EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Smart toys and minors' protection in the context of the Internet of everything

MARIA CRISTINA GAETA
Research Fellow in Private Law at the University Suor Orsola Benincasa of Naples
Lawyer in Naples

Abstract

Smart toys are devices with the appearance of traditional children's toys (e.g. dolls or cuddly toys) but they are capable of interacting with the surrounding environment, connecting to the Internet and using technological systems. They are robots, characterized by a more or less developed level of automation, to the point that the most recent models of connected toys are equipped with artificial intelligence. Although smart toys are fun and sometimes even educational games, they are still tools that collect, process and communicate data, with possible risks, especially for minors. Indeed, first of all it is very concrete and serious the risk of unlawful processing of minors' personal data, but also the risk of hacker attacks, issues related to possible emotional bonds between the minor and the toy, as well as psychical manipulation.

This paper will deepen the concept of smart toys, starting from the characteristics and the technical aspects and then moving on to the analysis of their possibilities and risks, in order to identify the possible legal remedies to be foreseen for protecting minors.

Keywords: Smart toys - IoToys - data protection - minors - GDPR.

1. Characteristics and peculiarities of smart toys.

In the 21st century, the impact of new technologies is enormous. Technologies have changed the way of life of the human being, from personal relationships to work activities. On one side, new technologies represent an evolution but, on the other side, this evolution has to be regulated in order to put technologies at the service of man and not the opposite. Indeed, human beings are constantly monitored through the growing number of identification and tracking technologies and, in some cases, their behaviour is already influenced by the (ab)use of smart devices.

In this scenario characterised by the quick evolution of technologies, Internet development has played a central role which has been enhanced by the extension of this network to the world of objects, giving birth to the phenomenon known as the Internet of Things (IoT).[1] This information architecture has been defined as a network which connects

[1] With regard to the introduction of the term Internet of Things K Ashton, 'That "Internet of Things" Thing. In the real world, things matter more than ideas' (2009) RFID J, 1; S Haller, S Karnouskos, C

tangible or intangible goods, that becomes recognisable and can also acquires intelligence through the ability to collect and communicate data about themselves and the surrounding environment.[2] For their peculiarities, these objects are well known as 'smart things'.[3] Indeed, they are capable of interacting with the surrounding environment, connecting to the Internet and using a different kind of technological systems which change in accordance with the types of intelligent object. Nowadays, included in this category are incredibly wide kinds of objects developed in different sectors. So, in the smart mobility sectors, there are things such as ADAS or even highly automated vehicles,[4] in the medical sector,[5] instead, the intelligent medical equipment develops more and more quickly from the field of prostheses to the machinery needed to implant them, while, in the domotics sector,[6] we have for example intelligent thermostats or refrigerators. Regarding private life sector, then, are very spread smartphones but also smartwatches and, finally, in the recreational sector, not very known but problematic, are included the so-called smart toys for kids and teenagers, which will be the topic of this articles. There are so many smart things in the world that the concept of "Internet of Things" has moved to that of 'Internet of everything'.[7]

Reaching now the heart of the article, it is necessary to give a more precise definition of smart toys. Smart toys are part of the macro-category of smart things, connected online in

---

Schiroh, 'The Internet of Things in an enterprise context' (2008) Future Internet, Lecture Notes in 5468 Computer Science, 1. About Internet of Things definition, instead, *see* S Ziegler (ed), *Internet of Things Security and Data Protection* (Springer, 2019); G Noto La Diega, I Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) 219 Queen Mary School of Law Legal Studies Research Paper; SR Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93 Texas Law Review, 85 ff.; RH Weber, 'Internet of Things, New security and privacy challenges' (2010) Computer law & security rep, 23 ff..

[2] European Research Cluster on the Internet of Things (IERC), Internet of Things Strategic Research Roadmap (2nd edn. 2011) 10, http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf, accessed 27th November 2020.

[3] Smart things are tagged with a Radio Frequency Identification (RFID) tag with a single ID called Electronic Product Code (EPC). About RFID *see* EK Pallone, '"Internet of Things" e l'importanza del diritto alla privacy tra opportunità e rischi' (2016) 17 (55) Ciberspazio e diritto, 174 f..

[4] On self-driving cars legal regulation *see* A Bertolini, M Riccaboni, 'Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules' [2020] Eur J Law Econ, 1 ff.; E Al Mureden, '"Autonomous cars e responsabilità civile tra disciplina vigente e prospettive de iure condendo' (2019) 3 Contr. impr., 2019, 895 ff.; U Ruffolo, E Al Mureden '"Autonomous vehicles" e responsabilità nel nostro sistema ed in quello statunitense' (2019) 7 Giur. It., 1657 ff.; A Albanese, 'La responsabilità civile per i danni da circolazione dei veicoli ad elevata automazione' (2019) 4 Europa e diritto privato, 995 ff.; A Davola, R Pardolesi, 'In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?' (2017) 5 Danno e responsabilità, 616 ff.. Please, allow me to refer to MC Gaeta, *Liability rules and self-driving cars: The evolution of tort law in the light of new technologies* (ESI, 2019). B Von Bodungen, IA Caggiano, H Steege, MC Gaeta (eds), *European regulation for self-driving cars* (Springer) (forthcoming).

[5] On the implementation of Robotics and AI in the medical sector, with specific reference to wearable robotics, *see* M Cardona, V Kumar Solanki CE García Cena (eds), *Internet of Medical Things. Paradigm of Wearable Devices* (Routhledge, 2021, forthcoming).

[6] *See* L Vizzoni, 'Dispositivi domotici e dati personali: dalle difficoltà applicative del GDPR alla prospettiva del futuro regolamento e-privacy' (2020) 4 Nuove Leggi Civ. Comm., 1032 ff.; F Pizzetti, 'Domotica. L'intelligenza artificiale che ci spia a casa: quali rischi e soluzioni per la privacy', available at https://www.agendadigitale.eu/sicurezza/privacy/lintelligenza-artificiale-che-ci-spia-a-casa-quali-rischi-e-soluzioni-per-la-privacy/, accessed 2nd December 2020.

[7] *See* B Di Martino, K Ching Li (et al.), *Internet of Everything. Algorithms, Methodologies, Technologies and Perspectives* (Springer, 2018); D Evans, 'Internet of Everything: Harnessing an Exponentially More Powerful Internet' (2012) Cisco Blog, available at https://blogs.cisco.com/digital/internet-of-everything-harnessing-an-exponentially-more-powerful-internet-ioe-infographic, accessed 2nd December 2020.

the IoT, and this is why they are also called Internet of Toys (IoToys).[8] They are devices with the appearance of traditional children's toys (e.g. dolls or cuddly toys) but they are capable of interacting with the surrounding environment, connecting through the Internet and using technological systems that range from sound systems (e.g. microphones), to visual systems (e.g. cameras), passing through the multiple types of sensors of movement or localisation, with which they are equipped. Interactive toys are robots, characterized by a more or less developed level of automation, to the point that the most automated models of connected toys can be equipped with artificial intelligence (AI).

Smart toys are, therefore, designed to interact actively with children and are often able to automatically perform various activities, such as recording sounds, taking photos or shooting videos, and sharing this data online (websites or social networks). The most advanced toys, then, include remote video control, gesture-based interactions, voice recognition and face tracking. Furthermore, smart toys can have medical sensors that monitor children's body temperature, heart pressure, blood values, and breathing.

Considering the fast and constant evolution of robotics and AI, machine learning and big data analytics, in all their applications, it is clear that these connected toys will continue to increase and evolve quickly bringing with them advantages but also serious risks.

2. Risks of smart toys.

2.1. Minors' personal data processing through an IoToy.

Although smart toys are fun and sometimes even educational games or toys capable of monitoring children's vital functions, they are still tools that collect, process and communicate information and personal data,[9] with consequent possible risks, especially for minors. Indeed, in relation to toys connection, there is a concrete risk of unlawful processing of minors' personal data, but also the risk of hacker attacks. Furthermore, problems related to possible emotional bonds between the child and the toy, as well as damages arising from a malfunctioning of the smart toy, can be configured. In this subparagraph all these risks will be in-dept, but let proceed with order, starting with the data protection issue.

