Let the Children Play. Smart Toys and Child Vulnerability*

Alessandra Pera, Sara Rigazio

A. Introduction

In the 1990s, children played with their toys asking questions and giving themselves the answers. Today, smart toys talk with the children through artificial intelligence and voice recognition systems, engaging in conversations and interacting with them, sharing stories and tailoring answers according to the kids' preferences. As a matter of fact, the extremely rapid technological advancement of recent years has abruptly affected also the children's entertainment sector, starting a completely new era.

Further confirming the growing importance and popularity of these new and revolutionary gaming instruments, in 2021 the World Economic Forum itself dedicated extensive research on this topic showing, indeed, that the trend is for the smart toy market to grow considerably over the years, increasing its market share by almost 200% from 2018 to 2023[1].

While smart toys' features offer undoubtedly exciting and educational opportunities, at the same time they raise several questions, mainly in terms of privacy, children's agency and market regulation, that all relate to the condition - concrete or potential, as further discussed below - of children's own vulnerability.

Therefore, this essay focuses on the concept of vulnerability and explores the vulnerable condition that arises from the use of these tools specifically in children belonging to the 5-10 age range group. This age range is the result of a precise methodological choice based on the two dimensions of this work, that are the taxonomy and the case-based one, respectively.

---

* This chapter is the result of a common research and reflection of the two authoresses. However, only within the scope of research evaluations, Alessandra Pera drafted Sections 2 and 3, while Sara Rigazio drafted Sections 4 and 5. The Introduction (section 1) and the conclusions (section 6) were co-authored.

1 Seth Bergenson, 'Smart toys: Your child's best friend or a creepy surveillance tool?' (*World Economic Forum*, 31 March 2021) <https://www.weforum.org/agenda/2021/03/smart-toys-your-child-s-best-friend-or-a-creepy-surveillance-tool/> accessed September 2023.

The first, relates to the multidimensional character and to the multifaceted factors of vulnerability that can vary, as we will explain in details, according to the context the individual is living in; the second, relates to the practical approach- that is necessary even if we work on taxonomies- linked to the case studies we analyze, that involve AI dolls and robots, quintessentially targeted at children-consumers of this age range.

In particular, through the analysis of two case studies, it shows some of the threats and the risks children can face, advancing some arguments on the possible alternatives and responses.

Whilst the concept of vulnerability is usually defined broadly as "the quality of being weak and easily hurt physically or emotionally"[2], referring to external risks, stress factors and circumstances within which an individual could be deprived of the capacity to self-determine and choose freely, we decide to employ a very exhaustive taxonomy that focuses on the different vulnerability's sources[3]. As we will explain in details, we apply the distinction between inherent and situational vulnerability, the first depending on intrinsic characteristics of the human nature, while the second mostly on the external setting. Through this distinction we can identify the sources of vulnerability in a specific case, making references to risk factors and highlighting their consequences.

The topic of smart toys shows, indeed, a multidimensional vulnerability often correlated within the context surrounding the kids. Consequently, our analysis engages with the intersectionality theory. As its leading thinker and scholar Kimberlé Crenshaw explains, various forms of inequality and oppression often operate together, exacerbating each other. To understand the real condition of the individual, then, it is necessary to look at the experience that the individual is going through, as a whole[4].

Such approach, therefore, will allow us to focus on the context-dependency of the personal experience of intersectionality including the inherent and the situational vulnerability: the single child or a specific type of vul-

2 See Oxford Dictionary, <https://www.oxfordlearnersdictionaries.com/definition/english/vulnerability?q=vulnerability> accessed September 2023.

3 Catriona Mackenzie, Wendy Rogers and Susan Dodds, 'Introduction: What Is Vulnerability and Why Does It Matter for Moral Theory?' in Wendy Rogers, Catriona Mackenzie & Susan Dodds (eds), *Vulnerability. New Essays in Ethics and Feminists Philosophy* (Oxford University Press, 2014) 1, 29.

4 Kimberlé Crenshaw, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination doctrine, Feminist Theory and Antiracist Politics' (1989) Un. Chi. Legal Forum 139.

nerable child might be individually exposed to many needs and restraints, meeting various social expectations, or dependent on limited material and social resources. While being exposed to a stable set of categorical (structural) interferences, the same child could encounter different forms of intersectionality within different backgrounds (i.e. inside the family, at school, at the hospital, in the religious community).

Within this framework, the response of the institutions, family and business operators, while noticeably complex, is equally necessary. Most importantly, we argue that the guiding principle of these actions must always stand for preserving and promoting the dignity of the person[5]. As we will try to foster through our analysis, the value of dignity represents the only and unique safeguard against the idea that the individual, and even more a child, represents solely an object and a source for data mining and collecting information.

Our paper is organized as follows: in the first part we will outline the concept of vulnerability by dwelling on the inherent-situational taxonomy referred to, continuing with the analysis of the two cases concerning smart toys and the issues underlying them, also with the support of the intersectionality theory. In the second part we will deal with the responses of the different actors involved to the concerns raised, suggesting that a child-centred approach, always oriented toward the fulfilment of the best interest of the child, not only is possible but imperative.

B. Vulnerability as a multidimensional concept

As Robert Chambers critically observed in his editorial of 1989[6], "Vulnerable and vulnerability are common terms in the lexicon of development but their use is often vague"[7]. Frequently confused with or used as a synonym of poverty or weakness, this author stressed instead the necessity and the opportunity of focusing on the effects vulnerability produces, that are the limitation or reduction of a person in her capacity, power or control to

5 See Stefano Rodotà, *Il diritto di avere diritti* (Laterza, 2015) 197.

6 Robert Chambers, 'Editorial Introduction: Vulnerability, Coping and Policy' (1989) 20 IDS Bulletin 1.

7 On the vagueness and the complexity of the term, see also Doris Schroeder, Eugenijus Gefenas, 'Vulnerability: Too Vague and Too Broad? (2009) (18) 2 Cambridge Quarterly of Healthcare Ethics 18.

protect her interests. From a biological or physiological perspective, then, vulnerability refers to a person's intrinsic characteristics and to a deficiency of means to manage without detrimental loss. In a social and relational length, therefore, vulnerability affects human being's access and effective exercise of fundamental rights and freedoms, undermining autonomy, curtailing individual capabilities or creating a sense of powerlessness[8].

