Acta Univ. Sapientiae, Legal Studies, **12**, 1 (2023) 43–59

DOI: 10.47745/AUSLEG.2023.12.1.04

Protection of Children's Personal Data and Risks Posed by Smart Toys[1]

Zsolt HAJNAL
PhD, Associate Professor, University Debrecen (Debrecen, Hungary),
Faculty of Law
e-mail: hajnal.zsolt@law.unideb.hu

Fanni TÓTH
PhD Student, University Debrecen (Debrecen, Hungary),
Faculty of Law, Marton Géza Doctoral School
Member of the Consumer Law Research Centre
e-mail: tothfanni22@gmail.com

Abstract. Data protection and consumer protection organizations have identified a number of data protection risks in connection with smart children's toys that use online services. This study presents the EU legislation that serves to protect the personal data of children using smart toys, with particular regard to the special provisions for children, and it also points out the extent to which these laws oblige the relevant economic actors to establish adequate protection. Examining all of this shows that the current legal framework is only able to manage the risks to a limited extent.

Keywords: consumer protection, cybersecurity, consumer safety, data protection, smart toys, Internet of Things

1. Smart Toys and Their Risks to Personal Data Protection

Digitalization, smart technology, and the Internet of Things (IoT) are unstoppable in our daily lives. Manufacturers have realized that children's toys can also be digitized, and in the middle of the second decade of the 21st century, intelligent toys have been launched on the market, combining the characteristics of toys and communication devices. In the case of traditional toys, the child is the active party and toys are passive; however, intelligent toys are able to respond to the child's

1 The research and publication were supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

instructions and questions with the help of sensors placed in the toys that provide data about the voice and other information regarding the child interacting with them. In terms of operation, the child asks a question from the toy, the toy records the sound using an internal microphone and then transmits the audio recordings via Wi-Fi or Bluetooth to a smartphone, which sends it to a server of a cloud service provider, where the voice is converted into text. Forwarding the text question is the next step, for example to Wikipedia, where the answer to the child's question is born, which an application sends back to the toy.[2] Due to these series of operations, once again, the European Union legislator is under pressure to act if it wants to ensure a high level of consumer protection in the internal market.[3]

Among smart toys, this study only looks at networked, so-called 'connected' toys. These are either toys with indirect Internet connection, i.e. they can communicate with a smartphone or tablet via interfaces such as Bluetooth, or toys connected directly to the Internet, i.e. connected to the Internet or directly to external servers through Wi-Fi via an integrated IP interface.[4]

Users of smart children's toys are exposed to multiple risks. Hackers accessed the database of one Chinese toy company and obtained millions of pieces of data, including children's voice data. The attacker was only interested in exposing the vulnerability: the toy vendor was transmitting data over an unencrypted channel.[5] However, in the environment of connected toys using unauthenticated Bluetooth devices, virtually anyone can talk to the child, and the toy can even act as a spying tool. These problems have shown that it is not the products themselves that pose risks, but the online services associated with the products that pose data security and data protection risks, i.e. the type of interaction through the IoT is the novelty of the product.

These problems have been highlighted by numerous consumer protection and data protection professional organizations in the case of children, the most vulnerable social group. In 2016–2017, an investigation by the Norwegian Consumer Council found that Internet-connected toys pose a potential risk to children's safety from a consumer and data protection perspective.[6] In addition to Norway, investigations have been launched in several countries, and similar errors have been identified.[7] In Germany, the baby 'Cayla' toy was withdrawn from circulation in 2017 due to unauthenticated Bluetooth connectivity, as the German Telecommunications Act prohibits the use of devices for spying, hidden cameras, and microphones.[8]

2 Hessel–Rebmann 2020. 27–37.
3 Hajnal 2011. 2419–2433; Hajnal 2019. 197–212.
4 Rauber–Thorun 2019. 14–16.
5 Dömös 2015.
6 #*Toyfail: An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys* 2016.
7 *International Working Group on Data Protection in Telecommunications: Privacy Risks with Smart Devices for Children. Working Paper* 2019.
8 *Bundesnetzagentur zieht Kinderpuppe 'Cayla' aus dem Verkehr* 2017; Hessel–Rebmann 2020.