Today, personal data, including that of the children are processed in huge quantities, that continuously grow and are updated, and that can be structured (such as date from databases) but also semi-structured or completely unstructured such as email obtained from profiles, images on social networks and GPS data. This is such a large amount of data that they are known as big data, i.e. a data set so extensive in terms of volume, speed and variety that requires specific analytical technologies and methods for the extraction of value or knowledge. This phenomenon is developing more and more quickly in recent years following

---

[8] About the definition of 'Internet of Toys' *see* European Commission, Joint Research Centre, Technical Reports, Kaleidoscope on the Internet of Toys, 2017; G Mascheroni, D Holloway (eds), *The Internet of Toys. Practices, Affordances and the Political Economy of Children's Smart Play* (Springer, 2020); L Green, D Holloway, 'Discursive constructions of the internet of toys' (2017), in 'Refereed Proceedings of the Australian and New Zealand Communication Association Conference. Communication Worlds: Access, Voice, Diversity, Engagement', available at https://ro.ecu.edu.au/ecuworkspost2013/4496/, accessed 3rd December 2020, L De Carvalho, M Eler, 'Security Requirements for Smart Toys', in Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017), Vol. 2, 144 ff..; C Tschider 'Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age' (2018) 96 (87) Denv. U. L. Rev., 120 ff.

[9] About privacy and smart toys *see* T Milosevic, P Dias, C Mifsud, CW Trültzsch-Wijnen, 'Media Representation of Children's Privacy in the Context of the Use of "Smart" Toys and Commercial Data Collection' (2018), 9 Media Studies, 26 ff..

the contextual rapid evolution of new technologies.[10]

The reasons why minors' personal data are processed are different. Of course, data are processed to guarantee the functioning of their operating system. Indeed, the operative systems works thought data to provide services for which they were designed (e.g. measure blood pressure or calculate the right body weight for that single child to whom the toy is given) or to provide better tailored services by analysing personal data relating to the child's interests and preferences (i.e. profiling him or her). However, there are other reasons for minors' data processing through IoToys.

About the domain of the marketing activities, personal data are used to profile minors (art. 4, para 1, n. 4, GDPR), i.e. any form of automated processing with the aim to analyse or predict minors' personal preferences, interests, health, behaviour and location, in order to offer directly to them via targeted ads, or put on the market, good and services in line with their profile.[11] The kind of data analysis related to the behaviour, go through the name of data commercialization practices and, in particular, is behavioural advertising or behavioural targeting, because is based around the behaviour of the users, usually online. Moreover, the behavioural advertising is so sophisticated activity that affects human being's and, especially, children, manipulating their choices and, in this case, their interests in purchasing of products and services.

In addition to this, minor's personal data processing can be used for potentially discriminatory practices, such as excluding children with certain profiles from particular types of education or refusing to grant specific health care or insurance policies on the base of the data collected. These forms of discrimination are made possible by the knowledge of the most intimate aspects of the person (special categories of personal data), such as those suitable for revealing the state of health, sexual orientation or ethnic origin.

An example of particular relevance regarding the unlawful processing of the minor's personal data concerns the case of 'Hello Barbie'. 'Hello Barbie' is an interactive doll produced by Mattel Inc., which features a computer chip, microphone, speaker and is Wi-Fi

---

[10] A definition of big data is provided by A De Mauro, M Greco, M Grimaldi, 'A Formal definition of Big Data based on its essential features' (2016) 63(3) Library Review, 122 ff. Down a legal point of view with particular regard to data protection egal issues, *see* Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017, T-PD(2017)01; Italian Competition Authority, Italian Authority for Communications Guarantees and Italian Data, Guidelines and policy recommendations for Big Data, July 2019. Literature on the topic: A Mantelero, 'Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework' (2017) Computer Law and Security Review, 584 ff.; A Mantelero, 'La privacy all'epoca dei Big Data', in V Cuffaro, R D'Orazio, V Ricciuto (eds) *I dati personali nel diritto europeo* (Giappichelli, 2019), 1181 ff.; G D'Acquisto, M Naldi, *Big Data e Privacy By Design* (Giappichelli, 2018); A Mantelero, La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence, in A Mantelero, D Poletti (eds), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (Pisa University Press, 2018), 289 ff.; A Mantelero, 'Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo' (2012) 1 Dir. Inf., 135 ff..

[11] On risks and remedies of the automated decision making, including profiling process through the analysis of the data collected online, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe, Guidelines on Artificial Intelligence and Data Protection, 25 January 2019, T-PD(2019)01. The guidelines follow and are based on a Report by A Mantelero on Artificial Intelligence and Data Protection: Challanges and Possible Remedies of the same Consultative committee, of 25 January 2019, T-PD(2018)09Rev. *See* also A Mantelero, 'Regulating AI within the Human Rights Framework: A Roadmapping Methodology' in P Czech , L Heschl, K Lukas, M Nowak and G Oberleitner (eds), *European Yearbook on Human Rights 2020*, (Intersentia, 2020) 484 ff.; A Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: from an Individual to a Collective Dimension of Data Protection' (2016) 32 Comp. Law & Secur. Rev., 238 ff..

enabled. By pressing her belt, the doll asks a question and records the child's response. The message is encrypted and sent via the Internet to be processed by the voice recognition software of ToyTalk, Inc. (now PullString, Inc.), a partner of Mattel Inc.. The software then sends a command to Barbie to play an answer chosen among those stored in the doll which results appropriate according to the topic the child wants to talk about. What is of concern is privacy: the secrets confided to the doll by a child are shared with Mattel and its medical partners and could be illegally treated, even for discriminatory purposes. In addition, hackers are able to steal data processed by Hello Barbie, such as names, addresses, email and sensitive data from millions of families around the world. Hackers are also able to extract the name of the Wi-Fi network, the internal MAC address, the account ID and MP3 files, that are enough to get access to the Hello Barbie account and a home network.[12]

The legal protection of minors' personal data is contained in different international, European and national regulations that deal with internet minors and privacy,[13] among these a role of primary importance is covered by the new European regulation on data protection (GDPR).[14] Indeed, minors are data subjects that, knowingly or unknowingly, disclose information about themselves. They fall into the category of particularly vulnerable subjects, precisely because of their tender age which implies reasoning skills not completely defined and less awareness of their data processing.[15] The protection of the privacy of minors is an extremely important and topical topic in particular when the same processing takes place through new technologies tools and this contribution deals with the case in which the processing of minors' personal data takes place through smart toys. In this context, it is, therefore, necessary to establish when and how minors or their parents are informed about the processing of minors' personal data and what the legal basis for the lawful data processing.

The information on the processing of minors' personal data, included that related to profiling processes, should be drawn up in compliance with the provisions of articles 13 and 14 GDPR. This information should be provided in a privacy policy provided by the seller of the smart toy or it should be included in the software of the toy and appear at its first installation. Among the contents to be necessarily included in the privacy policy there are also the rights of the data subject (art. 12 - 23, GDPR), have also the function of preventing the discriminatory processing mentioned above.

The GDPR requires owners to demonstrate that the correlations applied in the algorithm are impartial, i.e. non-discriminatory and that there is a legitimate justification for the automated decision. Individuals subject to the automated decision, in fact, have a plurality of rights, such as opposition to profiling (Article 21), the request for cancellation or the rectification of their profile (Article 17), the challenge to automated decisions (Article 22, paragraph 3).

With specific regard to the content of the privacy policy, it must be emphasized that it is

---

12 *See* ID Manta, IS Olson, 'Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly' (2015) 67 Alabama Law Review, 135 ff.. From a comparative point of view, *see* M Fantinato, PCK Hung (et al.), 'A preliminary study of Hello Barbie in Brazil and Argentina' (2018) 40 Sustainable Cities and Society, 83 ff.. More recently, starting from 2017, a new Barbie model, Barbie hologram, was designed but no studies have yet been published on it.

13 IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (2018) 1 Familia, 7 ff.; F. Scia, *Diritti dei minori e responsabilità dei genitori nell'era digitale* (ESI, 2020), 17 ff..