In a similar perspective is the definition given by the UN Division of Social Policy and Affairs, which refers vulnerability to "a state of high exposure to certain risks, combined with a reduced ability to protect or defend oneself against those risks and cope with their negative consequences"[9].

As previously mentioned, we choose a different, specific approach to investigate vulnerability that is the one that takes into consideration and describes its different sources. Indeed, some authors[10] have proposed a very exhaustive taxonomy that distinguishes between inherent and situational vulnerability. The former, relies on the intrinsic characteristics of the human nature, connected to corporeality and dependent on others affective and social natures. The latter, instead, depends mostly on the external context and may be influenced by the personal, social, political, economic or environmental circumstances within which individuals or social groups live in, including oppression, domination and injustice. This last category stresses on inequalities of power, dependency, capacity or need, which could make a person vulnerable to harm or exploitation by others.

Inherent and situational vulnerability may be either dispositional (potential) or occurrent (actual). For example, considering our topic, minor children are dispositional vulnerable to digital technologies, but whether or not they will be actually harmed by them, it depends on a range of diverse factors, such as their age, capacity of understanding and consequently will and self-determination, level of digital literacy (personal and of the members of the family), level of education, family support, socio-economic status, their geographical location, the school infrastructures (material and human resources) and so on.

8 Martha Nussbaum, *Women and human development: the capabilities' approach* (Cambridge 2000). There are also scholars who criticise only negative association of vulnerability. For example, see Erin C. Gilson, *The Ethics of Vulnerability: A Feminist Analysis of Social Life and Practice* (New York and London Routledge 2016) 7, 8.

9 Division of Social Policy and Affairs, *Report on the world social situation, social and human rights questions: social development*, UN (United Nations), New York, 2001.

10 Catriona Mackenzie, Wendy Rogers and Susan Dodds, n 3 above.

As it becomes clearer, this distinction plays a crucial role since not only does it allow a more complete analysis of the specific situation of vulnerability at stake, but it also offers the opportunity to capture the peculiar side of the concept of vulnerability itself, i.e. its dynamic and layered dimension and nature. Moreover, this new framing is consistent with the recent critical advances in the vulnerability discourse that have criticized a static, stigmatized and categorical notion in favour of an alternative approach[11]. An interesting example is given by some policy documents from the European Commission in the matter of vulnerable consumers, where an evident change toward a new conception of vulnerability can be clearly observed[12]. Indeed, a new interpretation of the Commission recalls "that consumer vulnerability is situational, meaning that a consumer can be vulnerable in one situation but not in others, and that some consumers may be more vulnerable than others"[13]. Such a *dynamic* approach, therefore, can be reasonably deemed acquired in the broader theoretical vulnerability discourse[14].

11 One of the most prominent scholars who advances an alternative approach to vulnerability is Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2009) (20) Yale Journal of Law and Feminism, 23. In her vulnerability theory she employs the idea that "no individual can avoid vulnerability". See also Alison Cole, 'All of us are vulnerable, but some are more vulnerable than others: The political ambiguity of vulnerability studies, an ambivalent critique' (2016) 17(2) Critical Horizons 260, 277; Gianclaudio Malgieri, Jędrzej Niklas, 'Vulnerable data subjects' (2020) 37 Computer Law & Security Review 105415; Lourdes Peroni, Alexandra Timmers, 'Vulnerable groups: The promise of an emerging concept in European human rights convention law' (2013) 11(4) International Journal of Constitutional Law 1056, 1085; Carol Levine et al., 'The Limitations of 'Vulnerability' as a Protection for Human Research Participants' (2004) 4 (3) The American Journal of Bioethics 44; Ryan Calo, 'Privacy, Vulnerability, and Affordance,' (2017) 66 DePaul L. Rev., 592.

12 London Economics, VVA Consulting, & Ipsos Mori consortium (2016). Consumer vulnerability across key markets in the European Union. Study for the European Commission, DG Justice and Consumers, Brussels <https://commission.europa.eu/system/files/2018-04/consumers-approved-report_en.pdf.> accessed September 2023.

13 European Commission. (2016). Understanding consumer vulnerability in the EU's key markets. Factsheet, Brussels <https://commission.europa.eu/system/files/2018-04/consumer-vulnerability-factsheet_en.pdf> accessed September 2023.

14 This approach has been employed also in the vulnerability assessment of refugees. In this respect, among others, see Daria Mendola, Alessandra Pera, 'Vulnerability of refugees: Some reflections on definitions and measurement practices' (2021) International Migration, 00, 1, 14.

Whilst Kate Brown and others pointed out, indeed, "the ubiquity and elasticity of [the term] vulnerability generates a sense of familiarity and common-sense or assumed understandings which conceals diverse uses with enormously varied conceptual dimensions"[15].

Accordingly, we shall now look at the specific case of the smart toys.

C. Smart toys

With the rise of the Internet of Things (IoT)[16], a growing number of households devices from television, security systems, to cooling and heating tools, are now able to perform a range of functions thanks to the Internet connectivity, sharing data[17]. Among them, toys have become part of the digital world as well, with the growth of the so called smart connected toys. Smart connected toys, or simply smart toys, are devices that encompass physical components of traditional toys connected to computer systems with online communication services. Given the fact that they can connect to mobile and cloud services, as well as to other smart toys, game consoles, tablets or smart phones, and also to underline how popular and widespread

15 Kate Brown, Kathryn Ecclestone and Nick Emmel, 'The Many Faces of Vulnerability' (2017) 16(3) Social Policy & Society 497, 510.