The International Working Group on Data Protection in Telecommunications (IWGDPT) has issued two working documents: One addresses children's privacy issues in online services and the other analyses data protection risks in relation to children's smart devices. Both draw attention to data protection challenges and make recommendations to decision-makers, developers, and providers of online services, especially with regard to the activities of data controllers, data protection authorities, responsible persons, and standardization bodies.[9]

A study commissioned by the German Standards Institute (DIN) revealed key consumer expectations for smart toys to support the standardization process.[10] The expectations can be paralleled with the data protection principles of the General Data Protection Regulation[11] (henceforth: GDPR) and with the provisions of individual articles, in particular Article 25 on data protection by design and by default and Article 32 on security of processing. However, practice shows that personal data in the case of toys is not processed on the basis of the legislation in force. The wide range of risks associated with the use of smart toys and confirmed by studies suggests that they threaten children's privacy.

In order to address vulnerabilities, companies can designate contact points for reporting misuse. Sadly, in 2018, more than 90% of IoT devices were not connected to this option. This data, together with the privacy and data security risks identified by professional organizations, proves that throughout human history, the notion that industry will regulate itself is doomed to failure.[12] It is therefore up to legislators to ensure the protection of children's privacy and personal data with a single legislative framework. The risks related to the handling and storage of data show that the current regulation does not fully serve the protection of children's personal data, which may raise product safety problems.

The study would like to find out which EU norms in force can protect the personal data of children using smart toys and to what extent it obliges economic operators to establish adequate protection. On the one hand, the aim of the examination was to prove how inadequate and incompetent the current legislative framework was to handle the above-mentioned problems and, on other hand, to highlight the need for a specific regulation. In addition, we will examine the latest legislation of the European Union.

9 *International Working Group on Data Protection in Telecommunications: Protecting the Privacy of Children in Online Services. Working Paper* 2019; *International Working Group on Data Protection in Telecommunications: Privacy Risks with Smart Devices for Children. Working Paper* 2019.

10 Rauber–Thorun 2019. 17–36.

11 *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)*. OJ L 119 4.5.2016. 1.

12 Winder 2018.

2. The Toy Safety Directive and Smart Toys

In terms of scope, Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (henceforth: *Toy Safety Directive*)[13] applies to products designed or intended exclusively or not exclusively for toy use by children under fourteen years of age.[14] Smart toys fall within the scope of the Toy Safety Directive, as they are electronic devices specifically designed for children and constitute toys in themselves.[15] This means smart toys are designed for playing purposes and the online feature is added to the original doll, teddy bear, etc.

However, the Toy Safety Directive does not contain provisions on the protection of privacy or personal data protection for smart toys. Although it has been amended twelve times so far, and every five years Member States evaluate the experience gained in applying it, there has been no proposal for smart toys. The summary of the Commission's evaluation stresses that the Directive focuses on the protection of children's health, i.e. a physical characteristic, and that, consequently, devices connected to the Internet, including smart toys, fall within the scope of the Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonization of the laws of the Member States relating to the market of radio equipment and repealing Directive 1999/5/EC[16] (henceforth: *RED*).[17] In doing so, the Commission argued that smart toys for children are products whose intrinsic toy safety requirements are regulated by the Toy Safety Directive; requirements related to online services, including privacy and personal data protection, are regulated by the RED. The boundaries between toys as products and services closely related to them are blurred during digitization, resulting in a so-called[18] hybrid product, a hybrid toy. In hybrid toys, the EU has identified the nature of online services as a stronger, multifaceted problem as opposed to the toy function, placing the former under a general law and the latter under a specific piece of legislation.

13 *Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys*. OJ L 170, 30.6.2009. 1–37.

14 *Toy Safety Directive* Article 2(1).

15 Annex I.14 of the *Toy Safety Directive*.

16 *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*. OJ L 153, 22.5.2014. 62–106. Hungary amended Act C of 2003 on Electronic Communications on several points on the basis of Act CLXVIII of 2016 on the Amendment of Certain Acts Related to Electronic Communications and Consumer Protection. Related Regulation: 2/2017. (I. 17.) NMHH Regulation on radio equipment.

17 European Commission 2020.

18 Rauber–Thorun 2019. 17–18.

3. Smart Toys under the RED

The RED establishes a regulatory framework for the marketing and putting into service of radio equipment in the European Union.[19] Radio equipment is an electrical or electronic product intended to emit and/or receive radio waves for the purposes of radio communication and/or positioning or an electrical or electronic product which must be supplemented by accessories, such as antennas, in order to emit and/or receive radio waves.[20] Consequently, where a smart toy communicates via a radio link, such as Bluetooth or Wi-Fi, it is considered radio equipment and falls within the scope of the RED.

