensure the protection of personal data and privacy of the user (Article 3(3)(e) of the RED) and to provide protection against fraud (Article 3(3)(f) of the RED). The directive, therefore, may be the basis for specific cybersecurity requirements for specific types of devices that use radio communication in their operation (including, of course, wireless communication).

If the competent market surveillance authority determines that a product placed on the market does not meet the requirements established in the directive, it may require the entrepreneur to take all necessary corrective measures or withdraw the device from the market. Information on the non-compliance that is identified can also be forwarded to the Commission and other Member States which, in the statistics presented by the EPIC according to which, in 2017, a total of 227 million smart toys were produced worldwide [p. 3 in 48]. Therefore, it is difficult to consider the segment of these types of products as negligible or insignificant from the perspective of consumer safety.

References to broadly understood cybersecurity are also missing from the so-called new ‘Goods Package’ that aims at ensuring better functioning of the single market for goods and improving the existing conformity assessment system in respect of market surveillance. This package contains two regulations from the European Parliament and the Council of the EU. The first, Regulation 2019/1020 [49], which will apply from 16 July 2021, is intended to increase compliance with and enforcement of EU product-related legislation. The purpose of the second one, Regulation 2019/515 [50], is to enhance and facilitate the application of the principle of mutual recognition in the single market.8

First, the directive only covers radio equipment. Even when employing a broad definition of the term according to which all devices that allow wireless communication (e.g. communication via Wi-Fi or Bluetooth) fall into this category, it is obvious that a significant quantity of consumer electronics consists of wired devices. Such devices are, by definition, excluded from the application of the RED. As a result, even if the provisions of the directive led to the introduction of standards in the field of cybersecurity, they would not apply to all products that share similar features but only to those that perform communication functions in a wireless manner.

The second limitation of the model arising from the directive is a result of limiting the scope of IT security requirements to the extent that it only affects the protection of privacy or personal data. As previously discussed, the problem of the cybersecurity of devices should not be reduced solely to the issue of protecting data that is processed by the device. No less important is protection against unauthorized access to device functions. In this regard, another essential requirement indicated in the RED may be invoked according to which radio equipment should not have an adverse effect on the telecommunications network or use network resources in an inappropriate manner. This requirement, however, does not apply to protecting the device against unauthorized access (e.g. using the device as a zombie in a botnet) but to ensure that the device effectively uses the radio spectrum. An expanding interpretation—leading to the recognition that a DDoS attack is, in fact, a functional equivalent of radio spectrum interference and, as a consequence, that the RED should also be interpreted as introducing requirements related to the protection of devices against the possibility of their unauthorized use—seems to be deprived of sufficient grounds in the provisions of the directive.

The last aspect of the protection model established in the RED that may limit its effectiveness is that the competent authorities on data protection and those on cybersecurity have not been provided with powers relating to the supervision of cybersecurity of consumer products. EU law does not contain any requirements or limitations relating to the establishment of such a competent authority and leave this to the discretion of Member States. As a result, the responsibility for compliance with the RED requirements in Poland was assigned to the authority supervising the telecommunications market. However, it is mainly a regulatory authority focused on

8 This regulation entered into force on 24 April 2019 but will apply from 19 April 2020.
spectrum management rather than ensuring compliance with cybersecurity requirements.

False or misleading information about the IT security measures of a product as an example of an unfair market practice

In addition to the regulations concerning manufacturers’ obligations related to the placing of products on the market, EU law also provides for the protection of consumers to the extent that they receive the relevant information needed to make a purchasing decision. Such information encompasses important product features including the technical capabilities it offers and the risks associated with its use. Concealment or misrepresentation in terms of product characteristics may be a manifestation of unfair market practice and, as a result, may invoke the response of bodies appointed to protect consumer rights.

The grounds for such an action are provided primarily by Directive 2005/29 concerning unfair business-to-consumer commercial practices in the internal market (UCPD)\(^9\) in conjunction with Directive 2009/22 on injunctions for the protection of consumers' interests.\(^10\) The scope of application of the UCPD is limited solely to consumer protection; therefore, its provisions do not affect the application of national regulations concerning those unfair commercial practices that exclusively violate the principles of fair competition or business transactions between companies [p. 128 in 54].