14 Regulation 2016/679/EU 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 - GDPR) [2016] OJ L119/1.

15 In this sence rec. 38 GDPR.

not enough to include the information requested by the GDPR, but a greater effort is needed in order to guarantee an adequate level of awareness of the data subject, especially of the minor. In order to implement minor awareness, it should be necessary to simplify the privacy policy, in the double direction of limiting the contents to those strictly necessary according to article 13 and 14 of the GDPR and explain them in the simpler and effective way in relation to the category of data subject involved, which does not only concern the language used but also how the information is represented graphically. Regarding the information, the privacy notice must contain information that is concise, transparent,[16] intelligible, easily accessible and to understand, as well as written in clear and plain language, according to the first paragraph of the article 12 and the recital 58 of the GDPR. Additionally, where appropriate, visualization principles can be used for the organization of the information contained therein. Indeed, the paragraph 7 of the article 12 of GDPR states that information can be provided in combination with standardised icons, in order to help the data subject to know and understand whether, by whom, for what purpose and how long his or her personal data are being processed.[17]

On the other hand, in relation to the legal basis of the processing, the same could be based on the data subject consent or, in some cases, to the performance of a contract of which the data subject is a party. GDPR provides, as one of the legal basis, the rule of the express consent of the processing of personal data (art. 6, para 1, let a), GDPR) with the exception constituted by the explicit consent, required only with regard to special categories of personal data (art 9, para 2, let a), GDPR), profiling activities included the above mentioned (art. 22, para 2, GDPR), to which is added the case of the transfers of personal data to a third country or an international organisation (art. 49, para 1, lett. a), GDPR).[18]

About minors' consent to the processing of personal data, the GDPR provides specific discipline, in particular, it is envisaged that they can provide consent to the processing of their personal data with regard to the processing through the information and

[16] Concerning the transparency processing *see* Article 29 WP, Guidelines on transparency under Regulation 2016/679, 11th April 2018, no. 260. During its first plenary meeting the EDPB endorsed the GDPR WP29 Guidelines on transparency.

[17] About the icons that could be included in a privacy policy, the first reading of the European Parliament on COM (2012)0011, was supplemented by an Annex containing an iconic privacy policy. This annex, indeed, provided, standardised icons that would have been helpful to understand the information contained in the privacy policy. However, the annex has been eliminated in the final version of the GDPR proposal (Proposal for a Regulation of the European Parliament and of the Council of the 25.01.2012 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011). On the GDPR proposal, with specific reference to the iconic privacy policy, *see* JS Pettersson, 'A brief evaluation of icons suggested for use in standardized information policies. Referring to the Annex in the first reading of the European Parliament on COM (2012) 0011', WP Universitetstryckeriet Karlstad, 2014. More in general *see* S de Jong, D Spagnuelo, 'Iconified Representations of Privacy Policies: A GDPR Perspective', in Á Rocha, H Adeli, L Reis, et all (eds.), *Trends and Innovations in Information Systems and Technologies* (Springer, 2020).

[18] The difference between express and explicit consent is unclear and it would appear that explicit consent is nothing more than an express consent characterized by greater determination in the behaviour of the user. IA Caggiano, 'Il consenso al trattamento dei dati personali' [2017] DIMT 20 ff.; G Zanfir, 'Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law' (2014) Reloading Data Protection 11.

communication technologies (ICT)[19] from the age of 16 (art. 8 GDPR).[20] However, each dingle Member States can establish a lower age for the processing of minors' personal data (in any case not less than 13), that in Italy it is set at 14 years (art. 2 *quinquies* of the Italian privacy code).[21] Moreover, if the minor is under the established age to give his or her consent, the processing is lawful when such consent is given or authorised by the holder of parental responsibility. More specifically, recital 32 considers as lawful any positive act clearly indicating the willingness of the user to consent to the processing of his or her personal data, such as in the case of the consent provided online. This mode of consent is currently very common with the use of electronic means, such as a smart toy, where are accepted certain actions that appear to be more closely related to implied consent rather than the express consent that does not match the definition of positive act. In this light, in the last year has been clearly highlighted the limits of the current consent to the processing of personal data both because the data subject is unaware of the kind of data processed and the type of data processing carried out in relation to his or her data, and because, even when it is consciously given, it does not prevent a harmful processing for the user, unless accompanied by adequate security protection tools.[22]

Concerning the performance of a contract of which the data subject is a party as a lawful basis (art. 6, para.1, let. b), GDPR).[23] It seems important to underline that these are rather

---

[19] Precisely art. 8 GDPR refers to the direct offer of the information society services, i.e. those services normally provided for remuneration, at distance, electronically and at the individual request of a recipient of the services, such as social networks and sharing platforms, pursuant to art. 1, directive 2015/1535/EU, expressly mentioned by art. 4 GDPR). The applicability of art. 8 GDPR only to information society services is a main distinction between this European standard and the US one applicable in general to online activities (§312.5 on Parental consent) of the Children's Online Privacy Protection Act of 1998 (so-called COPPA), available at https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5, accessed by 7th December 2020. *See* IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori', in C Fabricatore, A Gemma, G Guizzi, N Rascio, A Scotti (eds), *Liber amicorum per Paolo Pollice* (Giappichelli, 2020), 87.

[20] On minors' consent to the processing of personal data in a digital age, authoritative academic literature has been pronounced. Reference is made to Caggiano for an in-depth analysis of the issue: IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori' (n 19), 87 ff.; IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (n 13), 10 ff..

[21] Italian legislative decree 30 June 2003, no. 196, Code regarding the protection of personal data, containing provisions for the adaptation of national law to Regulation (EU) no. 2016/679 of the European Parliament and of the Council, of 27 April 2016, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46 / EC, as at last amended by legislative decree 10 August 2018, no. 101 (Italian privacy code) OJ 174. In Italy, the choice of setting the minimum limit for consent to the processing of personal data at 14 years appeared to be an appropriate choice as it complies with the provisions established for consents relating to other national legislation: adoption law n. 184/1983 and cyberbullying law n. 17/2017.

[22] L. Gatt, R. Montanari, IA Caggiano (eds), *Privacy and Consent. A Legal and UX&HMI Approach* (forthcoming); L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 2 Politica del diritto 350 f.; IA Caggiano, 'Il consenso al trattamento dei dati personali' [2017] DIMT online, 20 ff.; G Zanfir, 'Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law' (2014) Reloading Data Protection 237 ff.. More specifically on the efficacy of minors' data protection law *see* IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori' (n 19), 90 ff..

[23] EDPB, Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 8 October 2019, no. 2. IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori' (n 19), 89 ff.; IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (n 13), 14 ff..

limited for two kinds of reasons. First of all, and more generally, this legal basis of the processing refers only to cases in which the processing of data is necessary for the execution of the contract or to take steps at the request of the data subject prior to entering into a contract and does concern only the processing of the personal data strictly necessary for this purpose. Secondly, and more specifically in relation to the processing of minor's personal data, since the data subject is a minor and is lacking his or her capacity to act, the contract should be concluded by the subject in charge of the parental responsibility who would simultaneously authorise the data processing of the minor, but only those processing expressly necessary for the execution of the contract. Obviously, the contracts of the everyday life, of modest value, and not very risky, are an exception, been able to be concluded by the minor (according to authoritative thesis,[24] at least 16 years of age or that established by national law) who contextually agrees to the processing of his personal data (such as contract to purchase a mobile phone number or to by a mobile app).[25]

Last but not least, a possible way to strengthening the *ex ante* remedies of data protection should be the implementation of the principle of privacy by design and by default (art 25, GDPR) and that of security by design by default, the seconds will be analysed in following subparagraph (2.2). These principles are clear examples of techno-regulation: at the time of the determination of the means for processing and at the time of the processing itself, the controller shall implement appropriate technical and organisational measures, which are designed to implement users' privacy and security.[26]

2.2. Smart toys' cyberattacks.

Another very serious and concrete problem relating the IoToys is the possibility that they can be hacked. Concerning cybersecurity and, in particular, the protection of minors from hacker attacks of their smart toys, this risk is strictly connected to the first concerns: how smart toys are connected online, hackers can enter in the smart toys producing personal or property injury.

In particular, cyberattacks imply the hackers can enter in the smart toys' systems producing psychophysical injury or property damages. Among physical injury, very possible are that of data breach, psychological manipulation and personal injury. About property damages, instead, damages to the smart toy or other goods in the surrounding environment, are very serious.

The Fisher-Price 'Smart Toy' could be an example of what the risks involved in smart toys could be, as an effect of cybersecurity issues. The Fisher-Price 'Smart Toy' was one of the first, if not the first, smart toy on the market. The range included three different plush animals - a bear, a monkey and a panda – all connected to the Internet, which worked along with a companion app and smart cards that provided different activities the child could have done with the toy.[27] The toy was able to interact with the children on the base of the command given through an app managed by the parent(s). It was basically a robot but was

---

[24] IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (n 13), 16.

