Rocco Panetta, Federico Sartore:

Data protection for networked and robotic toys – a legal perspective

Abstract:

This paper is aimed to understand the state of the art and the resulting consequences of the legal framework in Europe, with regard to the protection of children's data. Especially when they interact with networked and robotic toys, like in 'My friend Cayla' case. In order to evaluate the practical implications of the use of IoT devices by children or teenager users, the first part of the paper presents an analysis of the international guiding principles of the protection of minors, a category which enjoys a higher level of protection of their fundamental rights, due to their condition of lack of physical and psychological maturity. Secondly, the focus is moved upon the protection of personal data of children. Only after confronting previous data protection legal instruments and having compared them with the novelties set forth in General Data Protection Regulation, it is reasonable to assume that new provisions such as "privacy by design" principle, adequacy of security measures and codes of conduct, can support data controllers in ensuring compliance (in line with the accountability principle) in the field of IoT toys. In conclusion, the paper supports a view of Data Protection Authorities as a relevant player in enhancing these renovated tools in order to achieve the protection of children's rights, as to ensure their substantial protection against the threats of the interconnected world.

Agenda:

Authors:

Rocco Panetta

- Managing Partner at Panetta & Associati law firm, International Association of Privacy Professionals, Country Leader Italy and Board of Directors Member. Email: r.panetta@panetta.net

Federico Sartore

- Associate at Panetta & Associati law firm, Ph.D. student at Maastricht University. Email: f.sartore@panetta.net

ISSN 1614-1687

Introduction

In February 2017, the German Federal Network Agency (*Bundesnetzagentur*) stated that 'My friend Cayla' – an interactive doll manufactured by an American company – constituted a perfect example of "*unauthorised wireless transmitting equipment*"[1]. Accordingly, German regulators feared that smart toys of this kind, with concealed microphones and cameras, may constitute a severe threat to fundamental rights of children and their families.

And there is more, no highly-sophisticated hacker attack was needed to breach security measures of the connected database: due to an error of configuration it started leaking children personal data, later estimated in around half a million records.

Moreover, the case of Cayla is not an isolated threat, security failures were discovered in the Furby Connect, i-Que Intelligent Robot, Toy-Fi Teddy and CloudPets[2]. In all these cases the vulnerability was represented by a flawed Bluetooth connection, resulting in a complete lack of security with the possibility for anyone to gain access – without pin, password or other forms of authentication – to the toy. Again, no sophisticated hacking techniques were needed to pose a serious threat for the security and privacy of kids.

Once again, public authorities and commentators have moved the spotlight of inquiry on manufacturers of the so-called IoT devices and on the fundamental role played by data controllers. In fact, dystopian sceneries of mass-surveillance are simply an actual threat to our rights and freedoms. Cases like the switch of 'My friend Cayla' into a disturbing and Orwellian Pandora's box have to be taken as the last call for investing economically and culturally on cybersecurity and data protection at societal level.

These alarming facts represent the tip of the iceberg of one of the foremost issues related to robo-connected-toys: guaranteeing the maximum level protection and safeguard for personal data collected during the interactions between children and toys.

Indeed, an interesting question consists in asking whether this should be addressed as an ethical or a legal issue, and to what extent.

Beside the endless debate on law and ethics, the protection of privacy and personal data has to be considered as a fundamental right and, for this reason, deeply permeated by natural law doctrines. And no substantial difference should be found in assessing the nature of this fundamental right for an adult or a child; at most, one could argue that the special declination of fundamental rights for children is provided by other fundamental rights, specifically addressing the condition of the child and thus combining themselves. In other words, the protection of children's data is both a matter of law and ethics; in particular, of ethics in their legal transposition by means of fundamental rights legal instruments.