What are the requirements of the RED to protect privacy and personal data with regard to smart toys? An essential requirement is that radio equipment should be fitted with security devices to protect the personal data and privacy of users and subscribers before it is placed on the market.[21] Manufacturers should be able to meet these requirements: all economic operators intervening in the supply and distribution chain should take appropriate measures to ensure that only radio equipment that is in conformity with this Directive[22] is made available on the market. Since the requirements for the protection of privacy and personal data cannot be sufficiently achieved by the Member States but can rather be better achieved at a Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty of Lisbon,[23] whereby the RED empowers the Commission to adopt measures. In this context, a public consultation was carried out and an impact assessment was made on Internet-connected radio equipment and wearable radio equipment on behalf of the Commission, focusing specifically on the protection of personal data and privacy.[24]

The purpose of the inquiry was to determine whether the Commission should activate regulatory measures or delegated acts. During the related assessment, a number of vulnerabilities and risks were identified, mainly in consumer IoT devices. In order to address existing regulatory gaps, the impact assessment study considered a number of options, among which it argued that the Commission should adopt a legal act to ensure the protection of personal data, the provisions of which should make the existence of security protection a condition for market access. These requirements, together with 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

19 *RED*, Article 1(1).
20 *RED*, Article 2 para. (1), point (1).
21 *RED*, Article 3, paragraph 3, point (e).
22 *RED*, Recital (27).
23 *RED*, Recital (73).
24 *Radio Equipment Directive*.

repealing Directive 95/46/EC (henceforth: GDPR),[25] the ePrivacy Directive, and the forthcoming regulation would complement and uniformly require manufacturers to integrate data protection by default into their products, the technical solutions of which require the harmonization of technical standards.

In its product-based case studies, this impact assessment identified the types of Internet-connected devices in which vulnerabilities had been identified, including smart toys.[26] It not only made findings along the lines of the goals of the investigators but also pointed out the latent deficiency of the RED in that it does not take into account that children are the most vulnerable user group and does not contain any special requirements or rules pertinent to them.

The Council acknowledged the Commission's initiative for a legal act on short-term cybersecurity aspects in relation to the RED, but it also stressed the importance of assessing the need for horizontal legislation in the long term with regard to the conditions for placing radio equipment on the market and relevant aspects of cybersecurity of connected devices.[27]

4. The Cybersecurity Act and Smart Toys

We use information and communication technologies (ICT), i.e. elements or groups of elements of a network or information system (smartphones, tablets, etc.), on a daily basis and use ICT services, i.e. services consisting of transmitting, storing, querying, or managing information through network and information systems.[28] All these are underpinned by the ICT processes: all activities carried out to design, develop, provide, or maintain them.[29] In parallel with the spread of ICT, cyberattacks and crimes have increased. To prevent this and to guarantee the safe use of IT tools, the Internet and networks, a European cybersecurity certification scheme is implemented. The EU framework for the establishment of European cybersecurity certification schemes is laid down in 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 (henceforth: *Cybersecurity Act*).[30]

This legislation also covers IoT devices, including connected smart children's toys, through digitalization and connectivity. With regard to IoT products, the

25 Published in the Official Journal L 119 4.5.2016. 1.
26 *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment.*
27 Council of the European Union 2020. 7.
28 *Cybersecurity Act*, Article 2, points (12) and (13).
29 *Cybersecurity Act*, Article 2, point (14).
30 *Cybersecurity Act*, Article 1(1)(b).

Cybersecurity Act recognizes that security and resilience are not sufficiently built in, leading to insufficient cybersecurity, and that limited use of certification means that users do not have sufficient information about the cybersecurity features of ICT products, services, and processes.[31] There does not seem to be a coherent and holistic approach to horizontal cybersecurity issues such as IoT; the existing schemes show significant shortcomings and differences in terms of product coverage, assurance levels, essential criteria, and practical use, which hamper mutual recognition mechanisms within the Union.[32]

The Cybersecurity Act provides only principles, options, and a procedural mechanism for a European cybersecurity certification scheme but does not set binding requirements. However, it supports voluntary measures by the private sector, encourages manufacturers to carry out certifications, and introduces the concept of conformity self-assessment into the mechanism in this regard.[33] The economic operators concerned are encouraged to design for lifetime built-in protection, to develop it and to design user-friendly and secure settings, thereby achieving security by default.[34] This could be part of the duty of care principle, which should be further developed with industry.[35]

Given that the Cybersecurity Act currently only provides a recommendation and framework for a European certificate but does not impose obligations on manufacturers, it does not advance privacy or personal data protection for IoT devices, technologies, or smart toys in general.