[25] To better analyse the relationship between privacy consent (Art. 6, para 1, lett a), GDPR) and contractual consent (Art. 6, para 1, lett b) GDPR) of the minor *see* IA Caggiano, 'L'età del consenso e il trattamento dei dati personali dei minori' (n 19), 89-90 ff..

[26] For a complete analysis on the principles of data protection and security by design and by default, please see European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 2018. May me refers to MC Gaeta, Critical issues arising from the Legal Analysis (L.A.)., in L. Gatt, R. Montanari, IA Caggiano (eds), *Privacy and Consent. A Legal and UX&HMI Approach* (n 22).

[27] Fisher-Price described the smart toy as 'an interactive learning friend with all the brains of a computer, without the screen'.*See* https://www.fisher-price.com/en_CA/brands/smarttoy, accessed 3rd December 2020.

equipped with a very basic level of AI,[28] just able to learn some children preferences in order to better interact with him/here. This toy processed personal data and it was a typical example of data-surveillance.

With a tweet dated 22nd July 2019, Mattel (owner of Fisher-Price Company) announced that the 'Smart Toy' was no longer available on the market probably due to different problems that included hiking attacks, which had a huge impact in the public opinion.[29] In fact, already in 2016, it was highlighted some serious vulnerabilities of the so-called Fisher-Price 'Smart Toy',[30] which was analysed at hardware, software, and network levels. Through this analysis, it has been clarified that many of the platform's web service (so-called 'API') calls were not appropriately verifying the 'sender' of messages. This circumstance has strong implications, exposing the smart toy to the risk of cyberattacks, the consequences of which can range from the theft of the minor's personal data to even more. It emerged that the architecture of the smart toy allowed a potential attacker to send requests that should not be authorized under ideal operating conditions. The analysis carried out also highlighted in detail the list of APIs that were found at risk identifying, case by case, the impacts due to each vulnerability.

In particular, it turned out to be possible to find all customers, which provides a list of those customers' toy details and find all children's profiles (identified with name, birthdate, gender, language, which toys they have played with, which purchases have been made). In addition, it seemed also to be possible to create, edit, or delete children's profiles on any customer's account: in the range of the editing activities, it was possible to delete toys, add someone else's toy to a different account) or delete some of the device's built-in functionality. It was also possible to find the status of whether a parent is actively using their associated mobile application or if a child is interacting with their toy at that specific time.

The personal data that an unauthorised person could have stolen would certainly not seem to be sensitive data but, since these are data relating to the personal sphere of children, it is still necessary to pay close attention. First of all, even if the single data may not be relevant in itself, the combination of several data can return a rather detailed profile of the child. Furthermore, the possibilities of modifying the toy or the account linked to the toy, as well as the mere stealing of data, make it clear that the cyberattacks carried out on the smart toy could end up affecting the child.

As it was said, a cyberattack 'could effectively force the toy to perform actions that the child user didn't intend, interfering with normal operation of the device'.[31]That said, it is clear that the smart toy could be used to enable strangers to talk to children through the doll, pushing the child into behaviours that he/she would not otherwise have had, or to make explode the smart toy creating a physical damage for the child. So, the need for straightening the cybersecurity protection it is clear.

---

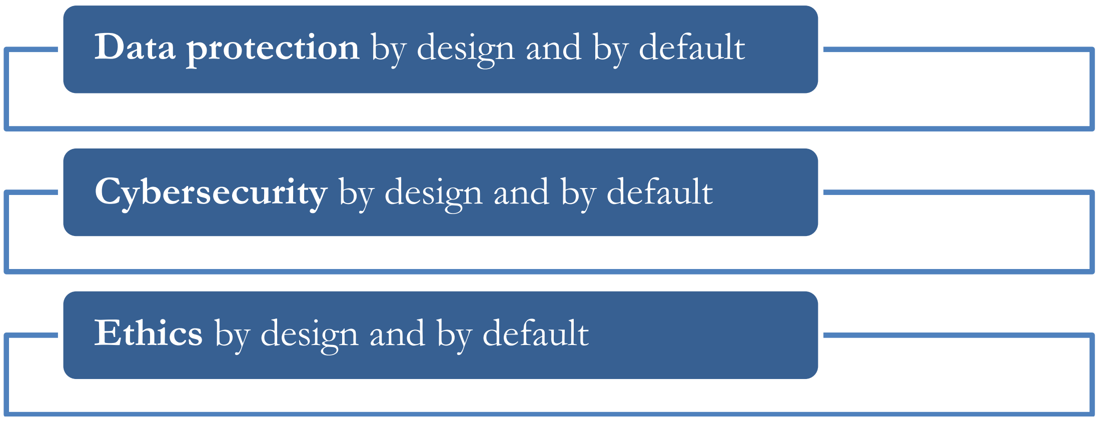
[28] For a definition of AI *see* HLEG, A definition on AI: Main capabilities and Disciplines, 8 April 2019.

[29] *See* D Yadron, 'Fisher-Price smart bear allowed hacking of children's biographical data', available at https://www.theguardian.com/technology/2016/feb/02/fisher-price-mattel-smart-toy-bear-data-hack-technology, accessed 3rd December 2020.

[30] M Stanislav, 'R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy® hereO GPS Platform Vulnerabilities (FIXED)' (2016) Rapid7 Blog, available at https://blog.rapid7.com/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform/, accessed 3rd December 2020. Mark Stanislav was at the time manager for security advisory services at Rapid7. Also *see* R Pinkham, 'API Security Lessons from Fisher-Price's Smart Toy Bear Security Flaw', available at https://smartbear.com/blog/test-and-monitor/fisher-price-smart-toy-data-hackers/, accessed 3rd December 2020. About this analysis, also from a juridical point of view, *see* KL Smith and L Regan Shade, 'Children's digital playgrounds as data assemblages: Problematics of privacy' (2018) Big Data & Society, 2 ff..

[31] M Stanislav, 'R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy®' (n 30).

In order to implement effective preventive protection in the dimension of cybersecurity, certainly, the principles of security by design and by default represents a valid measure. More precisely, in addition to the principles of data protection by design and by default (art. 25, GDPR), that also should be implemented more effectively and efficiently, could be enhanced security measures by design and by default (to which the principle of ethics by design and by default is added, as will be explained inn the following subparagraph). Although not expressly regulated in the GDPR, are however provided in a broad sense in articles 32 and following of the regulation.



The concept of security by design (eg. designing secure hardware, password, PIN, face ID, fingerprint, security key) and by default (eg. installing good antivirus or providing the automatic periodic updating of software) implies that, in addition to the functional requirement, also the design, development and the maintenance of the operative systems must be taken into account to guarantee security (in our case cybersecurity), throughout the life cycle of the operative system. In this direction also the Data Protection Impact Assessment (DPIA), regulated under articles 35 and following of GDPR, can play a very important role in order to evaluate if is it is necessary to implement the cybersecurity measures. In particular, it is useful for the part of the DPIA relating to risks such as offline and online data storage, website and IT channel security, hardware security (including the security key), and measures against malware.

Cybersecurity plays a fundamental role, as data security also implies greater protection of the same data and, therefore, greater privacy of the data subjects. The importance of cybersecurity it is now also known to the legislator, who, although did not intervene properly on security by design by default, however, intervened on the regulation of the so-called essential services characterised by a strong impact of ICT. On this topic, it is worth mentioning that the European legislator in 2016 introduced the so-called NIS directive (Dir. 2016/1148/EU)[32] which aimed to improve national cybersecurity capabilities by preparing member states and requesting them to be adequately equipped. It created European cooperation by setting up a Cooperation Group (art. 11, NIS directive),[33] in order to collaborate at European level and manage cybersecurity risks in all services considered

[32] Directive 2016/1148/EU of the European parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1. The Directive was implemented in Italy by legislative decree 18 May 2018, n. 65 on Implementation of the (EU) NIS Directive.

[33] The Cooperation Group is composed by the representative of the Member State, the Commission and ENISA (art. 11, para 2, NIS Directive).

essential for the economy and the society, strictly related on ICT[34]. In addition, the article 9 of the NIS Directive has also allowed the creation of Computer Security Incident Response Teams (CSIRTs) in each individual Member States that must deal with incidents and risks and ensure effective cooperation at the Union level.[35] After the NIS Directive, the main among the regulation recently adopted for cybersecurity was the Cybersecurity Act (Reg. 2019/881/UE). It consists in a Regulation aimed at creating a European framework for the certification of IT security of ICT products and digital services, and to strengthen the role of the European Union Agency for Cybersecurity (ENISA).[36]

2.3. Ethical issue related to smart toys: from the emotional bonds to the psychological manipulation.

Legal challenges arising from the development of new technologies impose to pay attention on ethical principles. It is undoubtable that ethical principles have the function of integrating and assisting the legal regulation of these phenomena. In particular, with specific regard to smart toys, ethics should strengthen its discipline also endowing it with moral and social values, even intervening before the law, where it appears backward and inadequate.