As defined by the UCPD, an unfair market practice is a practice that is misleading in its nature; stated differently, an action that causes or may cause the average consumer to make a transactional decision that they would otherwise not have made. The intention of the EU legislature was to regard as misleading both practices when dissemination of false information actually results in the consumer being misled and those that could only potentially have such an effect on the average consumer [55]. Such a practice should result in guiding the consumer’s choice in the form of a potential or real possibility of influencing the consumer’s transactional decision. The information required by law that is relevant from the perspective of the average consumer’s decision as to the use of the entrepreneur’s offer should be true, presented in an unambiguous, understandable and clearly visible manner, and also be exhaustive.

In its case law, the Court of Justice has repeatedly confirmed the accuracy of a broad interpretation of the prohibitions on unfair commercial practices under the UCPD. In the Perenicoa and Perenic case, the CJEU stressed that, for a practice to be unfair within the meaning of the directive, it is sufficient for it to cause the consumer to take a transactional decision that they would not otherwise have taken [para 47 in 56]. In turn, in the judgment in Trento Sviluppo srl, the Court emphasized that the purpose of the UCPD was to ensure a high level of consumer protection by establishing a general prohibition of unfair commercial practices that distort consumers’ economic behaviour [para 32 in 57]. To this end, demonstrated by the case of Carrefour Hypermarchés SAS, it is the entrepreneur’s responsibility to provide the consumer with the ‘material information’ that is needed to take an informed transactional decision [para 30 in 58].

Such information should particularly be on the scale and scope of threats or risks associated with the use of the product but not necessarily connected with traditional threats to life, health and property. In the area of cybersecurity, this should result in providing consumers with detailed information on the properties of the products or services offered and the risks to security that may be associated with using them. When making a purchase decision, the consumer should not only rely on the manufacturer’s assurance that the product is ‘safe’ but also be able to understand what features or properties from which this conclusion results. John Blythe, Nissy Sombatruang, and Shane Johnson have conducted an interesting study on the content of manuals attached to IoT products offered in the consumer market that covered over 200 devices belonging to 23 product groups. It revealed that only 20% of device manuals specified the adopted encryption standard for wireless communication (Wi-Fi) and, in only 15% of the cases, did they discuss how encrypting data was stored in the device memory [p. 5 in 59]. In relation to products using cloud services, the manual included a discussion of the risks that may be associated with this form of data processing in only 5.3% of the cases. It is difficult to expect that the consumer, based on such fragmentary data, could make a fully informed purchase decision. On the contrary, the practice of not providing key information on the products that are offered can be considered as an example of an unfair market practice that also adversely affects competition between entrepreneurs.

However, detailed information on product features will not always be sufficient to enable consumers to reliably assess the risks involved in the choice of a given technology. In particular, there is no doubt that devices that allow monitoring of the physical environment (in particular sound or image recording) pose a greater threat to user privacy than comparable devices that perform similar tasks but lack the capability of collecting such data. The above problem can be explained with a simple example. Currently, one type of smart connected devices that is increasingly used in households is the so-called vacuum cleaning robot. Devices for which their primary function is cleanliness are equipped with a number of sensors and systems that allow smooth navigation around rooms. Yet users are often not aware that this type of product also has built-in cameras that can be used to record images. What is more, the data collected by these devices can be stored on remote servers located in third countries (e.g. the United States or China). There is no doubt that a user deciding to buy a cleaning robot should have access not only to information on the performance properties of the product (cleaning algorithms applied, battery life, etc.) but also on additional features that may affect the assessment of this product. Information that a particular type of robot cleans more effectively than other models because it uses a built-in camera should be clearly presented to the consumer. Otherwise, they cannot consciously accept the risk that better cleaning effectiveness may be attained at the cost of compromising their privacy. Moreover, this example illustrates that even assuming (rather unrealistically) that a specific device is completely secure (and, therefore, not susceptible to any cyberattack), the user’s privacy can be threatened as a result of the collection of detailed information about various aspects of their life by third parties (in this case: suppliers of household appliances). Consequently, with some categories of products intended for the consumer market (in

---

9 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (Text with EEA relevance), OJ 2005 L 149/22.

10 Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers’ interests, OJ 2009 L 110/30.
particular devices that enable monitoring of the physical environment, it seems reasonable that not only omitting relevant information about the cybersecurity mechanisms that are applied but also the lack of indication of key risk factors may be assessed as a violation of the collective rights of consumers.