Differently from what is commonly said and written, EU regulators have not been left behind by the fast-growing pace of technology development. Under this perspective, the Regulation (EU) 2016/679 (the '**GDPR**'), that will come into force from 25 May 2018, consolidates the fundamental data protection principles, confirms the utmost relevance of setting appropriate safeguards for childhood and – provided a number of guarantees

[1] The press release of *Bundesnetzagentur* on the point can be found at: https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2017/17022017_cayla.pdf?__blob=publicationFile&v=2

[2] R. Smithers, *Strangers can talk to your child through 'connected' toys, investigation finds*, The Guardian, 14 november 2017, available at: https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children.

– lighten some burdensome obligations for data controllers under the threat of significantly increased pecuniary sanctions[3].

The purpose of this article is to sketch a map of the legal protection accorded to children's data. After a brief description of the traditional legal framework, the main novelties brought by the GDPR on the point will be analysed in order to set the stage for the current state of art of children's data protection.

Guiding principles for the protection of children

Although no doubt persists with regard to the full attribution of fundamental rights to children, these rights should be also considered and interpreted against the special situation and characteristics of childhood. In this sense, simplifying, legal systems are prone to consider the child in a double-faced perspective: static and dynamic.

Where the static nature is represented by the fact that the child is a person who has not achieved yet physical and psychological maturity, the dynamic aspect is reconnected to the state of constant development of the child toward adulthood. For this reason, any discourse over children rights should address and take into consideration both these perspectives, a sort of biphasic attention of the legislator.

Taking into account the fundamental principles regulating the rights of the child, while some of them are contained within the most fundamental applicable international instruments[4], other can be found in acts specifically drafted to protect the rights of the child[5]. Regardless to the source, they can be identified – within the purpose of this article – as follows.

Best interest of the child

The 'best interest of the child' represents the core principle with regard to children's fundamental rights. Enshrined in the UN Convention on the Rights of the Child (Article 3), it has been reaffirmed in other international instruments. Its rationale is strictly linked to the unachieved physical and psychological maturity. In such a situation, the interest of the child is a useful criterion in order to avoid harmful generalizations, concretely setting a balancing exercise.

Protection and care necessary for the wellbeing of the child

This principle and its fundamental role are extremely interlaced to the above-mentioned immaturity of the child and the deriving vulnerability. This status of being defenceless shall be therefore compensated by adequate

[3] Pursuant to art. 83 of the GDPR, infringement of the provisions of the Regulation may lead to different tiers of administrative fines. The first, for less serious violations, provides for fines up to EUR 10.000.000 or, in case of undertakings, up to the 2% of the total worldwide annual turnover. The second, for gross violations, provides for fines up to EUR 20.000.000 or, in case of undertakings, up to the 4% of the total worldwide annual turnover.

[4] E.g., articles 25, 26.3 of the Universal Declaration of Human Rights (1948), article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) and article 24 of the EU Charter of Fundamental Rights (2000).

[5] *Inter alia,* the Geneva Declaration on the Rights of the Child (1923), the UN Convention on the Rights of the Child (1989), the European Convention on the Exercise of Children's Rights (1996).

care and protection. Consequently, the focus for the full realization of this principle should be moved upon the subjects entitled to guarantee this right: (from micro to macro level) family, State and society[6].

From a data protection perspective, the pursue of this principle may entail and require processing operations of personal data or, conversely, the protection from harmful processing activities.

Representation

As it is easily comprehensible, the exercise of children's rights needs some form of legal representation. However, the application of the corollaries of the dynamic nature of the legal dimension of the child requires children's consultation on matters impacting on them and their will should be taken into account, proportionally to their stage of development. In the context of the protection of children's data, the concept of representation is crucial because it identifies an interposed data subject who has the duty to understand the meaning of the information made available by the controller and to provide the consent where needed. In fact, the first line of defence for the protection of personal data of the child is represented by the awareness of parents and guardians of the fundamental role they play in guaranteeing this protection.

Right to participate

The other side of the right to be represented consists in the right to be consulted, in relation to the degree of personal development. This right of consultation can be addressed as a duty of taking into account the child's belief and opinion, without necessarily submit to them.

In data protection terms, the application of this principle may result in a duty of taking into account the child's will of making use of a certain good of service, that may entail processing activities on personal data. However, it is highly implausible that a child may really comprehend the meaning and relevance of sharing personal data.