A recent study of the European Parliamentary Research Service affirms that 'any robot with moving physical parts poses a risk, especially to vulnerable people such as children and the elderly'.[37] This is more and more true in the case of smart toys: in fact, they have very strong ethical implications, due to the possible emotional bonds between the child and the toy.

So, it is not possible to regulate new technologies, and in particular smart toys, without also providing ethical principles (included the principles of ethics by design and by default as an example of techno-regulation) which, in some cases, even precede the introduction of the relevant legal framework. At the same time, it is not possible to provide ethical principles without also binding regulatory principles, which guarantee the certainty of action and its consequences.

It is clear that minors are particularly vulnerable subjects and fall within those categories of vulnerable subjects who can most easily be affected by a bad use of technologies that could lead to an alienation from the real life, or, in the worst cases, could lead to make esteem act that could even lead to the loss of life.

The more recent examples of this terrible problem are the so-called 'Blue Whale'[38] and

---

[34] Concerning the essential services, the figure of operator of the essential service (OSE) has been established. They must take all appropriate and proportionate technical and organizational measures to manage the risks posed to the security of networks and information systems, to prevent and minimize the impact of accidents; they must also notify the incident to the competent NIS authority or the CSIRT.

[35] In Italy, the CSIRT will replace, by merging them, the National CERT (operating at the Ministry of Economic Development -MISE) and the CERT-PA (operating at the Digital Italy Agency - AGID).

[36] All the information on ENISA are available here: www.enisa.europa.eu. At national level, in 2019, the competent NIS Authorities have drawn up guidelines for the risk management and the prevention and mitigation of accidents that have a significant impact on the continuity and provision of essential services.

[37] European Parliamentary Research Service, 'The ethics of artificial intelligence: Issues and initiatives' [2020]. Also *see* V Dignum, 'Ethics in artificial intelligence: introduction to the special issue' (2018) 20 Ethics and Information Technology, 1 ff..

[38] To start Blue Whale you would need to attend forums or groups dedicated to suicide, they usually have names related to whales, and write a message using the hashtag # f57. At that point you would be contacted by a "master" who, it is not known how, would convince the victim that he has personal information that can be used to harm his family. Then the victim has to undergo a series of tests that involve listening to or watching films and songs proposed by the master, self-inflicted injuries or staying for a while on the edge of a very high building or on the tracks of a railway. Obviously, everything must be kept secret, under penalty of death of family members. *See* A Khasawnen, K Chalil Madathil, E Dixon, P Wiśniewski, H Zinzow, R Roth, 'Examining

'Jonathan Galindo'[39] games. Even though are not smart toys, they are both online games where teenagers decide to participate voluntarily following an established procedure. The serious risk of those games is that the teenager could fall into a trap on the web, forced by someone to kill himself, perhaps to save the life of his family or to save himself. The 'Blue Whale' and 'Jonathan Galindo' cases highlight further problematic profiles also in relation to IoToys, even if they are not physical toys but online games.

In fact, if hacking a smart toy is possible, as we have seen in the Hello Barbie and Fisher-Price 'Smart Toy' examples, it could be also possible to talk with the child thought the smart toy, forcing him or her to fall into a trap, exactly as seen on the web with the abovementioned cases. Furthermore, there is the aggravating circumstance that the smart toy is a physical object, with the aspect of an animal or a friend, therefore it can even more easily influence vulnerable subjects such as children. Since the 'Jonathan Galindo' game is even more dangerous than 'Blue Whale', because the unknown person has the aspect of a Disney-like fictional character, an hacked smart toy could be even more dangerous, being a physical 'friend'.

If problems of this type are serious even for boys around eighteen years old, the risk must be taken more seriously with regard to children. Indeed, children do not yet have a well-developed decision-making capacity. In this context, the emotional bonds between children and smart toys could be a serious issue. Therefore, it is necessary that minors, albeit digital natives, are able to understand technologies and their use, as well as distinguish what is human from what is not, without creating emotional relationships with these kinds of toys that are unable to return the feelings.

3. Current regulation for minors' protection as vulnerable subjects in relation to new technologies[40].

3.1. The evolution of the category of personality rights in the digital era.

Coming to this point of the work it is important to focus on the regulation of the individual protection in relation to new technologies, in particular when they are minors. In this line the present subchapter (3.1) will put on the table the personality right and their evolution, while the second subchapter (3.2) will focus on the civil regulation of individuals protection, both in relation to smart product (category that includes smart toys).

The legislator of the second half of the 1900s, after the Second World War, began to move towards the affirmation of values all inspired by the centrality of the individual whose inviolability had to be guaranteed above all other interests and without limitations. Hence the discussion on personality rights initially divided between those who claimed the existence of a single personality right of the individual in all its qualifying manifestations regardless of the single and specific reference legal rule,[41] while others - now prevalent thesis - believed

---

the Self-Harm and Suicide Contagion Effects of the Blue Whale Challenge on YouTube and Twitter: Qualitative Study' (2020) 7 (6) JMIR Ment Health.

[39] *See* D Urietti, 'Cosa sappiamo di Jonathan Galindo' (2020) Corriere della Sera, available at https://www.corriere.it/tecnologia/20_ottobre_01/jonathan-galindo-cosa-sappiamo-sfida-diffusa-online-9ef9beb0-03c1-11eb-84c6-5a6c097a97a1.shtml, accessed 3rd December 2020.

[40] The title refers to the Jean Monnet Chair PROTECH ('European Protection Law of Individuals in Relation to New Technologies') project, co-founded by the Erasmus+ Program (Proposal: Call for Proposals 2019 - EACEA-03-2018; Application number of the project: 611876 -EPP-1-2019-1-IT-EPPJMO-CHAIR), of which Prof. Lucilla Gatt is the chair holder and the author of this contribution is one of the members of the teaching staff. For more information see the website of the project www.protech-jeanmonnet.eu

[41] G Alpa, 'Le persone fisiche (art. 1-10)', in *Il Codice civile*, Commentary Directed by P Schlesinger, G Alpa A Ansaldo (eds), (Giuffrè, 1996); G. Alpa e G Resta, 'Le persone e la famiglia. Le persone fisiche e i diritti della

the existence of many personal rights according to the various provisions of ordinary legislation, all protected under the Italian Constitution, in particular article 2 of the Constitution as an 'open catalog' of these personality rights.[42]

As a matter of fact, the Constitution literarily attributes the character of inviolability only to four rights: personal freedom (Art. 13), of domicile (Art. 14), freedom and secrecy of correspondence (Art. 15), the right to defense (Art. 24, para. 2). Among these inviolable rights expressly guaranteed by the Constitutional Charter, in the case of smart toys, we should consider the right of domicile, understood in a broad sense (online domicile),[43] or the freedom and secrecy of correspondence. These rights, in fact, appear to be involved in a pathological use of smart toys, for example following cyberattacks.

It has been observed that the domicile,[44] the place where human personality develops more than any other, must be protected from external intrusions, since it is elevated to an inviolable area on a par with personal freedom itself.[45] In an era in which the home has, in turn, become a smart home, thanks to domotics development, particular attention must be paid to the protection of the home and its inviolability. This is all the truer when technological innovation leads to the introduction of particularly advanced smart devices such as smart toys, which come into contact with the subjects most exposed to the risk of being influenced: children, in fact, are unlikely to be aware of a greater or lesser intrusion of the smart toy into one's home and personal sphere. It is possible to think, from the hypothesis in which the child authorizes the smart toy (or the same toy is hacked) to take videos[46] of moments of private and personal life that take place within the home, to that of the hacker how may manipulate the child, even reaching to asking him/her to open the front door or commit other inappropriate acts. Makes us reflect also the very concrete cases in which the smart toy processes children's personal data for profiling purposes to improve its AI through machine learning algorithms. From this point of view, therefore, the protection of rights such as that, takes on further facets in light of the introduction of smart devices and in particular smart toys, since these are devices intended to be used by less aware individuals, such as children.