16 The term 'Internet of Things' is attributed to Kevin Ashton. See Kevin Ashton, That Internet of Things, RFID J. (June 22, 2009) <http://www.rfidjournal.com/that-internet-of-things-thing>. There is no universally agreed-upon definition, but generally, the term is used to describe networks of objects that are not themselves computers but have embedded components connected to the Internet. "Things" may include, for example, fitness trackers, personal vehicles, home appliances, medical devices, and even clothing used by individual consumers. The IoT potentially includes huge numbers and kinds of interconnected objects. In practice, IoT refers not to a simple or uniform network of objects but rather to a complex collection of objects and networks. See, Roberto Minerva, Abyi Biru, Domenico Rotondi, 'Towards a Definition of the Internet of Things (IoT)' (IEEE Internet Initiative, May 27, 2015), <http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf> accessed September 2023.

17 See Vivek Wadhwa, When the Toaster Shares Your Data with the Refrigerator, the Bathroom Scale, and Tech Firms, Singularityhub (June 30, 2015) <https://singularityhub.com/2015/06/30/when-the-toaster-shares-your-data-with-the-refrigerator-the-bathroom-scale-and-tech-firms/> accessed September 2023.

they have become in the recent years, some authors have even proposed the concept of the Internet of toys[18].

Recent reports have indeed confirmed that smart toys will represent an $18 billion software and hardware market by 2023, starting from an estimated $6 billion in 2018[19]. This increase is due mainly to the growing popularity, as mentioned, of smart-phones connected toys and related in-app purchases. In addition, another element to take into consideration is the flourishing market of educational smart toys, which grew exponentially especially during and after the pandemic and that now are often part of the schools' curricula[20].

Although there is no consensus regarding smart toy terminology, this phrase has long been used in the industry[21]. Consumers, usually, refer to smart toys in contrast with traditional toys such as puzzles or board games. The latest and most innovative examples are characterized by the direct interaction systems between the child and the toy, A.I. devices employed, image and voice processors and, of course, Internet connection through iOS or Android mobile applications.

As previously pointed out, the issues underlying the use of smart toys are several and diverse. In order to identify the profiles that we think affect and contribute mostly to the children's vulnerable condition, we decided to analyze two examples of recent marketed smart toys: *My friend Cayla* and *i-Que Intelligent Robot.*

I. The case studies

My friend Cayla and *i-Que Intelligent robot* are two Internet-connected toys, targeted to young girls and boys in the 5-10 age range, that talk and interact with children by capturing and recording children's communications

18 See, Wem-Nan Wang, Vivian Kuo, Chung-Ta King, Chiu-Ping Chang, 'Internet of Toys: An e-Pet overview and proposed innovative Social Toy Service Platform' *(2010) International Computer Symposium (ICS2010)*, Tainan, Taiwan, 2010, 264.

19 See Juniper Research (2018) <https://www.juniperresearch.com/press/smart-toy-revenues-grow-almost-200pc-by-2023> accessed September 2023.

20 Mariya Stoilova, Sonia Livingstone, Rana Khazbak, *Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes* (2021) *Innocenti Discussion Papers*, no. 2020-03, UNICEF Office of Research - Innocenti, Florence.

21 P.C.K. Hung, L. Rafferty, M. Fantinato 'Toy computing' in N. Lee (Ed.), *Encyclopedia of Computer Graphics and Games* (Springer Verlag 2019).

and by analyzing the recordings to determine the words spoken. They are both produced by Genesis Toys, a company based in California, which also markets and sells several other interactive toys and robots in the United States and abroad. In 2016 Genesis went under the scrutiny and was the object of an investigation by the Federal Trade Commission (FTC), as well as by the German Federal Network Agency and the Norwegian Consumer Council[22].

Specifically, Cayla and i-Que are made of two components: a physical doll and a companion mobile application.

The physical doll includes a Bluetooth microphone and a speaker and the companion app provides the data processing to enable the toy's ability to capture the private communications of children. Before playing with them, children are required to download the Cayla and/or i-Que application on a mobile device, to which the doll connects using Bluetooth technology. The companion apps are available from the Google Play and iTunes app stores.

Interestingly, the companion app for Cayla requests permission to access the hardware, storage, microphones and Wi-Fi connections, but fails to explain the significance of this permission. I-Que asks for access to the device camera even though the camera itself is not necessary to the robot's functionality and neither is explained to the users. Once the companion app establishes a Bluetooth connection, it connects the smart toys to the Internet. Cayla and i-Que record the conversations they have with the kids; moreover, the children's statements are converted into text that it is used to retrieve answers in Google or in Wikipedia.

Cayla and i-Que encourage children to converse openly with the toys, as if they were with a friend. According to the FTC's findings, Cayla was pre-programmed with many phrases that referenced to Disneyworld and Disney movies. For example, Cayla kept repeating that her favorite song was the one from the movie Frozen. And that she wanted to go to Disneyworld. This product placement was not disclosed so that parents were completely unaware of this in the conversations their child had with

22 See Federal Trade Commission, 6 December 2016, Genesis Toys and Nuances Communications <https://epic.org/wp-content/uploads/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf> accessed September 2023; Bundesnetzagentur removes children's doll "Cayla" from the market <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422> accessed September 2023; <https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws> accessed September 2023.

the doll. Similarly, i-Que was programmed to tell funny stories as well as scientific facts and to make strange sounds.

In addition, both Cayla and i-Que were programmed with a kid safe proprietary software, called Violet, designed to protect children from sensitive images or words that parents did not want the doll to use in front of their children. The Cayla companion app requires then a series of information to be set up: the kid's name, the parents' name, their favorite movie, their favorite meal, the name of the place where the kid lives, which school the kid goes to. Finally, Cayla explicitly invites children to set up their physical location in the general setting of the doll.

After some investigations, the FTC found out that Genesis did not comply with the general provisions regarding parental consent in order to collect, use or disclosure the personal information recorded in Cayla and i-Que[23] according to the Children's Online Protection Act (COPPA)[24]. Indeed, the company violated COPPA "by failing to make reasonable efforts to ensure parents receive direct notice of its information practices, including direct notice of any material changes to those practices"[25].