5. Smart Toys and the Provisions of General Data Protection Law

The GDPR protects the fundamental rights and freedoms of natural persons and, in particular, their right to the protection of personal data.[36] This defends users and provides businesses with a clear legal framework.

The territorial scope of application of the GDPR covers all data controllers that carry out effective activities within the territory of the EU and process personal data, i.e. it protects not only the rights of EU citizens but also the data of any other person located in the EU. On the other hand, it also covers data controllers that process data of EU citizens anywhere in the world.[37] Tasks of the controller with

31 *Cybersecurity Act*, Recital 2.
32 *Cybersecurity Act*, Recital 65.
33 *Cybersecurity Act*, Recitals 79 to 82 and Article 53.
34 *Cybersecurity Act*, Recitals 12 to 13.
35 *Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* 2017. 6.
36 GDPR, Article 1(2).
37 GDPR, Article 3.

regard to the protection of personal data include implementation of appropriate technical and organizational measures for the processing of personal data in accordance with the GDPR. With these measures, it implements data protection by design and by default, guarantees data security, and, if necessary, carries out a data protection impact assessment.[38]

Data protection by design and by default serves the effective implementation of the principles governing data processing; therefore, producers of products, services, and applications should be encouraged to take into account the right to the protection of personal data during their design and development and to ensure that controllers and processors comply with their data protection obligations.[39]

GDPR provisions are also relevant in the context of IoT devices, including smart toys, but the best interests of children also prevail in the GDPR regulatory system. Children are among the consumer groups in need of special protection in the field of data protection, which the GDPR justifies by the fact that they may be less aware of the risks, consequences, and safeguards and rights associated with the processing of personal data.[40] It follows that the EU legislature separates children as users from their legal guardians and requires compliance with specific provisions relating to children's consent – information society services, that is to say, services normally provided for remuneration, at a distance, by electronic means, and at the individual request of the recipient.[41] Based on this, data processing related to the use of smart toys also falls within this scope since the devices use online services during their operation.

As a general rule, a child may independently give his/her consent to processing when he/she has reached the age of sixteen – Hungary regulates according to this principle –, but Member States may set a lower age, but not lower than the age of thirteen. In the case of a child under the age of sixteen, the processing of his/her personal data is lawful only if and to the extent that consent has been given by the holder of parental responsibility over the child.[42] Operators may develop appropriate methods to monitor this themselves, but they or organizations representing categories of processors may draw up codes of conduct.[43]

The fact that the processing of personal data of children under the age of sixteen has been authorized by their legal representative does not mean that the status of legal representative is absolute or takes unconditional precedence over that of the child since the best interests of the child remain the primary consideration even

38 GDPR, Chapter IV.
39 GDPR, Recital (78).
40 GDPR, Recital (38).
41 The GDPR establishes the definition by reference to Directive 2015/1535 of the European Parliament and of the Council.
42 GDPR, Article 8(1).
43 GDPR, Article 40(2)(g).

if they need representation in exercising their rights.[44] Once the child has reached the age required for digital consent, he/she will have the possibility to withdraw consent himself/herself; the controller shall inform the child of this possibility.[45] The right to be forgotten also applies to a data subject who gave consent to the processing of his or her personal data as a child or who gave consent by his or her legal representative but later wishes to remove the personal data in question from the Internet.[46]

In order to be able to take an appropriate decision to grant or even refuse prior consent, the data subject should be well informed about the subsequent processing. With regard to the achievement of this objective, the preamble to the GDPR states that the processing of personal data must be transparent to data subjects in addition to lawfulness and fairness.[47] The principle of transparency requires that the information provided to the data subject be concise, easily accessible, and easy to understand and that it be drafted in clear and plain language and, where necessary, presented visually.[48] Elements of clear and understandable language are: child-centred vocabulary (common words; explanations), tone and style (contact with children; immediacy; avoidance of multiple complex sentences, foreign words). For a child-friendly approach, the Article 29 Data Protection Working Party recommends an example of a *UN Convention on the Rights of the Child in a Child-Friendly Language*.[49] The information must comply with these requirements even if the consent to data processing is given by the holder of parental authority, since children are the target group.