Furthermore, even in the absence of an express wording, it is also known that other rights recognised by the Constitution are also included in the 'open catalogue' of inviolable rights enshrined in Article 2. Thus, for example, the Constitutional Court affirmed that have to be considered inviolable also the right to life,[47] the right to freedom of expression (art. 21),[48] the

---

personalità', I, *Trattato di diritto civile*, directed by R. Sacco (Utet, 2019) 145 ff.; P Rescigno, 'Personalità (Diritti della), *Enc. Giur. Treccani XXVI* (1994)

42 P Rescigno, 'Personalità (Diritti della) (n 41).

43 On the new concept of online domicile *see* article 7 of the Commission for Internet rights and duties, Declaration of Internet rights, version after consultation of 14 July 2015, available at https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf, accessed 4th December 2020.

44 About the freedom of domicile *see* M della Morte, 'Art. 14', in R Bifulco, A Celotto, M Olivetti, *Commentario alla Costituzione* (2006) 1 Torino, 56 ff..

45 L Vizzoni, 'Dispositivi domotici e dati personali' (n 6), 1032 ff..

46 In this regard, *see* Italian Constitutional Court, 11th April 2002, no. 135. In this decision, the Italian Constitutional Court addressed the question of the constitutional legitimacy of the visual recordings or video recordings made in the home, raised with reference to Articles 3 and 14 of the Constitution. The decision, in particular, intends home freedom as the "right to protect from external interference, public or private, certain places in which the intimate life of each individual takes place." On this decision, *see* A Pace, 'Le videoregistrazioni 'ambientali' tra gli artt. 14 e 15 Cost.' (2002) Giur. cost., 1070 ff..

47 Italian Constitutional Court, 15 June 1979, no. 54 and 25 June 1996, no. 223.

48 Italian Constitutional Court, 24 June 1970, no. 122.

right to health (art. 32),[49] which may be considered of course also as a right to psychological health. Moreover, the Constitutional Court included the rights of the person in the family,[50] the rights relating to the possibility of having a family,[51] the children's rights[52] to education, maintenance and upbringing.[53]

Many of the rights above mentioned, as have been seen, may equally risk being compromised in the event of a pathological use of smart toys. Moreover, as is well known, constitutional jurisprudence now believes that the category of inviolable rights must extend beyond those explicitly or implicitly recognised by the Constitution, giving life to an 'open catalog' of rights,[54] which can therefore also include new generation rights, including those of the personality, born on the occasion of the development of new technologies and the Internet.[55]

The meaning of article 2 of the Constitution would be, according to this now practically peaceful concept, to open the category to new personality rights that arise due to the evolution of society and, therefore, in this case, also due to the development of new technologies.

Concerning privacy, the Italian Constitutional Charter does not expressly provide a privacy right, even if it finds a Constitutional basis, first of all, in article 2,[56] and then in articles 14, 15 and 21. Privacy right has been developed starting from the more general right to respect the private and family life, home and correspondence provided also at international level under article 8 of the European Convention on Human Rights (ECHR)[57] as well as, at European level, under article 7 of the Charter of Fundamental Rights of the European Union.[58] The data protection right, instead, is foreseen by article 8 of the Charter of Fundamental Rights of the European Union and article 16 of the Treaty on the Functioning of the European Union (TFEU), and it is an independent right with respect to the more general right to privacy.[59] As a matter of fact, the protection of personal data is a matter that has always affected society, re-emerging from time to time in different aspects. The terms confidentiality, privacy and data protection are often used as synonyms. While connected, these three are different concepts. Confidentiality can be divided into two aspects: (i) the right to privacy (more precisely is the respect of private life) and (ii) the protection of

---

[49] Italian Constitutional Court, 24 May 1977, no.103 and 5 July 2001, no. 252.

[50] Italian Constitutional Court, 22 December 1982, no. 258.

[51] Italian Constitutional Court, 1 July 1986, no. 199 and 14 July 1976, no. 181.

[52] For a more detailed analysis of children rights, *see* European Union Agency for Fundamental Rights and Council of Europe, Handbook on European law relating to the right of the child, 2015; European Commission, EU acquis and policy documents on the rights of the child, April 2020.

[53] Italian Constitutional Court, 1 July 1986, no. 199 and 23 May 2003, no. 198.

[54] In particular, this approach has been followed by constitutional jurisprudence starting from the judgement Italian Constitutional Court, 10 December 1987, no. 561. The majority literature was already oriented in this direction. *See* A Barbera, 'Art. 2 Cost.', in G Branca (ed), *Commentario alla Costituzione* (1975) Bologna-Roma, 84-85.

[55] *See* TE Frosini, 'Il costituzionalismo nella società tecnologica' (2020) 4 Dir. Inf., 465 ff.; R Romboli, M Labanca, *Il futuro dei diritti fondamentali* (2020) Pisa; A Iannotti della Valle, 'L'età digitale come "età dei diritti": un'utopia ancora possibile?' (2019) 16 Federalismi; TE Frosini, *Liberté Egalité Internet* (2015) Napoli; S Rodotà, *Il diritto di avere diritti* (2012) Roma-Bari; TE Frosini, 'Il diritto costituzionale di accesso a Internet' (2011) 1 Rivista AIC.

[56] Italian Constitutional Court, 4 December 2009, no. 320, according to which the right to privacy belongs to the sphere of protection of art. 2 of the Italian Constitution.

[57] European Convention on Human Rights of 4 November 1950 (ECHR).

[58] Charter of Fundamental Rights of the European Union of 18 December 2000 [2000] OJ C 364/10.

[59] The difference between the right to privacy and data protection is evident in the Charter of Fundamental Rights of the European Union arts 7–8.

personal data, as fundamental right,[60] and as autonomous personality right which is founded on the power of self-determination.[61] Even if data protection constitutes an autonomous personality right, could be considered as a subcategory of the right to privacy, since one of the cases in which the right to privacy is infringed is the abusive processing of personal data.[62]

Lastly, it should be recalled that Convention for the protection of individuals with regard to automatic processing of personal data (so-called Convention 108), firstly adopted by the Council of Europe in 1981 and lastly amended in 2018.[63] It was the first binding international agreement for the signatory States on data protection. In 2018 the Council of Europe updated the Convention 108 in order to address the challenges for privacy resulting from the use of new information and communication technologies as well as to strengthen the convention's follow-up mechanism.

3.2. The civil regulation applicable to smart products.

The meaning that is currently attributed to the rights of the personality is a recent achievement compared to previous frameworks which attributed a public law nature to the entire system of individual protection, limiting the effective protection of the individuals to only the cases of some interpretation of public law rules allowing to take legal action to assert the personality right.[64]

Fortunately, this public law framework for the rights of the individual has been completed by private law rules that made a step forward in the more direct regulation of the protection of the individual, also in relation to new technologies, even if it is only a starting point to be implemented in the optics of a strengthening of effective preventive and remedial protection.

In particular, in addition to the already mentioned GDPR and NIS Directive, it is necessary to consider the Product liability Directive (PLD)[65] and the two Directive sales contracts for goods and digital content.[66]

As a matter of fact, smart toys are product and so are regulated, at European level, by the PLD for all the cases of product defect. In Italy, the PLD was firstly implemented in 1988[67]

---

60 L Califano, *Privacy: affermazione e pratica di un diritto fondamentale* (ESI 2016); M. Gambini, 'La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela', (2013) 1 Espaço Jurídico, 149 ff.; GF Aiello, 'La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale «disomogeneo» alla luce della nuova proposta di General Data Protection Regulation' (2015) 2 Osservatorio del diritto civile e commerciale, 16 ff.

61 CM Bianca, FD Busnelli, (eds), *La protezione dei dati personali*, vol 1 (CEDAM 2007) XX ff.; CM Bianca, *Diritto civile*, vol. I, *La norma giuridica. I soggetti*, (2nd edn, Giuffrè, 2002), 180.

62 On the infringement of the right of privacy *see* M La Pietra, 'Il caso Soraya', in M Bianca, AM Gambino, R Messinetti (eds), *Libertà di manifestazione del pensiero e diritti fondamentali* (Giuffrè 2016), 169 ff..

63 Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) of 28 January 1981, lastly amended by the 2018. For in-depth Convention 108, see A Mantelero, 'The future of data protection: Gold standard vs. global standard' (2021) Computer Law & Security Review, 1 ff., who considers Convention 108 as a potential global standard, after GDPR that has been described as the gold standard.