Consequently, as previously recalled, also Germany and Norway started investigating and, as a result, they banned Cayla and i-Que from the market.

In particular, the German Federal Network Agency classified Cayla as an "illegal espionage apparatus" so that retailers and owners could face fines if they continued to stock the toy or fail to permanently disable the doll's wireless connection. According to the Agency, indeed, "the toy can be used

23 See Federal Trade Commission, 6 December 2016, Genesis Toys and Nuances Communications, point n. 58 <https://epic.org/wp-content/uploads/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf> accessed September 2023.

24 Children's Online Privacy Protection Act, 16 C.F.R. This Act regulates the collection of children's personal information by operators of online services. It applies to operators of online services, websites, and apps directed to children under 13 as well as operators of online services, websites and apps serving a general audience. See Eldar Haber, 'The Internet of Children: protecting Children's Privacy in a Hyper-Connected world' (2020) (4) University of Illinois Review 1209. The bibliography on COPPA is evidently large. On the specific matter of processing children's data, also in a comparative perspective, see Milda Macenaite, Eleni Kosta, 'Consent for processing children's personal data in the EU: following in US footsteps?' (2017) 26 (2) Information & Communications Technology Law 146.

25 See Federal Trade Commission, 6 December 2016, Genesis Toys and Nuances Communications, point n. 97 <https://epic.org/wp-content/uploads/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf> accessed September 2023.

by anyone in the vicinity to listen in on conversations undetected". Moreover, the Agency started further investigation against the manufacturers on the ground that they violated also section 90 of the German Telecommunications Act, according to which "Objects must, by their form, purport to be another object or are disguised as an object of daily use and, due to such circumstances or due to their operation, are particularly suitable for intercepting the non-publicly spoken words of another person without his detection or for taking pictures of another person without his detection"[26].

The Norwegian Consumer Council as well looked at the terms and the technical features of Cayla and i-Que, finding a serious lack of protection of children's rights in general, and to privacy and security in particular[27]. Specifically, the report underlined the actual security flaws that, as documented, led already to an episode of hacking in 2015. Nevertheless, this episode was quickly dismissed by the company as an isolated event with no consequences for the marketing of the doll[28]. As a matter of fact, a series of technical tests performed by the Norwegian authority demonstrated that

26 See, Bundesnetzagentur removes children's doll "Cayla" from the market <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422> accessed September 2023.

27 Interestingly, beyond the most evident issues on privacy and security, the report underlined also that these smart toys encouraged and embody the actual debate on sexism. As a matter of fact, taking into consideration the three smart toys considered – My Friend Cayla, i-Que Intelligent Robot and Hello Barbie – "Hello Barbie is very interested in talking about clothes and toys, although she will also occasionally suggest career choices such as "politician". Cayla is happy to chatter about family, friends, and cooking, while the i-Que robot mostly steers the "conversation" toward science, lasers, and silly jokes". This aspect looks much more serious if we think that Cayla and i-Que come also with the option of simulating real conversation with the child. Finally, the Norwegian report reminded also that the Norwegian version of the app in Cayla banned words such as "homo- sexual", "bisexual", "lesbian", "atheism", and "LGBT". See <https://storage02.forbrukerradet.no/media/2016/12/toyfail-report-desember2016.pdf>, accessed September 2023, 35.

28 See '#Toyfail An analysis of consumer and privacy issues in three internet-connected toys', December, 2016 <https://storage02.forbrukerradet.no/media/2016/12/toyfail-report-desember2016.pdf> accessed September 2023. It is the report commissioned by the Norwegian Consumer Council, part of the larger project centering on the Internet of Things (IoT), that chose to analyze the three most popular smart toys available on the market at that time: My Friend Cayla, i-Que Intelligent Robot and Hello Barbie.

neither of the statements made by the manufacturer company about the security measures put in place to protect children, were true[29].

As it becomes clearer, Cayla and i-Que represent a vivid example of the risks and threats kids face when using smart toys without any control or compliance with the rules. The underlying issues, as we explained at the beginning, are diverse and concern multiple aspects such as the protection of privacy and the regulation mechanisms offered by the market. These issues, while peculiar in their specificity, still concur and can be traced to the concept of vulnerability, which, in the case we investigated, proves to be certainly multidimensional.

And as our analysis chooses and looks exactly to the dynamic and multifaceted notion of vulnerability[30], we apply now the taxonomy we have referred to before, to the concrete cases of Cayla and i-Que.

D. Case subsumption and use of taxonomies

Based on the taxonomy Mackenzie and others have proposed, and taking into consideration what we have underlined regarding the need to assume a dynamic approach on the vulnerability discourse, we can now argue that the phrase 'children between 5 and 10 years old are vulnerable when playing with smart toys', does not give any useful information.

Instead, we should argue that: being a child in the age range 5-10 years old makes you indeed *dispositional* vulnerable to diverse types of exploitation in the digital world (economic, sexual, psychological) and *occurrent* vulnerable if, as a matter of fact, Cayla or i-Que spied on you, recorded your voice, took your picture and your market preferences have been collected, shared and sold to other companies for profiling.

Once clarified this distinction, at the same time, the situational vulnerability becomes dispositional when the same child lives in a particular situation: for example, is left alone most part of the day, the only existing parent works and has no high level of education, also digitally speaking. The situational vulnerability, then, becomes occurrent if, for instance, a

29 See < https://storage02.forbrukerradet.no/media/2016/12/toyfail-report-desember2016.pdf> accessed September 2023, 32.

30 In this respect, see Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2 International Journal of Feminist Approaches to Bioethics 121; Florencia Luna, 'Identifying and Evaluating Layers of Vulnerability – a Way Forward' (2019) 19 Developing World Bioethics 86.

family member gives the same child Cayla or i-Que as a gift and the child plays with it without any type of guidance or control for hours every day.