In this respect, such a practice does not necessarily violate the existing harmonized technical standards. This type of omission is a primarily violation of professional diligence defined by the UCPD, often referred to in the national laws of Member States under the concept of good practices. Professional diligence and good practices are lexically different terms; however, the semantic content of these phrases is identical. In light of the directive, ‘professional diligence’ means the standard of special skill and care that a trader may reasonably be expected to exercise toward consumers that is commensurate with honest market practice and the general principle of good faith in the trader’s field of activity. Hence, it refers to good practices in the economic and functional aspect, which makes it possible to assess entrepreneurs’ conduct through the prism of transparent, undistorted and, therefore, fair competition in the market. It also corresponds to the public interest which is manifested by the general interests of participants in a particular market: entrepreneurs and also—at the lowest trade level—consumers. In relation to consumers, it should be expressed by providing proper information about their rights, taking no advantage of the professional’s privileged position, and fair treatment of contractual partners. Actions aimed at providing insufficient information, causing confusion, creating misconceptions, and taking advantage of consumers’ ignorance or naivety can be considered as being contrary to good practice.

The UCPD regulations on misleading commercial practices are often juxtaposed with the successfully applied US federal law regulations on the basis of which the US supervisory authority (FTC) pursues violations of obligations related to the cybersecurity of consumer products [60]. An example could be the D-Link Systems case in which the FTC charged the entrepreneur with non-compliance with security requirements that led to a security breach in over 400,000 devices including routers, modems, and IP cameras. D-Link’s fault resulted from a lack of systemic care for the safety of the products that were offered was manifested, inter alia, by using the same easy-to-guess default passwords or the lack of counteraction against known and foreseeable types of attacks. As part of the settlement that was reached, the company was required to implement a comprehensive cybersecurity management programme for the products it offered.11

The case of D-Link illustrates the possibility of effectively raising the level of security of devices offered on the consumer market without introducing new legal regulations or technical standards. In general, the FTC achieves the same objectives that are to be reached in the EU model through Regulation 2019/881 and the cybersecurity certification framework arising therefrom solely on the basis of provisions relating to competition protection and the prevention of unfair or deceptive market practices. Although the D-Link case concerns the US market, there are no legal obstacles for European consumer protection authorities to implement such actions. In this way, they could proactively shape the practices of entrepreneurs placing consumer products on the market in order to increase their level of IT security, especially considering the fact that EU regulations provide for this possibility. To this end, supervisory authorities should utilize mechanisms applied by the FTC, such as entering into binding settlements with entrepreneurs. As Nico van Eijk, Chris Jay Hoofnagle and Emilie Kannekens point out, in this way, the body will not only be limited to imposing penalties for the violations that are found, but it will also be able to proactively influence the shape of the market, affecting the behaviour of its participants [p. 12 in 61].

The cybersecurity certification framework in light of the definition of a(n) (un)safe product

Taking the above analysis of legal circumstances into consideration, an extension of the protection of home users under consumer protection law would prima facie require three important changes: the first relating to an extension of the concept of product safety, the second regarding the development of IT security standards for particular product categories; and the third—as far as the law enforcement stage is concerned—strengthening the protection of collective consumer interests under the UCPD.

Relating safety only to life-threatening or health-threatening cases is undoubtedly too narrow an approach and obviously inadequate for both changing social expectations and the realities of using modern consumer products [p. 10–11 at 62]. There are many known types of attacks on smart devices, the result of which is not a threat to the life or health of their users but certainly a violation of their privacy and often also their sense of security [63, 64]. Currently, webcams are widely used not only for video surveillance purposes but also for monitoring children’s activity. It is difficult to accept the view that an objectively functional camera that is transmitting the image via the IP network to the parent’s mobile device could be considered a product fulfilling its basic functions if, due to technical vulnerabilities known for years, unauthorized persons might gain access to this image. This poses a risk of outside distribution, including on the Darknet, e.g., on forums containing paedophile content [65]. Therefore, it is correct to infer that the mere fact of connecting a consumer product to the Internet reveals new, previously absent risks for which the analysis and minimization is, first and foremost, the manufacturer’s responsibility.

In computer science, information system security is defined by its ability to protect the three basic attributes of information: confidentiality, integrity, and availability (see the definition introduced in [66]). In technical applications, ‘privacy’ is not defined as a separate property (feature) of information. Privacy is a term related to psychological, sociological, and legal sciences. Preserving privacy, from the perspective of the owner of the information, is not possible without maintaining (controlling) its confidentiality. Therefore, when considering privacy and information security issues, the most important aspect is confidentiality. If the IT security of a product can be defined as a state in which the confidentiality, integrity, and availability of processed information have not been violated, then, conversely, a dangerous product can be characterized as not having mechanisms in place to ensure at least one of the indicated security attributes.