The GDPR states that special protection applies when using personal data of children for marketing purposes and for creating personal or user profiles.[50] Children who use smart toys can also easily become targets for businesses seeking ever-greater profit: several of the toys tested had pre-programmed phrases embedded in them that advertised commercial products.[51] Although the GDPR does not prohibit the use of children's personal data for marketing purposes,[52] the processing must still be lawful, fair, comply with data protection principles, and not exploit the child's age-related vulnerability. Children have the right to

44 Zavodnyik 2019. 130.
45 *Guidelines 05/2020 on Consent under Regulation 2016/679. Version 1.1.*
46 GDPR, Recital (65) and Article 17(1)(f).
47 GDPR, Recital (39).
48 GDPR, Recital (58).
49 *Guidelines 05/2020 on Consent under Regulation 2016/679. Version 1.1.*
50 GDPR, Recital (38).
51 #*Toyfail: An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys* 2016. 21–23.
52 In Hungary, the following legal norms serve to protect children in relation to advertising: Act CLXXXV of 2010 on Media Services and Mass Media, Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Commercial Advertising Activities, relevant provisions of Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers.

object to the processing of their personal data for marketing purposes and must be informed of this right.[53]

For the purpose of behavioural advertising, in the case of applications related to smart devices, controllers should not process children's data because the child rarely understands these and therefore is unable to grant informed consent. In addition, controllers should explicitly refrain from collecting data relating to parents such as requesting and using financial information or medical data relating to family members of the child.[54]

Both the principles governing the processing of personal data and the specific rules applicable to children show that the provisions of the GDPR provide a secure background for the protection of personal data. Yet principles are being violated with regard to smart toys, as described and demonstrated by consumer protection and data protection organizations. On the one hand, the above contradiction can be explained by the fact that the GDPR was adopted in 2016 and is applied from 2018, which can be a small excuse in the case of older products since businesses have to constantly monitor and prepare for data protection processes. The authors Hessel and Rebmann argue that the reason for the problems is that the provisions of the GDPR apply to data controllers, and measures can only be directed against them, i.e. data protection authorities cannot take measures against manufacturers, suppliers, importers, or sellers. In the case of smart toys, data controllers are often East Asian companies that do not have branches in the EU or an appointed representative.[55] A similar conclusion is made in the impact assessment for radio equipment connected to the Internet, which highlights a regulatory gap: imposing fines is in the jurisdiction of data protection authorities, but national market surveillance authorities are responsible for placing products on the market and for the withdrawal of products.[56] As a solution, it is proposed that the GDPR provisions should be enforced strongly against manufacturers, especially with regard to data protection by design and by default, through fines imposed by data protection authorities, which over time will provide incentives to comply.[57]

53 *Information Commissioner's Office Consultation: Children and the GDPR guidance* 2018. 32–33.
54 Article 29 Data Protection Working Party 2013. 26.
55 Hessel–Rebmann 2020.
56 *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment* 2020. 45–46.
57 *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment* 2020. 10.

6. The Draft ePrivacy Regulation and Smart Toys

Compared to the GDPR, the forthcoming ePrivacy Regulation (henceforth: Draft ePrivacy Regulation)[58] – and the currently applicable ePrivacy Directive – aim to regulate the processing, use, and protection of personal data related to electronic communications services, especially those generated during electronic communications. While the GDPR operates as a framework regulation, i.e. it regulates the protection of personal data in a general sense, this regulation (draft) covers only the rules of one sector or a subfield, so it details, clarifies, and complements the provisions of the GDPR as a special legal act. Do the provisions of the draft ePrivacy Regulation apply to smart toys and related services?