The scope of traditional data protection legislation for children

In the context of the main directives composing the traditional data protection legal framework – the directive 95/46/EU (the "Data Protection Directive") and the directive 2002/58/EU (the "e-Privacy Directive) – data protection rights of the children are not mentioned. The subjective scope of application of the directives broadly refers to any 'natural person', therefore including also children, without distinctions in terms of legal discipline.

This lack of attention of the European legislator resulted in a number of open questions with regard to the peculiarity of the status of the child in the context of the protection of personal data, both in terms of the definition of the degree of individual maturity as well as the requirement for representation in legal acts. In other words, the traditional data protection legislation was in particular lacking on two different layers: (1) the floating degree of consciousness determining when children can start managing their own personal data and (2) the provision of *ad hoc* guarantees in order to reinforce the level of protection for children's data.

[6] The fundamental nature of this right is confirmed by the primary consideration given by the Universal Declaration of Human Rights (Article 25), the International Covenant on Civil and Political Rights (Article 24), the International Covenant on Economic, Social and Cultural Rights (Article 10.3), and the EU Charter of Fundamental Rights (Article 24).

Consequently, rules and regulations on the validity of consent provided by kids had to be drawn from national legislation and the regulatory vacuum had to be filled by the intervention at national or EU level of Data Protection Authorities of the Member States. In particular, the Working Party *ex* art. 29 – the advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the Commission – issued the Opinion 2/2009, specifically addressing the state of the art for the protection of children's personal data[7].

In particular, with regard to the legal requirements for obtaining personal data of children in the online environment, a recent study conducted across the EU Member States concluded that many countries have not developed specific legal requirements[8]. In Spain, it is foreseen an obligation for data controllers to obtain parental consent to process personal data of children under the age of 14[9]; while in the UK the age threshold is set at 12[10].

Increased data protection safeguards for children under the GDPR

The renewed importance of protecting personal data of children is mentioned several times within the GDPR. However, most of them merely represent programmatic statements and it is likely that most of the substantive limitations to the processing of children data will come from either existing or new national laws or codes of conduct.

Therefore, the scenario arising from the traditional data protection legal framework has been only partially innovated by the GDPR, considering how the provisions of the Regulation do not provide for particularly wider harmonisation on the point. Thus, the major provision that can be found regarding the processing of children data is Article 8.1 of the Regulation, which identifies a general obligation for data controllers of attaining the parental consent to lawfully process personal data of a child where (s)he is below the age of 16 years[11] and the request for consent applies in relation to the offer of information society services directly to a child. It is undoubtable that services provided by connected toys represent information society ones and, accordingly, the awareness and control abilities of parents over their children personal data will become a crucial factor when facing the robo-toys dilemma (i.e. how to protect the children from abusive technologies).

On the other hand, data controllers are asked, pursuant to Article 8.2 of the GDPR, to make 'reasonable efforts' in order to assess and verify that consent has been given or authorized by the holder of parental responsibility over the child, taking into account the current state of art for technology. Moreover, the applicability of the 'legitimate interest' of the controller – as legal basis to undertake processing activities – finds a narrower scope of application when conflicting interests, rights or freedoms pertain to a child[12].

---

[7] Opinion 2/2009 of the WP 29 on the protection of children's personal data (General Guidelines and the special case of schools), available at: http://194.242.234.211/documents/10160/10704/1619292.

[8] N. Fulford, '*Survey: Consent to the Processing of Children's Data Across the EU'* (2011) 11(2) Privacy and Data Protection 13.

[9] Royal Decree 1720/2007, of 21 December, which approves the regulation implementing Organic Law 15/1999, of 13 December, on the protection of personal data.

[10] Information Commissioner's Office, Personal Information Online Code of Practice (2010), 15.

[11] The provision applies where the processing activities of personal data are based on consent pursuant to article 6.1 (a) of the GDPR and Member States can set a lower age threshold as low as 13.