Of course, the point of proactive consumer protection is to prevent the possibility of launching products that should not be on the market rather than to respond reactively if incidents occur.

11 Details of the FTC’s recommendations were presented in proposed stipulated order for injunction and judgment formulated in the case Federal Trade Commission v. D-Link Systems (see [p. 3–6 in 61]).
Transferring this model to the field of consumer product IT security, therefore, would require the implementation of assessment standards that would make it possible to confirm that a given technology contains adequate security mechanisms when taking into account the use of the product intended by the manufacturer and the risks it involves.

However, information security is a process rather than a state. Security is to be ensured, not achieved. This is due to the fact that, among others, the final level of security of a given technical solution is influenced not only by the manufacturer’s acts or omissions (e.g. errors at the design or testing stage) but also by errors relating to the manner in which the product is implemented and used. In addition, the dynamics of creating new attack vectors and revealing previously unknown vulnerabilities may also change the assessment of a product that was previously considered as safe. Therefore, instead of attempting to assess (measure) the current state of ‘security’, the prevailing approach is the one based on assessing the maturity of the process of ensuring security. The Common Criteria (CC) evaluation model, described in the family of ISO/IEC 15408 standards, works in the way described above thus allowing the security assessment of any IT systems [69]. This standard is based on the development of earlier standards, in particular the TCSEC [70], especially popular in the United States, and the later ITSEC standard [71]. However, while TCSEC was a solution created for the purposes of assessing classified information processing systems and was widely used in the defence sector, for many years, the CC has been the formal basis for the evaluation of many commonly used IT systems, including popular operating systems such as MS Windows [72]. The evaluation framework described in the CC makes it possible to carry out a formal process of assessing whether the technical safeguards implemented in the product are adequate for the risks identified while, at the same time, confirming the appropriate maturity of the design, implementation, and testing processes of a specific solution. Therefore, formal CC certification is not only to confirm that a particular solution contains a set of declared technical safeguards but also to verify that the process within which the system was created took account of IT security requirements at every stage of its development.

The introduction of compulsory certification for selected types of connected products intended for the consumer market would be a solution that would not only increase the level of IT security in this market sector but would also enable easy adoption of regulations on dangerous products to the area of cybersecurity. The veracity of this evaluation can be demonstrated by activities relating to the implementation, design, implementation, and testing processes of a specific solution. Therefore, formal CC certification is not only to confirm that a particular solution contains a set of declared technical safeguards but also to verify that the process within which the system was created took account of IT security requirements at every stage of its development.

As a result, cybersecurity should be perceived as a process that requires continuous improvement—hence the popularity of the ISO/IEC 27001 standard and the concepts introduced in management systems (including the Plan-Do-Check-Act model) in the discussion of the EU cybersecurity model. See [67, 68].

See [73]: ‘The candidate scheme is envisaged to provide for cybersecurity certification of ICT products and ICT services. It will be based on the Common Criteria for Information Security Evaluation, the Common Methodology for Information Technology Security Evaluation and the corresponding standards, namely ISO/IEC 15408 and ISO/IEC 18045.’

A similar recommendation can be found in the ANEC/BEUC position paper [p. 15 in 62]: ‘For this reason, BEUC believes that it is necessary to establish binding minimum security requirements before connected products and services are placed on the market.’ Examples of security measures for IoT devices are discussed in [76].

More on Privacy Shield programme in [78]. Although this framework has been found by the CJEU to be non-compliant with EU law and was annulled in a recent judgment [79], this decision was not related to the nature of the program (based on a self-certification model) but to a critical assessment of the US federal legislation established in the area of national security that, in the opinion of the Court, led to disproportionate interference with the right to privacy of EU individuals [80, 81].

Cross-border data transfers to third countries is one of key issues in EU data protection model. See [83–86].