The territorial scope of the draft ePrivacy Regulation – parallel to the relevant provision of the GDPR – covers the entire territory of the European Union, i.e. everyone who provides electronic communications services to users located in the territory of the European Union.[59] This does not require the provider to be located or established in the EU but requires a representative in the EU to be established in writing, who must be established in one of the Member States where the end-users of electronic communications services are located.[60]

Exactly which services fall within its scope can be clarified on the basis of definitions. The draft ePrivacy Regulation does not contain definitions in this respect but refers to the definitions of the European Electronic Communications Code.[61] On this basis, electronic communications services shall mean services normally provided for remuneration over electronic communications networks comprising Internet access, interpersonal communications services, and services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine communications and for broadcasting.[62] This means that the draft ePrivacy Regulation extends data protection rules for electronic communications to services already widespread at the current level of technological development and named in the draft: VOIP services, OTT services, hotspots, IoT services, and M2M.[63] It is proposed that the ePrivacy Regulation is to be applied to providers of electronic communications

58 *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).*

59 *Draft ePrivacy Regulation*, Article 3(1)(a).

60 *Draft ePrivacy Regulation*, Article 3(2) and (3).

61 *Draft ePrivacy Regulation*, Article 4(1)(b). The use of the forthcoming ePrivacy Regulation has been criticized by the European Data Protection Supervisor. See: *EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation).*

62 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 Establishing the European Electronic Communications Code (Recast). OJ L 321, 17.12.2018. 36–214. Article 2, point 4(a) to (c).

63 *Draft ePrivacy Regulation*, Recitals (1) and (11) to (13).

services and providers of public directories, and it should apply also to manufacturers of software enabling electronic communications.[64]

The draft ePrivacy Regulation extended the GDPR's definition of personal data to include electronic communications data, distinguishing between two types: electronic communications content and electronic communications metadata.[65] The former means content sent or received by means of an electronic communications service:[66] textual, visual, videographic, spoken information, etc.; the latter means data processed in an electronic communications network for the purpose of transmitting, distributing, or exchanging electronic communications content: data used to trace and identify the sender and destination of a communication, data generated in the course of providing services concerning the location of the device, date, time, duration, and type of communication.[67] Metadata does not appear to convey direct information, but in reality it can provide companies with data suitable for policy analysis. When it comes to IoT devices for kids, metadata is a treasure-trove, and for smart toys, even the time spent playing can result in important information for marketing companies, service providers, and manufacturers. According to the draft ePrivacy Regulation, both communication content and metadata are personal data and must therefore be protected and confidential: persons other than end-users are prohibited from accessing, listening, tapping, storing, monitoring, reading, or otherwise intercepting, monitoring, or processing them, unless permitted by the Regulation.[68] Electronic communications content should be protected until it reaches the end-user; after receipt of the message by the end-user, both the communication content and metadata should be erased or made anonymous.[69]

The original proposal for the ePrivacy Regulation has been amended several times, which is both a clarification and covers two problematic areas. The most controversial are the provisions on how electronic communications data and metadata are allowed to be processed and on cookies. This is because Member States prioritize different issues – to put it more harshly: 'it concerns such vital economic interests that it has yet to be adopted'.[70] However, it is already apparent that this draft regulation – although IoT devices themselves have come to the attention of the legislators – does not lay down a specific provision for children belonging to particularly vulnerable groups.

64 *Draft ePrivacy Regulation*, Recital (8).
65 *Draft ePrivacy Regulation*, Article 4(3)(a).
66 *Draft ePrivacy Regulation*, Article 4(3)(b).
67 *Draft ePrivacy Regulation*, Article 4(3)(c).
68 *Draft ePrivacy Regulation*, Article 5.
69 *Draft ePrivacy Regulation*, Recital (15a).
70 Fézer 2018. 57.

7. The Draft CRA and Smart Toys

EU decision-making bodies are increasingly recognizing that the growing penetration of IoT devices and technologies is both a key cornerstone of economic development and poses serious risks in terms of privacy and personal data protection. To address these issues, the Council supports the introduction of horizontal cybersecurity requirements in its *Council Conclusions on Cybersecurity of Connected Devices* and is committed to promoting the global competitiveness of the EU's IoT sector by ensuring the highest possible level of resilience and security. To this end, the EU Agency for Cybersecurity is working on European cybersecurity certification schemes,[71] and the Commission presented a legislative proposal on cybersecurity requirements for interoperable products.