64 P Rescigno, 'Personalità (Diritti della) (n 41).

65 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L210/29.

66 Directive 2019/770/EU of the European parliament and of the Council of 20 may 2019 on certain aspects concerning contracts for the supply of digital content and digital services, [2019] OJ L136/1; Directive 2019/771/EU of the European parliament and of the Council of 20 may 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28.

67 D.P.R., 24 May 1988, n. 224, Implementation of the EEC directive n. 85/374 relating to the approximation of the laws, regulations and administrative provisions of the Member States regarding liability for damage caused by defective products, pursuant to art. 15 of the law of 16 April 1987, n. 183

and then repealed by the Italian Consumer Code (in particular, artt. 114 and following).[68] Actually, the PLD refers to traditional goods and not specifically reference to the so-called 'smart products' has done but, according to the European Commission thesis,[69] PLD can also be applied to these second one, at least until there will not be an *ad hoc* regulatory intervention for the creation of a framework of rules that organically discipline Robotics and AI.

To complete this framework there are the tow European directives, among which the sale of goods Directive (SGD) appears most relevant in particular because it refers also to goods with digital elements, so including also smart toys, regardless of whether the sale takes place physically (in shops), online or, more in general, at distance. However also the digital content Directive (DCD) has its relevance for the protection for consumers that pay for a service or provide personal data in exchange for such service. In particular, the DCD concern data produced and supplied in digital form, for example music o video reproduced online, services for the creation, processing or storage of data in digital form, as cloud storage services, services for the data sharing such as social network and sharing platform, and any durable medium used exclusively as a carrier of digital content as USB or DVD. 'Over the top' interpersonal communication services (OTTs), bundle contracts and the processing of personal data are included within the scope of the DCD directive.

This hard law regulation which, as already underlined, represents an implementation of the legislation applicable to the phenomena involving new technologies but it is not enough for the regulation of the smart product and, in our case, IoToys. From 2017 to date, there have been many non-binding initiatives, along with studies and report, symptomatic of the fact that Institutions have understood the need to regulate robotics and artificial intelligence,[70] but specifically concerning smart toys is the Technical Report of the Joint

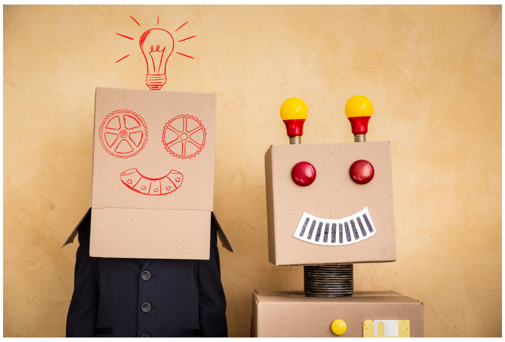
[68] Legislative Decree 6 September 2015, no. 206 (Italian consumer code) OJ 235. To deepen product liability in Italy see A Giorgetti, G Iorio, 'Product Liability (in Italy)', in A Hughes, C Chambers Westgarth, R Freeman, H Lovells (eds), *Product Liability, Jurisdictional comparisons* (European Lawyer, 2014) 215ff..

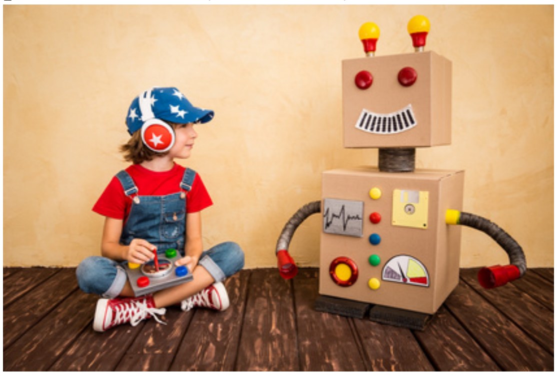
[69] In 2018 the European Commission has intervened with the last quinquennial report (the fifth for precision, covering the period 2011-2015) on the PLD, which has been complemented by a formal evaluation of the directive. *See* European Commission Report to the European parliament, the Council and the European economic and social committee, of 7 May 2018, on the application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) (COM(2018)246 final). The reporting period is 2011-2017 during which the EU Commission declares that did not receive any complaints or launch any infringement proceedings. At the same time, though, the EU Commission mean PLD does not cover all aspects of product liability. Indeed, there is space for different national approaches (e.g. on systems to settle claims for damages, or on how to bring proof of damage). Completing the quinquennial report European Commission Staff Working Document, of 7 May 2018, on the evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products SWD(2018) 157 final. The evaluation aims to assess the 'functioning and the performance' of the PLD for the period 2000-2016 and it covers the EU-28 Member States.

[70] European initiative in the field of the regulation of robotics and AI, with particular regard to civil law rules, are different: European Parliament, Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)); European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and social committee and the Committee of the regions on Artificial Intelligence for Europe, 25 April 2018, COM(2018) 237 final; European Commission, Communication from the commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Coordinated plan on Artificial Intelligence, 7 December 2018, COM(2018) 795 final; European Commission, Report from the Commission to the European parliament, the Council and the European Economic and Social Committee, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, 19 February 2020, COM(2020) 64 final; Study of the European Parliament, Civil liability regime for artificial intelligence, PE 654.178, September 2020; Report from the Expert

Research Centre of the European Commission. The report in-depth safety, security, privacy and societal issues emerging from the use of the Internet of Toys. At the same time, the report underline possible benefits of higher collaboration between research and the Internet Connected Toy Industry in order to make them more trustworthy.

In Italy, the Italian Data Protection Authority has already shown interest on the matter and its risks that have been demonstrated by the informative schedule published on its website.[71] In the schedule, the Italian DPA aims to make aware the community about the functioning and the risks related to smart toys, specifically on data protection and cybersecurity.





Italian Data Protection Authority, Smart Toys: i suggerimenti del Garante per giochi a prova di privacy, 15 October 2018, www.garanteprivacy.it

4. Conclusions: The need for effective preventive and remedial measures.

The straightening of the preventive protection, the enforcement of the duties and of the accountability of the IoToys providers should be implemented. This objective could be realised through the actions of the competent Authorities with their supervisory powers (preventive measures) and, if necessary, imposing high fines (remedial measures), following the way that appears to have been undertaken in recent years. Also, the competent Courts have the power to impose fines and, depending on the case, can be sued as alternatively or in addition to the competent Authorities. Furthermore, it is fundamental the power to orient and positively influence the producers trough soft law (codes of conduct and guidelines),[72] the programmer and the developers.

First of all, it is scientifically proofed that the users do not take necessary attention to the privacy policy and are unaware about the kind of processing of their personal data as well as the kind of data processed.[73] Secondly even when they try to read the policies these appear very difficult to understand. So, more than incentives user to read policies, it should be better to push the producer to respect GDPR principles, writing clear privacy policies and using

Group on Liability and New Technologies, New Technologies Formation, Liability for Artificial Intelligence and other emerging digital technologies, (Publication Office of the European Union, 2019).

[71] Italian Data Protection Authority, Smart Toys: i suggerimenti del Garante per giochi a prova di privacy, 15 October 2018, available at https://www.garanteprivacy.it/iot/smarttoys, accessed 4th December 2020.

[72] *See* A Iannotti della Valle, 'L'età digitale come "età dei diritti": un'utopia ancora possibile?' (n 55); E Mostacci, La soft law nel sistema delle fonti: uno studio comparato (2008) Milano, 2008; A Somma, 'Soft law sed law: diritto morbido e neocorporativismo nella costruzione dell'Europa dei mercati e nella distruzione dell'Europa dei diritti' (2008) 3 Rivista critica del diritto privato, 437 ff.. May me also refers to MC Gaeta, 'Hard law and soft law on data protection: what a DPO should know to better perform his or her tasks in compliance with the GDPR' (2019) 1 EJPLT

[73] L. Gatt, R. Montanari, IA Caggiano (eds), *Privacy and Consent. A Legal and UX&HMI Approach* (n 22).

effective lawful basis for the processing, as well as to introduce safety standards that the producer has to respect in order to put the product on the market and this security standard has to include privacy and security by design and by default measures.