More about FTC competences in the area of data protection in [87].
this proposal would require a new legal act since the current provisions of the cybersecurity framework do not provide for the possibility of introducing mandatory certification programmes. Therefore, if the legislature intends—such as in the RED model—to connect the possibility of placing a product on the market with meeting a certain safety standard, it would be necessary to either amend Regulation 2019/881 or introduce a new, complementary act with a horizontal effect. Although this proposal is supported by a large number of experts, it is also expected that it would take approximately 5 years to implement it [p. 115–16 in 53]. This is a relatively extensive time perspective, especially taking into account the dynamics of threats appearing in cyberspace, including the increase in the scale of attacks targeted at networked consumer devices. Therefore, it seems reasonable to adopt a hybrid model—combining the mechanisms present in consumer protection law with cybersecurity law—that can be described in terms of the following recommendations:

1. Extension of the definition of general product safety by including essential cybersecurity requirements in it,
2. Adoption of (optional) security standards based on Regulation 2019/881,
3. Initiation of legislative work related to the creation of a mandatory certification framework for consumer products (a new horizontal directive on cybersecurity),
4. Strengthening the protection of collective consumer interests on the basis of the UCPCD—in respect of changing the practice of supervisory authorities’ activities.

The purpose of the first recommendation would be to transpose regulations based on the RED model into the GPSD with the difference that the new safety requirements would apply to all products (and not only those using radio communications) and would encompass the entire spectrum of cybersecurity risks and not just those regarding data security. Extending the definition of general product safety would allow competent supervisory authorities to take steps to eliminate devices posing a threat due to the absence, inadequacy, or ineffectiveness of IT security measures implemented in them. Due to the horizontal scope of application of the GPSD, the requirements associated with the cybersecurity area defined in it would have to be of a more general nature. The recommendations included in the Code of Practice for Industry on Consumer IoT, published in 2018 by the British Government, could be helpful in developing such requirements [88].

The next two recommendations relate to the development of standards that could shape the market for connected consumer products. Naturally, these standards should include a reference to specific requirements that are stipulated, for example, in data protection law or electronic communications law. The implementation of the second recommendation does not require any legal changes, yet the security standards developed as part of it would not be mandatory. Such an effect could be achieved only after carrying out the third, which is the last, recommendation. The result of its implementation would be the development of a new horizontal directive that would be part of the EU product conformity assessment system. It is worth noting that this concept is also supported by organizations representing manufacturers according to which the problem of consistent cybersecurity requirements should be resolved at the EU level and for all product categories [89].

The fourth recommendation relates solely to the application of law. There are no formal obstacles for national consumer protection authorities to more intensively use the regulations that allow for the enforcement of the protection of collective consumer interests. Indeed, the Court of Justice has adopted in its case law the model of a consumer as a reasonable, observant and, above all, well-informed person [90–92]. This results from the concept of protection through information formulated in EU law; therefore, failure to provide consumers with reliable, true, and complete information is a violation of collective consumer interests. This would also put into practice the necessary cyber hygiene, promoted especially in the provisions of Regulation 2019/881, and thus guarantee a genuine level of cybersecurity for users of connected products.

Impact of support and maintenance on perception of product cybersecurity

A comprehensive approach to the issue of cybersecurity of consumer products makes it necessary not only to ensure that solutions introduced to the market are equipped with an appropriate set of risk-based technical safeguards but also to refer to the manufacturer’s obligations in respect of maintaining an adequate level of IT security for products that are already in the market. Every year, thousands of new vulnerabilities are disclosed in common IT systems; it is increasingly often that such vulnerabilities affect smart connected consumer products. Their exploitation (penetration) usually leads to a security breach or circumvention of security features which means that the user is deprived of the protection against such violations. In this case, only the manufacturer can provide the appropriate patches, the installation of which enables an effective and permanent resolution of the problem. Therefore, it is reasonable to extend the obligations relating to ensuring the cybersecurity of consumer products to include tasks related to responding to vulnerabilities and errors that emerge or are disclosed in the period after the product launch. The scope of these obligations should also be adapted to the expected lifetime of a product.

The manufacturer’s provision of technical support services, including issues relating to the cybersecurity of products, is a separate problem. Access to appropriate knowledge and support is crucial especially given that a significant proportion of users do not have the technical knowledge to independently configure numerous advanced features of modern products [59]. Providing a web camera with a function that allows the user to change their password is one thing, but the user’s ability to take advantage of this option is another thing. In many cases, a user who does not have the knowledge or the possibility of acquiring it (e.g. from a readable manual that is written in an understandable language) will not be able to properly configure the device in a way that minimizes the most common types of cyberattacks [90]. Therefore, the researchers who point out that ‘much of the responsibility for DDoS attacks often lies with users who practice poor security behaviours and system administrators who fail to deploy adequate safeguards’ are correct [p. 83 in 94]. The obligatory technical support provided by the entrepreneur, therefore, should encompass not only access to knowledge about the product but also promotion of appropriate behaviour in the field of cybersecurity.