Applying this taxonomy clearly increases the variables concerning the vulnerability condition to consider, making it more difficult in some sense to identify and connect with each other the different sources of vulnerability. At the same time, tough, as the example clearly shows, it allows to recognize a peculiar situation of vulnerability distinguishing case by case (the child with no help from the family members from the child who, instead, lives in a situation where she has help and opportunities and is guided through the digital environment) and, most importantly, to decide and implement the right responses by the legal system and, in general, by the institutions[31].

Specifically in relation to the answers that can be given to erase or diminish the vulnerability's conditions, we believe that our analysis should also look at and could benefit from what Robert Goodin calls "pathogenic vulnerability"[32]. According to Goodin, this particular type of vulnerability depends on "all those morally unacceptable vulnerabilities and dependencies which we should, but have not yet managed to, eliminate". These are caused by prejudice or abuse in interpersonal relationships and by social domination, oppression, or political violence. The expression "pathogenic vulnerability" contributes to stress the attention on some institutional interventions, drafted to amend inherent or situational vulnerability, which, instead and in concrete circumstances, can have the paradoxical effect of increasing vulnerability[33].

In the case of children and smart toys is clear that all types of vulnerability co-exist: inherent and situational, occurrent and dispositional, with the risk of creating a pathogenic one. This is why we need also to consider the intersectionality theory.

---

31 In the matter of wrong responses by the institutions, see also Alessandra Pera, 'Il difficile bilanciamento tra tutela della madre vulnerabile, best interest del minore e diritti culturali della donna migrante al vaglio della Corte Europea dei Diritti dell'Uomo' (2021) (3) Comparazione e diritto civile 1179, where the author, retracing the case of a migrant woman whose daughters were given in adoption after she was considered unable to take care of them, suggests that, instead, a correct analysis of the woman's vulnerability, based on the taxonomy inherent/situational, could have prevented such a decision.

32 Robert E. Goodin, *Protecting the vulnerable: a reanalysis of our social responsibilities* (Chicago 1985) 203.

33 Catriona Mackenzie, Wendy Rogers and Susan Dodds, 'Introduction: What Is Vulnerability and Why Does It Matter for Moral Theory? 39.

As it is well known, the notion of intersectionality was originally conceived in the area of gender studies: Kimberlé Crenshaw used the metaphorical image of a car accident occurring at the crossroad of several streets or axes of discrimination to represent the sociocultural composition of underprivileged groups - in this case of black women - highlighting that inequality tends to be constituted by particular situations and contexts rather than by uniform class structures. In a famous article entitled "Demarginalizing the Intersection of Race and Sex"[34], the authoress describes the dynamics by which these two identity characteristics intersect with each other and the way in which their combination actually reinforces the subordination of black women.

What has to be underlined is that intersectionality is more than a mere sum of factors, in which one form of subordination is added to the other, as a sort of double oppression, mutually reinforcing each other; but represents a *combination* of factors that interact with each other, influence and determine each other without being able to be distinguishable anymore, causing further prejudice, beyond that caused by each singular form of subordination[35].

While there were preliminary uncertainties about the application of the theoretical premises of intersectionality in other disciplines different from the gender studies, and on the opportunity of taking into consideration additional axes or factors, such as age, ability, religion, and ethnicity[36], this theory has in fact gradually become established and widespread in Europe as well[37].

---

34 Kimberlé Crenshaw, 'Demarginalizing the intersection of race and sex: a black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics' (1989) cit; Kimberlé Crenshaw, 'Mapping the margins: Intersectionality, identity politics, and violence against women of colour' (1991) 43(6), Stanford Law Review 1241, 1299; Kimberlé Crenshaw, 'Twenty Years of Critical Race theory: Looking back to move forward', (2011) (43) Conn. L. Rev. 1253.

35 On the complexity that characterizes the concept of intersectionality, see Leslie McCall, 'The complexity of intersectionality' (2005) 30(3) Signs: Journal of Women in Culture and Society 1771. See also, Ann Phoenix, Pamela Pattynama, 'Intersectionality' (2006) 13 (3) European Journal of Women's Studies 187.

36 Mieke Verloo, 'Multiple Inequalities, Intersectionality and the European Union', (2006) 13(3) European Journal of Women's Studies 213; Knap 2008.

37 See Giovanni Marini, 'Intersezionalità: geneaologia di un metodo giuridico' (2021) (4) Rivista Critica del Diritto Privato 472, 475 who describes intersectionality as a 'travelling theory' for its capacity of being beyond the time and space dimensions and geographical borders. For this reason, the author suggests that it would be more useful not to consider intersectionality as a theory; rather, an approach.

For the purposes of our analysis, intersectionality becomes relevant where it represents an additional opportunity and a privileged tool for observing and, possibly, understanding better the vulnerability's condition. It is exactly in this perspective, then, that the context-dependency we referred to when analyzing the child - smart toy interaction, gets significance.

The common core linking the three different kinds of vulnerability distinguished above (inherent, situational and pathogenic) together with the approach of intersectionality is that they can explain the troubling sense of powerlessness, loss of control, loss of agency, which are common when we talk about vulnerability. Therefore, the discourse on vulnerability is enhanced with an additional element: *intersectional vulnerability*, giving (cross) relevance to the different and concurring factors of vulnerability and how they affect children; their treatment and the assessment of public and private remedies to reduce or exclude vulnerabilities' effects and intersectional harm. Such approach might be useful in evaluating the adequateness and efficacy of interventions drafted to improve the conditions of the children when using smart toys and to reduce their vulnerability.

E. Institutional policies and responses

It is within this 'new' framework that we have developed, that we now look at the issue of the responses and the choices that institutions and legal systems are called upon to make. Interesting examples of such responses in this respect are the UK Children's Code, the California Age-Appropriate Design Code, as well as the recent initiatives undertaken by the European Union.

The UK Age-Appropriate Design Code or Children's Code is a code of conduct issued by the Information Commissioner's Office in England[38], entered into force in September 2020[39] – the first of its kind - aimed mainly at information service providers who manage data for online services such

38 The ICO is the UK's independent body set up to uphold information rights. The principal task of this office is to uphold information rights in the public interest. Specifically, the ICO covers different subject' matters such as data protection, privacy and electronic communications, freedom of information, eIDAS regulation. The work of ICO includes also a dedicated priority to artificial intelligence. See < https://ico.org.uk> accessed September 2023.