[12] Article 6.1, (f) considers processing of personal data lawful when "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*"

With regard to Article 8, some concerns were raised about the impact of this provision on key principles of human rights law[13]. In particular, three aspects of the provision were found to struggle with human rights principles: (1) the existence of a bright-line rule to determine the degree of maturity of the child; (2) the fact that Article 8 foresees no way for the child to express his own views regarding the data processing operation, leaving the responsibility to consent exclusively on parents; (3) the limitation of self-determination of the child reconnected to the invasion of their personal sphere by the parents in order to exercise their control. These criticisms are formally correct and embraceable; however, a certain degree of generalization cannot be avoided during the draft of a general regulation and the gap between the abstract and general rule and the actual behaviour of children and parents should be filled by soft law instruments – such as guidelines, recommendations and clarifications from the DPAs and other regulatory bodies.

Moreover, the GDPR also takes into consideration the provisions of concise, transparent and easily comprehensible information notices to data subjects, particularly with respect to children. Article 12 of the Regulation sets the principle that is further expanded in its meaning by Recital 58: "*Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand*". Given the well-known questions and doubts regarding the effectiveness of traditional information notices for adults, it is highly unlikely that children – even if teenagers or young adults – will benefit from simplified notices[14].

Finally, the processing of particular categories of children's data does not receive a specific and distinct regulatory framework due to the fact that processing of these categories of data involves a higher degree of risks for rights and freedoms of the individuals and, consequently, requires *per se* additional and enhanced safeguards, irrespectively to the status of the data subject.

Additional provisions regarding networked toys and IoT

The slightly different status of personal data of children is just a very limited part of the whole data protection legal framework, designed and implemented to protect individuals against the threats of an ubiquitous and always connected world.

In particular, the GDPR introduces the widely-discussed concept of 'Data Protection-by-design'[15]. In brief, data controllers – taking into account the state of the art, the cost of implementation and the nature of processing as well as the risks for rights and freedoms of natural persons – will be required to implement appropriate technical and organisational measures, designed to integrate data protection principles, such as data minimisation, necessity, transparency and connected necessary safeguards, into the processing operations[16].

Although the nature of the provision set by Article 25 is of being generally applicable, Internet-of-Things (IoT) represents the field on the front line to test the potentiality of embedding data protection and respect for data subjects' fundamental rights into the design of industrial processes and real objects. In these terms, the

[13] L. Jasmontaite, P. De Hert, "*The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet*", International Data Privacy Law, 2015, Vol. 5, No. 1.

[14] That would actually benefit data subjects as a whole in line with principles of transparency, extended user control and fairness of the processing.

[15] The origins of the concept can be found in the paper *Privacy-enhancing Technologies: the path to anonymity* (1995) by a joint team of the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and the Netherlands Organisation for Applied Scientific Research.

[16] See Article 25 of the GDPR.

circumstance of a good or service to be aimed to minor customers shall not be treated indifferently by the manufacturer. Curiously, while the obligation of implementing data protection by design features set by Article 25 is referred only to the controller, the Recital 78 sets a broader scope of application for the principle, encouraging also producers and manufacturers to design their products having in mind the respect for users' privacy, with special attention toward children. The choice of the legislator is clearly to identify in the controller the only subject directly responsible for the implementation of the "technical and organisational measures" required by the Privacy-by-Design principle. However, manufacturers and data processors should be prepared for a similar implementation because they will likely be asked by data controllers to act in this sense at a contractual level.

Therefore, the protection of children's data can be imagined as a multi-layered structure. The first basic level consists in the entire body of provisions generally applicable to any natural person. The second is represented by the ad hoc provisions for children with regard to consent and information notice to be provided. Finally, the top-level can be described as all the open provisions which require controllers and processors to adapt their processes to the movable parameter of adequacy of the safeguards to factual elements[17].