The issue of providing security updates was duly noted by the EU legislature and resulted in new provisions introduced in Directive 2019/771 [95], which replaces previous regulations established for sales contracts concluded with individual consumers. Its scope also includes digital content and digital services contained in or interconnected with goods which means that it applies to the sale of connected consumer products. Pursuant to Article 7(3), the seller is obligated to inform consumers about available updates—
including security updates—that are necessary for the goods offered to them to be compliant with the contract. The legislature did not specify the period for which such updates should be provided but merely indicated that this period should be adapted to the nature of the concluded contract and to the goods or digital content to which this contract pertains. However, the consumer has the freedom to decide whether to install the update made available to them (see Recital 30 in [93]) which—in the absence of such a decision—may relieve the seller of liability for non-compliance of the product with the contract (see Article 7(3) in [95]). This solution appears to be controversial, especially since it may lead to difficulties in demonstrating both negligence on the part of the user and due diligence on the part of the seller. Given the long period of time for the implementation of the directive into national law—the deadline is 1 July 2021—a better solution would be to introduce a default requirement to use an automatic mechanism for installing security updates with exceptions to what could be introduced in justified cases. Not only would this concept resolve the problem of users’ lack of awareness and technical knowledge, but it would also accord with the ‘security by default’ strategy that is promoted in Regulation 2019/881 (see recital 13 in [1]).

The purpose of introducing the provisions of Directive 2019/771 was not to establish technical standards for the cybersecurity of products but only to clarify the liability of sellers when such products are delivered to consumers. The same products that do not meet the requirements of the directive and thus should not be offered to consumers can be freely supplied to other target groups. For example, the provisions of the directive do not limit the sale of poorly designed IP cameras that allow unauthorized access to recorded images to kindergartens, hospitals, or other public facilities. It is, therefore, obvious that, although the directive—if properly implemented—will constitute an important element of the EU cybersecurity model, it cannot be regarded as the only legal safeguard against launching connected products onto the market without basic IT security measures.

A separate issue that requires consideration is how the enforcement stage should be implemented for these types of requirements. It seems to be reasonable to assume that, as a rule, the manufacturer of the product (rather than the seller) should be responsible for the performance of maintenance obligations. However, since Directive 2019/771 concerns sales contracts concluded with the consumer, the seller has been designated as the obliged entity—also for maintenance requirements. Such a solution may result in transferring to this group of market participants risks that are actually beyond their control. Additionally, consumer rights would be more effectively protected if the seller and the manufacturer were jointly and severally liable for the fulfilment of maintenance obligations. In this context, it would be reasonable for the EU legislature to adopt, together with Directive 2019/771, an amendment to Directive 2001/95 relating to general product safety. Providing for the application of cybersecurity mechanisms to products at the stages of both their placing on the market and their subsequent maintenance seems to be a solution that makes it possible to equip consumer protection authorities with the powers needed to comprehensively deal with product safety—in terms of both general safety and cybersecurity requirements.

Conclusions

With the entry into force of Regulation 2019/881, a new stage in the development of the EU cybersecurity model began. The creation of a legal framework for the establishment of certification programmes is an important stage, leading to increased standardization in terms of key ICT technologies that are used in particular Member States. Currently, the leading stream of considerations regarding the EU cybersecurity model concerns the development of mechanisms that would protect the most important digital infrastructure, in particular systems and networks belonging to operators of essential services. Focus on this aspect of the problem is visible, for example, in the ongoing discussion on the security of the 5G network in which participants are both EU institutions [97] and individual Member States. The 5G cybersecurity case reveals the risk that individual states will use standard-setting mechanisms in the field of cybersecurity with an intention of limiting competition in the domestic market [100]. Joel P. Trachtman points out that ‘as a result states may assert security exceptions to their trade commitments, blocking trade more broadly than necessary to achieve their security goals’ [101].