The adoption, entry into force, and application of 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 (henceforth: *draft CRA*)[72] will greatly enhance the protection of personal data and the integrity of privacy of users of smart toys. Due to its horizontal and comprehensive approach, its scope covers all products with digital elements, including interoperable products but excluding products covered by sectoral legislation, and therefore IoT devices in general[73] and consumer goods, such as toys for vulnerable consumers, among them.[74] We have seen that most of the relevant legislation described so far does not provide sufficient protection for users because it does not impose obligations on manufacturers, but the draft CRA sets cybersecurity standards precisely for economic operators, thus harmonizing the EU legislative environment during product manufacture from design through development to the entire life cycle, including vulnerability detection, management, and updates. The obligation of *security by design* will apply not only to manufacturers but also to other actors in the supply chain: importers and distributors.[75] However, the European Economic and Social Committee has drawn attention to the fact that the provisions of the draft CRA may overlap with other existing legislation.[76]

National authorities will exercise market surveillance in relation to this Regulation on the territory of the Member States and may take measures in relation to any product with inadequate cybersecurity features: requiring the

71 Council of the European 2020. Points 7, 9a, and 16.

72 *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).*

73 *Draft CRA*, Article 2.

74 *Draft CRA*, Recital (8).

75 *Draft CRA*, Chapter II.

76 *Opinion of the European Economic and Social Committee on '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'.*

relevant economic operator to eliminate the risk, recall, or withdraw the product from the market and imposing fines on companies that place the product on the market. As the draft CRA applies to all products with digital elements, it will also apply to smart toys. This means that while the sale of the 'Cayla' doll could only be prohibited in Germany on the basis of telecoms legislation – due to an unauthenticated Bluetooth connection –, in the future, the national supervisory authorities in the Member States of the European Union will be able to act on the basis of the CRA for any smart children's toy.

8. Final Thoughts and Conclusions

Smart toys are subject to several pieces of EU legislation, each with different approaches to reducing the risks to personal data protection and privacy associated with the products concerned. The Toy Safety Directive is not relevant in this respect, and the Cybersecurity Act only provides a recommendation and framework for a European certificate but does not impose obligations on manufacturers. The GDPR data protection principles and provisions ensure the protection of personal data related to the use of IoT devices, but some smart toys are not GDPR-compliant because its requirements apply to data controllers and not to manufacturers. The draft ePrivacy Regulation includes IoT devices within its scope if signals are transmitted over a publicly available electronic communications network. The regulation is planned to apply to software vendors in addition to service providers.

The key question with regard to the protection of children's privacy and the protection of their personal data is whether we succeed in requiring all economic operators involved in the supply and distribution chain, especially manufacturers, to integrate data protection by default into smart toys. The expected provisions of the Commission legal act related to RED, the GDPR, and the ePrivacy Regulation, which will replace the ePrivacy Directive, complement each other.

The other key question is whether it will be enough that only the GDPR sets out a special requirement regarding the protection of children's privacy and personal data. Looking at the relationship between GDPR and the draft ePrivacy regulation, the answer is affirmative, but this element is completely absent in relation to the RED of the Toy Safety Directive, as the RED does not take into account the vulnerability of children. In this direction, the legislator should strengthen the protection of privacy and personal data of children using smart children's toys.

The draft CRA, which will uniformly require manufacturers and distributors to comply with cybersecurity standards for all products with a digital element, is encouraging. However, some provisions of the draft CRA overlap with other EU regulations as regards the processing of personal data.

Therefore, the fact that EU legislative bodies are trying to tackle the rampant offshoots of the digital world using traditional legal frameworks does not bring us any closer to solving the problems, pushing regulators towards fragmentation instead of adopting a comprehensive legislation. In addition, the time factor is also key. On the one hand, legislation is unable to keep up with the accelerating pace of development, and, on the other hand, provided that the draft even becomes a living, effective law, a long time will pass before it will be possible to amend it. Addressing this issue calls for a new approach, for the introduction of a new regime, for example, by legislating a special product safety standard. And as long as the plans become reality, while the search for a path is ongoing, parents can also do something to keep their children's and their own data safe – by making conscious purchasing decisions, by acting responsibly online, by educating children to do the same from an early age.

References

ARTICLE 29 DATA PROTECTION WORKING PARTY. 2013. *Opinion 02/2013 on Apps on Smart Devices, 00461/13/EN WP 202*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (accessed: 26.04.2021).

COUNCIL OF THE EUROPEAN UNION. 2020. *Council Conclusions on the Cybersecurity of Connected Devices, 13629/20*. Brussels, 2 December 2020. https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf (accessed: 26.04.2021).

DÖMÖS, Zs. 2015. *Többmillió gyerekfotót loptak hackerek*. https://www.origo.hu/techbazis/20151201-gyermek-hack-biztonsag-privatszfera-barbie.html (accessed: 12.03.2021).