39 The Code was issued on 12 August 2020 and came into force on 2 September 2020. As stated in the Code, providers should bring their processing in line with the standards in this code by 2 September 2021. See, <https://ico.org.uk/for-organisations/guide-to

as apps, games, websites and social media that minors are *likely* to access. This code provides for a group of 15 standards that are defined as "a set of technology-neutral design principles and practical privacy features".

Part of these standards concern the personal interaction between the child and the technological tool: indeed, we find the standards regarding the data protection assessment, the fulfillment of the best interest and the default setting. The rest of the standards provided are more focused on aspects related to the functions of the technological tool and the potential harms that could derive from it.

As a matter of fact, we find the geolocation, the profiling, the data sharing standards and the part related to the smart toys. In this respect, the code offers interesting and straightforward guidance to business operators since it clearly requires that the types of data that will be processed by the smart toy (personal and family member's information for example) when connected to the Internet, is fully disclosed in advance[40]: this means, in practice, helping to create the conditions in order to avoid or, at least, to limit the possibilities of occurrent vulnerability to happen. Furthermore, when the code requires that this disclosure of information should take

-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/transitional-arrangements/#code2> accessed September 2023.

40 See standard n. 14 of the Code and the guidance <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/14-connected-toys-and-devices/> accessed September 2023. Also, in this respect, the idea of acting 'before' refers to the 'design thinking'. Since it was first used in the context of organizations, the 'design' term has over time taken on different nuances and traits depending on the context in which it was employed. The idea behind this new approach is to put the person, who may be the user of a good or service or the recipient of a decision, at the center. Scholars from different disciplines have then gradually tried to apply it in many diverse areas of interests, including the legal context. Without any attempt to be exhaustive, see Batya Freedman, considered the leading scholar in the value sensitive design, David G. Hendry, Batya Friedman, 'Value sensitive design as a formative framework', Ethics and Information Technology, 2021, 23, 39, 44; Helen Nissenbaum for the responsible design, Lucas D., Introna, Helen Nissenbaum, 'Shaping the Web: Why the politics of search engines matters', The Information Society (2000) 16, 3, 169; Lee A. Bygrave for privacy design related issues, 'Security by Design: Aspirations and Realities in a Regulatory Context', Oslo law review (2021) 8, 3; Ann Cavoukian, Privacy by Design: The 7 Foundational Principles, <https://www.ipc.on.ca/wp-ontent/uploads/Resources/7foundationalprinciples.pdf> accessed September 2023; Margareth Hagan, Law by design <lawbydesign.co> accessed September 2023; Lina Jasmontaite et al., 'Data Protection by Design and by Default', (2018) 4 European Data Protection Law Review 168.

place "just in time" and be facilitated through interactive messages with the user, this means also to intervene on the situational vulnerability when it could turn on to dispositional /occurrent. In the example we made above, applying the taxonomy to the child who lives in a particular disadvantaged situation in terms of lack of instruments available, the fact that all the information regarding the data processing is given in advance at the moment of the purchase, and also during the use of the smart toy, can evidently diminish the possibilities of her vulnerability.

Moreover, there is another aspect that deserves to be emphasized and it is the fact that the overall structure of this code fully reflects the rationale behind the UN Convention on the rights of the child[41], not only where it explicitly mentions it, but where the entire framework is an expression of it. As it is indeed stated, the code aims to protect the child *within* and not *from* the digital dimension[42]. This means that the code has made as its own the fundamental principle that the child, an active subject in the digital realm and in the legal system, should be recognized, according to the level of maturity demonstrated, gradual autonomy[43]. In relation to vulnerability,

41 A/RES/44/25. The U.N. General Assembly approved the Convention on the Rights of the Child (CRC) on 20 November, 1989, in New York. The Convention entered into force on 2 September 1990. Nowadays, it is the most recognized and ratified international document, with the sole exception of the United States of America. The text of the Convention is available on the U.N. website at <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child> accessed September 2023. For a general overview on the UN Convention, see Phylip Alston, J Tobin, *Laying the foundations for Children's rights* (Innocenti UNICEF 2005); Rachel Hodgkin, Peter Newell, 'Implementation handbook for the Convention on the Rights of the Child' (Innocenti UNICEF 2007); D. McGoldrick, 'The United Nations Convention on the Rights of the Child' (1991) 5 International Journal of Law and the Family 132.

42 See the executive summary of the UK Children's Code, https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/executive summary/ accessed September 2023.

43 The reference is to art. 5 of the UN Convention on the Rights of the Child according to which *States Parties shall respect the responsibilities, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention".* Particularly relevant, even tough written in a complete different setting where the digital dimension was still far away, the words by Gerison Lansdown, *The Evolving Capacities of the Child* (Innocenti UNICEF Firenze 2005): "*Action is needed in law, policy and practice to promote cultural change in which the contributions children make and the capacities they hold are acknowledged" e, ancora, "[…] the*

this reinforces, in turn, the idea that the context-dependency perspective (i.e. the gradual autonomy), is able to catch the dynamic essence and the in-progress nature of vulnerability itself, taking into consideration all the different possibilities according to the taxonomy we have explained.

Imitating the model of the UK Children's Code is the California Age-Appropriate Design Code (CAADC)[44], approved on September 15, 2022 by the California Assembly[45]. The CAADC is modelled after the UK Children's Code and it also targets primarily all services on line that are *likely* to be used by minors. Interestingly, the CAADC recalls the concept of the best interest of the child many times in the text. This seems quite remarkable considering that the United States is the only country that has not ratified the UN Convention yet[46].