Hence, it is even more justifiable to take account of the role of competition and consumer protection authorities in the work on developing a coherent cybersecurity model. Their involvement would allow a more effective transfer of best practice and standards developed for large enterprises to the consumer products market. An individual’s security and privacy are increasingly threatened not by large, extensive cyberattacks on leading digital service providers but by defective products launched onto the market in which disclosed vulnerabilities are not repaired promptly and thus posing a risk to thousands of users. Competition and consumer protection authorities can effectively counteract such events, often with the use of the legal tools they already possess. However, the analysis has also shown the need for greater intervention by the EU legislature, especially in terms of the reference of general product safety to the specific area of threats occurring in cyberspace. Nonetheless, no matter whether consumer protection was based on the cybersecurity framework, data protection, product safety, or contract law, the same result could be achieved—specifically, an increase in the effective level of security measures and product cycle management for smart connected consumer products.

One of the economic pillars of European integration is to ensure free conditions for the development of the internal market while at the same time respecting the principles of fair competition and protecting legitimate consumer rights. In an age of universal digitization, the pursuit of this objective must inevitably lead to the transfer of competition and consumer protection mechanisms that have developed throughout decades to the field of cybersecurity—newly emerged and yet vital for a modern economy.

References

1. Resolution 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). 2019:15–69.

18 The ENISA Advisory Group also defines the manufacturer’s role in ensuring product security during the maintenance phase [p. 7 in 96].

19 In particular, reservations about participation in the 5G project were raised by states that participate in the so-called Five-Eyes Alliance which includes the United States, the United Kingdom, Australia, Canada, and New Zealand. See [98]. More on Five-Eyes Alliance in [99].
48. Evaluation of the Toy Safety Directive (2009/48/EC). Electronic Privacy Information Center, 2018. https://epic.org/comments/EPIC-Comments-EU-Toy-Safety-Directive.pdf.

49. Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011. 2019:1−44.

50. Regulation (EU) 2019/515 of the European Parliament and of the Council of 19 March 2019 on the mutual recognition of goods lawfully marketed in another Member State and repealing Regulation (EC) No 764/2008. 2019:1−18.

51. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC. 2014:62–106.

52. RAPEX Alert number A12/0157/19. European Commission 2019. https://cldrive.eu/qny9YW.

53. Whittle M. Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment. Centre for Strategy & Evaluation Services LLP, 2020.

54. Schuhmacher W. The Unfair Commercial Practices Directive. In: Hilty RM, Henning-Bodewig F (eds), Law against Unfair Competition. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, 127–37.

55. Smith L. CJEU considers ‘misleading omissions’ under the unfair commercial practices directive. J Intellectual Property Law & Practice 2017;12:731–33.

56. Jana Perenicová, Vladislav Perenč v. SOS Financ, Spol. s r. o. CJEU. Case C-433/10. ECLI:EU:C:2012:144.

57. Trento Sviluppo Srl, Centrale Adriatica Soc. Coop. Arl v. Autorità Garante Della Concorrenza e Del Mercato. CJEU. Case C-281/12. ECLI:EU:C:2013:859.

58. Carrefour Hypermarchés SAS v. ITM Alimentaire International SASU. CJEU. Case C-562/15. ECLI:EU:C:2017:95.

59. Blythe JM, Sombatruang N, Johnson SD. What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? J Cybersecurity 2019;5: rzy005.

60. van Eijk N, Jay Hoofnagle C, Kannekens E. Unfair commercial practices: a complementary approach to privacy protection. Eur Data Protection Law Rev 2017;3:325–37.

61. Federal Trade Commission v. D-Link Systems, Inc., 2019. https://cldrive.eu/Bw5WwN.

62. Cybersecurity for Connected Products: Position Paper. Bureau Européen des Unions de Consommateurs & European Association for the Coordination of Consumer Representation in Standardisation, 2018. https://cldrive.eu/3PR8M.

63. Astor M. Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared. New York Times. https://cldrive.eu/X8dpY8. Published 25 July 2017.

64. Kan M. New IoT malware targets 100,000 IP cameras via known flaw. CIO 2017. https://cldrive.eu/9nByEx.

65. Rogers J. Paedophile hacked into thousands of people’s private home security cameras and secretly recorded their kids undressing. The Sun 2018; https://cldrive.eu/4b9Ww.

66. ISO/IEC. Information Technology — Security Techniques — Code of Practice for Information Security Controls 2013;27002.

67. Knapp KJ, Franklin MR, Marshall TE, et al. Information security policy: an organizational-level process model. Computers & Security 2009;28:493–508.

68. Katirciak A. In search of EU law in the domain of cyberspace protection – the proposal based on the Cyber-PIDCA model. J Cyber Security Technol 2017;1:127–43.

69. ISO/IEC 15048-1:2009, Information Technology — Security Techniques — Evaluation Criteria for IT Security — Part 1: Introduction and General Model.