EUROPEAN COMMISSION. 2020. *Commission Staff Working Document Executive Summary of the Evaluation of Directive 2009/48/EC of the European Parliament and of the Council on the Safety of Toys*. Brussels, 19.11.2020. SWD(2020)288 final.

FÉZER, T. 2018. A fogyasztók adatainak és privátszférájának védelme elektronikus környezetben [Protecting Consumer Data and Privacy in the Electronic Environment]. In: Szikora, V.–Árva, Zs. (eds), *A fogyasztók védelmének új irányai és kihívásai a XXI. században*. Debrecen: 57.

HAJNAL, Zs. 2011. Fogyasztóvédelmi politika 169. cikk [Consumer Protection Policy Article 169]. In: *Az Európai Unióról és az Európai Unió működéséről szóló szerződések magyarázata*. Budapest. 2419–2433.

2019. A fogyasztói szerződés alanya az aktuális jogalkotás középpontjában: a fogyasztó. In: Szikora, V. (ed.), *Kihívások és lehetőségek napjaink magánjogában*. Debrecen. 197–212.

HESSEL, S.–REBMANN, A. 2020. Regulation of Internet-of-Things Cybersecurity in Europe and Germany as Exemplified by Devices for Children. *International Cybersecurity Law Review* (1): 27–37. https://doi.org/10.1365/s43439-020-00006-3 (accessed: 12.03.2021).

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS. 2019. *Privacy Risks with Smart Devices for Children. Working Paper*. Bled. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2019/2019-IWGDPT-Working_Paper_Smart_Devices.pdf (accessed: 24.03.2021).

RAUBER, J.–THORUN, C. 2019. Digitalisierungsaspekte und Verbraucheranforderungen in Bezug auf „smartes" Spielzeug – Umsetzung in der Normung. In: *Ergebnisbericht für den DIN-Verbraucherrat*. Berlin. 14–16. https://www.din.de/resource/blob/858786/26e9eab19c973fe91bc6ab61b71db289/studie-des-din-vr-verbraucheranforderungen-an-smarte-spielzeuge-in-der-normung-data.pdf (accessed: 14.04.2021).

WINDER. D. 2018. *The Silence of the Brands: 90% of Consumer IoT Vendors Don't Let Researchers Report Vulnerabilities*. https://www.forbes.com/sites/daveywinder/2018/12/13/the-silence-of-the-brands-90-of-consumer-iot-vendors-dont-let-researchers-report-vulnerabilities/ (accessed: 28.04.2021).

ZAVODNYIK, J. 2019. Protection of Personal Data of Child Consumers. In: Szikora, V.–Árva, Zs. (eds), *Redesign – Consumer Regulatory Models, Digitalization, Data Protection*. Debrecen. 130.

*** *#Toyfail: An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys*. 2016. https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf. (accessed: 02.04.2021).

*** *Bundesnetzagentur zieht Kinderpuppe „Cayla" aus dem Verkehr*. 2017. https://www.deutschlandfunk.de/versteckte-ueberwachungsmoeglichkeit-bundesnetzagentur-100.html#:~:text=Die%20Bundesnetzagentur%20hat%20H%C3%A4ndler%20in,Sendeanlagen%20in%20Kinderspielzeug%E2%80%9C%20verboten%20sind. (accessed: 24.03.2021).

*** *EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*. https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf (accessed: 02.05.2022).

*** *Guidelines 05/2020 on Consent under Regulation 2016/679. Version 1.1.* 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (accessed: 26.04.2022).

*** *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment*. 2020. https://ec.europa.eu/docsroom/documents/40763 (accessed: 26.04.2021).

*** *Information Commissioner's Office Consultation: Children and the GDPR Guidance (2017–2018).* 2018. https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf (accessed: 02.05.2022).

*** *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*. Brussels, 2017. 9. 13. JOIN(2017) 450 final.

*** *Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020'*. (COM(2022) 454 final — 2022/0272 (COD)), EESC 2022/04103, OJ C 100, 16.3.2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2023.100.01.0101.01.ENG (accessed: 16.03.2023).

*** *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).* COM/2017/010 final – 2017/03 (COD). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010 (accessed: 02.05.2022).

*** *Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU)*. 2019/1020 COM/2022/454 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454 (accessed: 02.05.2022).