The European Union has also shown a growing interest and commitment to the issue of children's protection in the digital environment in general. It should, moreover, be noted that as early as 2012 the Commission launched the "Better Internet for kids – BIK+" initiative, which consisted of a real strategy of action on four main guidelines, concerning: the quality of online content aimed at minors, the awareness and subsequent empow-

---

most critical challenge is to create a better dialogue between adults and children about how the adult world can meet its responsibilities to fulfil, respect and protect children's rights". See, also, Sheila Varadan, 'The Principle of Evolving Capacities under the UN Convention on the Rights of the Child, (2019) (27(2)) The International Journal of Children's Rights 306.

44 AB2273 California Age-Appropriate Design Code, to entry into force on July 1st, 2024, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273.

45 At present, it is worth recalling that on September 18, 2023 a federal judge granted a preliminary injunction in favor of NetChoice, saying that the California Age-Appropriate Design Code violates the First Amendment. The rationale behind the decision lies in the fact that the law would force web sites to erect barriers on children and adult alike. In particular, the judge contested that the age verification method could involve invasive technology like face scans or biometric information. The motion was presented by NetChoice, a national trade association of online businesses whose members include, among others, Big Tech. The judge affirmed that NetChoice is likely to prevail on its claim that the CAADC violates First Amendment, so that the law cannot be enforced. At the moment, the State could still appeal the injunction. Nevertheless, the draft of the CAADC could serve as a roadmap for the future.

46 The reasons behind the missing ratification of the UN Convention on the Rights of the Child by the USA are multiple and diverse and they would go beyond the scope of this paper. For an overview on this matter, see the interesting analysis by Silvia Sonelli, 'I Children's Rights nel diritto statunitense tra Costituzione e Convenzione mancata', (2019) 3 Rivista Critica del Diritto Privato, 415.

erment of minors themselves, the creation of a safe digital environment and, finally, the fight against sexual abuse and the dissemination of child pornography online[47]. Since 2012, there have been many other projects, which have also gone hand in hand with as many legislative changes within the Union, by the EU institutions, at the forefront of child protection.

As a matter of fact, the 2012 BIK+ strategy was updated in 2022 in light of the imminent passage of the Digital Services Act and the commitment made in the proposed regulation on the European Digital Identity (EDi)[48]. Similarly, the European Data protection board's guidelines on data relating to children, expected soon, as announced in the work program 23/24[49], will also be relevant. Of all the initiatives, certainly the most significant in terms of our topic is the one concerning the establishment of a working group for the draft of the European age-appropriate design code. In December 2022, as a matter of fact, a call was launched to identify the members of this group that will have to draft the code by early 2024. The project certainly represents an important step by the EU institutions in the intended and shared direction, as already seen at the international level in the British and US experiences, of the protection of minors' vulnerability in the digital environment, in a context, tough, where the action required concern the diverse factors of vulnerability.

In this respect, the successful reception of the UK Children's Code model could be enlisted in the phenomenon of the circulation of legal models[50] and, therefore, albeit in a future perspective, of legal transplants. Without

47 COM (2012) 196, online on https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0196.

48 COM(2021) 281 final, online on https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281, amending Regulation (EU) No 910/2014.

49 See, https://edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf.

50 Generally, on the phenomenon of the circulation of legal models, see Alan Watson, *Legal transplants: an approach to comparative law* (Edinburgh, 1974); Alan Watson, 'Law and legal change' Camb. L. J. (1978) 38, 313.; Alan Watson, 'TwoTier Law, an approach to law making' Int. & Comp. L. Q. (1978) 552; Alan Watson, 'Legal change: sources of law and legal culture' Un. Of Pennsylvania L. Rev. (1983) 131, 1121. With some criticisms on Watson theory, see Otto Kahn-Freund 'Book Review, Legal Transplants' L.Q.R. (1975) 91, 292; William Twining, 'Diffusion of law: a global perspective' Journal of Legal Pluralism (2004) 49, 1, 34, 35; William Twining, 'General jurisprudence: understanding law from a global perspective' (Cambridge University Press London 2009); Pier Giuseppe Monateri, *The 'Weak Law': Contaminations and Legal Cultures (Borrowing of Legal and Political Forms)*, 2008, available on line at the Alan Watson Foundation website: <www.alanwatson.org> accessed September 2023.

claiming to delve into such a far-reaching topic, we simply observe that, as in the case of other phenomena, for example in the environmental matters[51], also for the issue of children's vulnerabilities in the digital environment, and so in the case of the smart toys, the acquisition of already established models could facilitate the achievement of reform goals.

Moreover, as proven by the data on the market growth in the sector, smart toys have already conquered a significant share in the economy with a global dimension. Therefore, we can easily recognize that this is a mutual and shared matter, that appear common in the globalized world, and not, instead, strictly linked to a particular cultural, social or legal background.

A further confirmation in this regard also comes from the General Comment n. 25 of 2021 by the Committee[52] on the Rights of the Child, devoted precisely to the protection of the child in the digital environment[53].

On legal formants and circulation of models, see again Rodolfo Sacco, 'Legal Formants: A Dynamic Approach to Comparative Law' The American Journal of Comparative Law (1991) I, 39, 1, 34 and II, 343; Rodolfo Sacco, Antonio Gambaro, *Sistemi Giuridici Comparati* (Utet Torino 1996) 4; Rodolfo Sacco, *Introduzione al diritto comparato* (Utet Torino 1992) 43; Rodolfo Sacco, *Circolazione e mutazione dei modelli giuridici*, Digesto civ., II, Utet, Torino 365.

For the dialogue between Rodolfo Sacco's and Alan Watson's theories, see Silvia Ferreri, 'Assonanze transoceaniche. Tendenze a confronto' Quadrimestre, rivista di diritto privato (1993) 1, 179; Ugo Mattei, 'Why the wind changed. Intellectual leadership in western law' Am. J. Comp. Law (1994) 42, 195; Alan Watson, 'From legal transplants to legal formants' American Law Journal of Comparative Law (1995) 43, 3, 469; Pier Giuseppe Monateri, 'Black Gaius' Hastings L.J. (2000) 51, 510.