70. Trusted Computer System Evaluation Criteria. US Department of Defense, 1983.

71. Information Technology Security Evaluation Criteria. Brussels/Luxembourg: European Communities, 1991.

72. Shapiro JS. Understanding the Windows EAL4 evaluation. Computer 2003;36:103–5.

73. Call for expression of interest for the first ad hoc working group on cybersecurity certification. ENISA News 2019. https://cldrive.eu/3JR1wE.

74. National Partnership Offers Benefits, but Faces Considerable Challenges. United States Government Accountability Office, 2006. https://www.gao.gov/new.items/id06392.pdf.

75. Kaluvuri SP, Bezni M, Rouder Y. A quantitative analysis of common criteria certification practice. In: Eckert C, Kakitsak SK, Pernul G (eds), Trust, Privacy, and Security in Digital Business. Vol. 8647. Cham: Springer International Publishing, 2014, 132–43.

76. Boeck K, Fagan M, Fisher W, et al. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. Gaithersburg, MD: National Institute of Standards and Technology, 2019:NIST IR 8228.

77. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield 2016;1–112.

78. Tracol XE-US. Privacy Shield: the saga continues. Computer Law & Security Rev 2016;32:775–77.

79. Commission Decision of 26 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. July 2000;2000:7–47.

80. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. CJEU. Case C-311/18. ECLI:EU:C:2020:539.

81. Rotenberg M. Schrems II. from Snowden to China: Toward a new alignment on transatlantic data protection. Eur Law J 2020;2020:617–30.

82. Ghont JX, Schrems II. The EU adequacy regime in existential crisis? Maastricht J Eur Comp L 2019;26:597–601.

83. Bender D. Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective. Int Data Privacy Law 2016;6:117–38.

84. Bu-Pasha S. Cross-border issues under EU data protection law with regards to personal data protection. Inform & Commun Technol Law 2017;26:213–28.

85. Mattoo A, Meltzer JP. International data flows and privacy: the conflict and its resolution. J Int Econ Law 2019;21:769–89.

86. Tehrani PM, Sabaruddin JSBH, Ramanathan DAP. Cross border data transfer: complexity of adequate protection and its exceptions. Computer Law & Security Rev 2018;34:982–94.

87. Solove D. The scope and potential of FTC data protection. George Washington Law Review 2015;83:223–37.

88. Code of Practice for Consumer IoT Security, Department for Digital, Culture, Media & Sport, 2018. https://cldrive.eu/ZipZGz2.

89. Horizontal Product Regulation for Cybersecurity. German Electrical and Electronic Manufacturers’ Association, 2018. https://cldrive.eu/VWyMeB.

90. Compagnie Des Montres Longines, Francillon SA. CJEU. Case T-505/12. ECLI:EU:C:2019:649.

91. Estée Lauder Cosmetics GmbH & Co. OHG. CJEU. Case T-61/12. ECLI:EU:C:2013:650.

92. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. CJEU. Case C-349/15. ECLI:EU:C:2016:257.

93. Knieriem B, Zhang X, Levine P, et al. The impact of the EU-U.S. Privacy Shield: a review. J Cybersecurity 2019;4:98–109.

94. Kolias C, Kambourakis G, Stavrou A, et al. An overview of the usage of the Digital Rights Management (DRM) technologies for Strategy & Evaluation Services LLP, 2020.

95. Dhont JX, Schrems II. The EU adequacy regime in existential crisis? Maastricht J Eur Comp L 2019;26:597–601.

96. Bender D. Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective. Int Data Privacy Law 2016;6:117–38.

97. Bu-Pasha S. Cross-border issues under EU data protection law with regards to personal data protection. Inform & Commun Technol Law 2017;26:213–28.
98. Holden M. Stubbs J. Five eyes will not use Huawei in sensitive networks: senior U.S. official. Reuters 2019; https://cli.re/nBqY4Y.

99. Pfluke C. A history of the Five Eyes Alliance: possibility for reform and additions: a history of the Five Eyes Alliance: possibility for reform and additions. Comp Strat 2019;38:302–15.

100. Mascitelli B, Chung M. Hue and cry over Huawei: cold war tensions, security threats or anti-competitive behaviour? Res Globalization 2019;1:100002.

101. Trachtman JP. Cybersecurity versus trade in internet of things products. Manchester J Int Econ Law 2019;16:301–40.