This third level is undoubtedly the context where relevant players will be asked to seriously take into account the general principles protecting the child. A strong link between the best interest of the child and these open provisions shall be established. Not only with regard to the above-mentioned Article 25 and its demand for a technological development able to adapt itself to the higher degree of risk posed by the interaction of a child with the "machine", but also referring to the important field of security. In particular, Article 32 of the GDPR, setting the general rule on security measures, openly refers to "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*", where the risk has to be assessed with regard to a number of factors and the fact that the data subject is a child cannot be excluded from consideration.

Furthermore, it has to be considered that the newly introduced tool represented by 'Codes of conduct' directly addresses the processing of children data. If well implemented and designed, codes of conduct may represent a form of proactive, ethical and competitive form of compliance for data controllers in the robo-toys market. Indeed, codes of conduct have been introduced by Article 40 of the GDPR and can be considered a form of *soft-law*, designed by the EU legislator in order to adjust the rules of the GDPR according to the needs and risks of specific sectors of the industry or categories of controllers or processors. The adherence to a code of conduct may be used by controllers and processors as an element whereby demonstrating compliance with the requirements of the GDPR. To this regard, the field of IoT and, in particular, IoT applied to toys may represent a perfect example of a sector which requires *ad hoc* specifications and differentiations of rules of detail in relation to the higher degree of risk necessarily implied by these technologies and categories of recipients.

Conclusion

The purpose of this brief analysis is to provide a sketch of the actual situation: the degree of risk for the rights and freedoms of children is certainly getting higher with the technological development, threatening those fundamental principles ingrained in our legal system. However, the reform of the legal framework for EU did not omit to update the rules, setting both specific provisions and open parameters to permit a better adaptability of data protection norms. As a result, from now on, a healthy and fast-growing market of robo-toys cannot

[17] Art. 25 of the GDPR sets as relevant parameters: (a) the state of the art, (b) the cost of implementation, (c) the nature, scope, context and purposes of processing, (d) the risks for rights and freedoms of natural persons posed by the processing.

neglect the respect of the specific provisions on children's data, the implementation of security measures, the principle of data protection by design and the opportunities provided by codes of conduct.

On the other hand, this open nature of important provisions – such as Article 32 on security measures – necessarily needs further specification by Data Protection Authorities in order to become really effective. Given the impressive sanctioning firepower provided by the GDPR to the DPAs[18], they should be in a perfect position to enact and make effective the provisions of the Regulation. In fact, cases such as 'my friend Cayla' are extremely serious and alarming, revealing that some players on the market still have not fully comprehended the importance of setting lawful processing activities and the actual level of risk posed by their misbehaviour for the special category of individuals represented by children. For this reason, it is important for DPAs to couple their guiding activity with effective enforcement toward those who violate the general rules of the Regulation and, more importantly, the specific rules regarding children's data.

References

Bundesnetzagentur. Bonn, 17 F Ebr Uary 2017 Page 1 of 2 Bundesnetzagentur Removes Children's Doll "Cayla" from the Market . 17 Feb. 2017, www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2017/17022017_cayla.pdf? blob=publicationFile&v=2.

Fulford, Nicola. "Survey: Consent to the Processing of Children's Data Across the EU." Privacy and Data Protection , vol. 11, no. 2, 2011.

"Opinion 2/2009 of the WP 29 on The Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)." 194.242.234.211/documents/10160/10704/1619292.

Palfrey, John G., and Urs Gasser. Born Digital: Understanding the First Generation of Digital Natives. Read How You Want, 2011.

Smithers, Rebecca. "Strangers Can Talk to Your Child through 'Connected' Toys, Investigation Finds." The Guardian, Guardian News and Media, 14 Nov. 2017, www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children.

Acts and authorities cited

EU Charter of Fundamental Rights (2000).

European Convention on the Exercise of Children's Rights (1996).

Geneva Declaration on the Rights of the Child (1923).

Information Commissioner's Office, Personal Information Online Code of Practice (2010), 15.

International Covenant on Civil and Political Rights (1966).

International Covenant on Economic, Social and Cultural Rights (1966).

[18] See note 3.

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).

UN Convention on the Rights of the Child (1989).

Universal Declaration of Human Rights (1948).