On the side of the *ex post* protection, of course, the roles and liabilities of the producers of smart toys, the software programmers and apps or platforms developers should be better regulated in terms of high fines for the damages occurred and clear right to clime of the damaged party.

Currently, we can still lean towards an extensive application of existing regulations to the Robotic and AI field. However, to allow a linear and controlled development of Robotics an AI, it is necessary to continue in the direction of the periodic review of current legislation in order to verify its applicability to the new scenario characterised by quick development of new technologies or the need to intervene by modifying it.

Although in part it is still possible to go for an extensive interpretation of the existing rules, in the near future the need to introduce a regulatory framework of rule for Robotics and AI, cannot be ignored. Furthermore, a general law for robotics will not be the solution to regulate the different legal types of Robots and AI.

In general, it is necessary that the ethical principles are reliable (to use the words of European Commission, 'trustworthy'[74]) and place the interests of the individual, as a vulnerable subject in relation to new technologies.[75] Therefore, in some specific sectors, such as smart toys, specific attention to the ethical principles should be given, with the function of integrating and assisting the legal regulation. In fact, as we highlighted, the possible emotional bonds between the minor and the toy, as well as risks of psychical manipulation, need an ethical approach to regulation, which considers these peculiarities.

To sum up, the law should keep up with technologies and evolve with them, in order to assure an effective protection of the vulnerable subject and, in this case, of minors, in the digital habitat or, more precisely, digital playground.

In the digital age, a user experience and human machine interface approaches (UX-HMI)[76]

---

[74] *See* European Commission, Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions: Building Trust in Human-Centric Artificial Intelligence COM(2019) 168 final, according to which: 'Only if AI is developed and used in a way that respects widely-shared ethical values, it can be considered trustworthy'. Also *see* HLEG, European Commission, The assessment list for trustworthy Artificial Intelligence (ALTAI) (2020); European Commission, White paper on Artificial Intelligence - A European approach to excellence and trust COM(2020) 65 final; European Parliament, Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), according to which it is necessary to emphasise 'that socially responsible artificial intelligence, robotics and related technologies have a role to play in contributing to finding solutions that safeguard and promote fundamental rights and values of our society such as […] protection of children'. In Italy *see* AGID, Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino (2018).

[75] *See* UNESCO, First draft of the recommendation on the ethics of artificial intelligence (2020), according to which: 'No human being should be harmed physically, economically, socially, politically, or mentally during any phase of the life cycle of AI systems. […] Persons may interact with AI systems throughout their life cycle and receive assistance from them such as care for vulnerable people, including but not limited to children, older persons, persons with disabilities or the ill'. Also see HLEG, European Commission, Ethics guidelines for trustworthy AI (2019), according to which it is also necessary, considering ethical principles, to 'pay particular attention to situations involving more vulnerable groups such as children, persons with disabilities and others that have historically been disadvantaged or are at risk of exclusion'. For the importance of ethics in regulating robotics *see* L Gatt, 'Per un'intelligenza artificiale antropocentrica. Intervista a Lucilla Gatt' [2020] DIMT, available at https://www.dimt.it/news/intelligenza-artificiale-antropocentrica/, accessed 4th December 2020.

[76] Please, refer to the definitions and the examples contained in the book L. Gatt, R. Montanari, IA Caggiano (eds), *Privacy and Consent. A Legal and UX&HMI Approach* (n 22) which is enterally based on the UX-HMI approach.

should be considered for measuring the efficacy and the efficiency of the legal rules and for promoting regulations adequate to the aforementioned digital context. In this sense, it is possible to speak not only of legal regulation but of tech-regulation (for example by implementing the principles of privacy, security and ethics by design and by default). The idea of using technologies to regulate technology itself and, in particular, aspects related to the protection of personal data, goes back to art. 17 of the Directive 95/46/EC, that already introduced the technical and organizational measures that the controller should take to protect the personal data. In those years, the Privacy Enhancing Technologies (PET), i.e. technologies to minimise processing of personal data without losing the functionality of an information system, has been developed.[77]

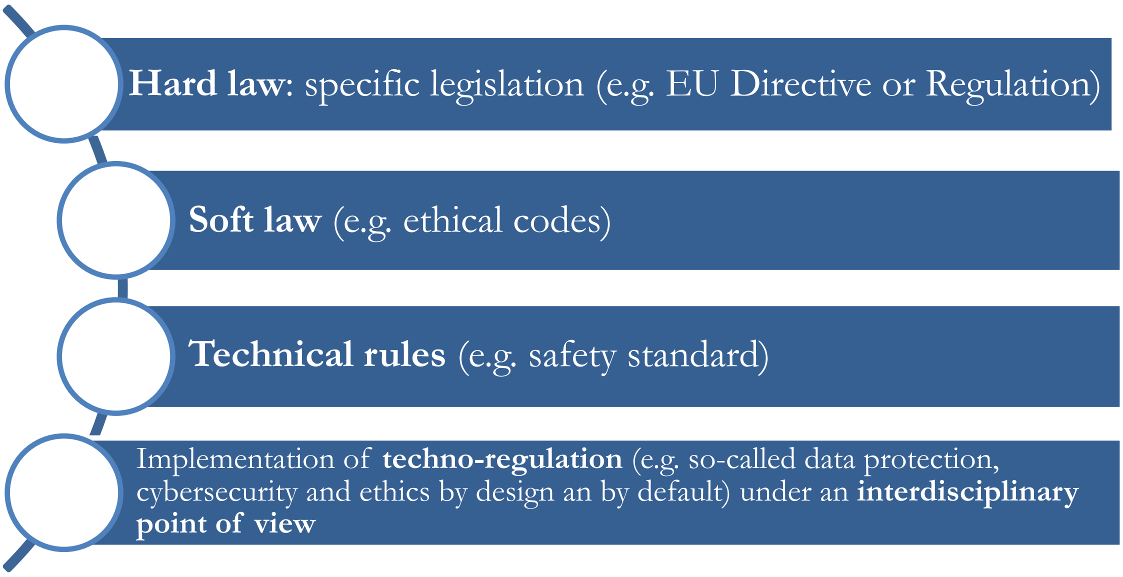
In order to develop techno-regulation, different sciences from the legal one come into play. In fact, nowadays, the level of in-depth analysis required of the new technology law is so high and complex that legal must work in synergy with experts from other sectors of science (e.g. engineers, computer scientists, statisticians, psychologists). As a matter of facts, on one side, legal science needs technical science to understand technologies and provide specific regulations based on its functioning, on the other side, technical science needs the social one for putting in place the principles of techno-regulation based on current law, first of all, hard law, but also soft law, which in this context plays a fundamental role of guidance and orientation.

In the case of the smart toys, which has strong ethical implications, hard law, such as European Directives or Regulations, should be accompanied by soft law, such as ethical codes along with safety standards,[78] to better protect children, as vulnerable subjects, in relation to the risks involved in new technologies.

---

[77] As usual, California is among the leading Countries in the technology sector and in fact one of the first studies on PETs is from California: I Goldberg, D Wagner, E Brewer, 'Privacy-enhancing technologies for the Internet' (1997) Study of the University of California, Berkeley, https://apps.dtic.mil/dtic/tr/fulltext/u2/a391508.pdf, accessed 24 November 2020. Anonymization technology are included in PET and a first complete definition was provided by A Pfitzmann, M Hansen, Marit, 'A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management' (2010) v0.34, Report of the University of Dresden, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, accessed 24 November 2020. In 2003, then, Borking, Blarkom and Olk reviewed the technologies from a data protection perspective in their Handbook of privacy enhancing technologies. An in-depth analysis is included in the book GW van Blarkom, JJ Borking, JGE Olk (eds), *"PET". Handbook of Privacy and Privacy-Enhancing Technologies. (The Case of Intelligent Software Agents)* (CBP, 2003); J Heurix, P Zimmermann, T Neubauer, S Fen, 'A taxonomy for privacy enhancing technologies' (2015) 53 Computers & Security, 1 ff..

[78] The definition of the standard as part of the soft law is frequent today; however, the standards are technical rules that behaves in very different ways, as to its contents and effects. *See* GM Marenghi *Standard e regolazione condivisa* (Giappichelli 2018), 1ff.


Hard law: specific legislation (e.g. EU Directive or Regulation)
Soft law (e.g. ethical codes)
Technical rules (e.g. safety standard)
Implementation of **techno-regulation** (e.g. so-called data protection, cybersecurity and ethics by design an by default) under an **interdisciplinary point of view**