51 On the specific matter of environoment, see Barbara Pozzo, "Modelli notevoli e circolazione dei modelli giuridici tra in campo ambientale: tra imitazione e innovazione" in *Studi in Onore di Antonio Gambaro. Un giurista di successo* (Giappichelli 2017).

52 The Committee is a body of 18 independent experts that monitors the implementation of the U.N. Convention on the Rights of the Child and of the two Optional Protocols to the Convention, by the State parties. In addition to this monitoring work the Committee publishes its interpretations on the content of human rights provisions, known as general comments, on specific matters. In these comments the Committee makes recommendations on thematic issues related to children that the State parties should dedicate more attention to, in terms of legislative and regulatory measures to adopt or improve.

53 See CRC/C/GC/25 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation accessed September 2023. In the matter of the protection of children in the digital environment the literature is very rich. Among the others, see Alessandro Mantelero, 'Children Online and the Future EU Data Protection Framework: Empirical Evidences and Legal Analysis' Int. J. Technology Policy and Law (2016) 2, 169; Lina Jasmontaite, Paul 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

The final text of the Comment is the result of a series of initiatives aimed at investigating the relationships between children's rights and the digital environment in the light of the rights recognized in the U.N. Convention. Specifically, the Committee received inputs in 2019 and in 2020 from State parties, regional organizations, stakeholders and, most importantly, from children[54].

The key elements of this document lie in the method by which it was drafted and the recipients to whom it is addressed. Regarding the method employed, as mentioned above, the comment is made of the observations coming from different actors. The most relevant part comes from the children: from 27 countries and different socioeconomic backgrounds, they are, therefore, the real protagonists, in full accordance with the essence of the rights recognized in the Convention. The concept of participation as one of the instruments for the child to affirm his or her own rights, and

Internet' International Data Privacy Law (2014) 5, 20; Eva Lievens, Valerie Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation', Computer Law & Security Review (2018) 34, 2, 269; Simone van der Hof, 'I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World', Wisconsin International Law Journal (2017) 34 (2) 409; Simone van der Hof, Eva Lievens, 'The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR', Communications Law 23 (2018) https://papers.ssrn.com/abstract=3107660 accessed September 2023; Esther Keymolen, Simone Van der Hof, Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust, Journal of Cyber Policy, (2019) 4:2, 143-159; Francesca Ippolito, '(De)Constructing Children's Vulnerability under European Law' in Protecting Vulnerable Groups, The European Human Rights Framework (Bloomsbury Publishing 2015) 23; Gary T. Marx, Valerie Steeves, 'From the Beginning: Children as Subjects and Agents of Surveillance', (2010) 7(3/4), Surveillance & Society 192; Ellen McGinnis et al., 'Giving Voice to Vulnerable Children: Machine Learning Analysis of Speech Detects Anxiety and Depression in Early Childhood,' (2019) IEEE Journal of Biomedical and Health Informatics, 1; Louise Holly, 'Health in the Digital Age: Where Do Children's Rights Fit In?', (2020) 22, 2 Health and Human Rights Journal 49; Simone van der Hof et. al., 'The Child's Right to Protection against Economic Exploitation in the Digital World', (2020) 28 International Journal of Children's Rights 833; Simone Van der Hof, *Children and data protection from the perspective of children's rights - Some difficult dilemmas under the General Data Protection Regulation* (Wolters Kluwer: Belgium 2018).

54 See, Amanda Third, Lily Moody, *Our rights in the digital world: A report on the children's consultations to inform UNCRC General Comment 25*, 2021 (London and Sydney: 5Rights Foundation and Western Sydney University) <https://5rightsfoundation.com/uploads/OurRIghtsinaDigitalWorld-FullReport.pdf> accessed September 2023.

as a duty for the other actors (states, businesses) to fully comply with the obligations of the U.N. Convention, is indeed at the base of the new concept of the child the Convention is expression of: an active subject with rights (and duties), and not a mere object of someone else's decisions and choices.

This approach moreover might reduce the risk of pathogenic vulnerabilities and ineffective institutional responses.

The recipients identified are the States parties but, also, parents and caregivers, civil society such as organizations working in the field of children's rights and in the field of the digital environment, and businesses. All the actors are required to meet a series of obligations not only to protect children from any potential harm in the digital environment, but also to *prevent* those harms through monitoring activities and child-rights impact assessments. This is possible due to the intrinsic strength and yet innovative side of the U.N. Convention, which is to *foresee* the protection of children also by private actors.

Regarding specifically the topic of vulnerability, recalling what we have established through the taxonomy we proposed, we can easily recognize that, if adequately addressed and acknowledged (also) in advance, situational or occurrent vulnerabilities can be avoided or limited. In this respect, therefore, the participation element plays a crucial role[55].

Another response, even if a different level, can be found also in the recent initiative of the *supported decision-making* (SDM) agreement[56], an instrument that puts the individuals' needs at the center, without depriving the subjects of their agency but, at the same time, assisting them in their choices. In the last few years this instrument has gained increasing attention in the public debate in the United States, in particular after the landmark

55 For the matter of participation related to vulnerable persons in the decision-making process, see Latifa Jackson et al., 'Including Vulnerable Populations in the Assessment of Data From Vulnerable Populations' Frontiers in Big Data 2 (June 28, 2019): 7 <https://doi.org/10.3389/fdata.2019.00019> accessed September 2023.

56 The *supported decision-making* (SDM) agreement allows people with disabilities to retain their decision- making capacity by choosing trusted advisors, such as friends, family members, or professionals, to serve as supporters in every day life's choosing. For a brief and practical overview see, https://www.aclu.org/wp-content/uploads/legal-documents/faq_about_supported_decision_making.pdf accessed September 2023; among scholarly writing see, Karrie A. Shogren, Michael L. Wehmeyer, Jonhathan Martinis, Peter Blanck, *Supported Decision-Making: Theory, Research, and Practice to Enhance Self-Determination and Quality of Life* (Cambridge University Press 2018).

decision in *Ross and Ross v. Hatch*, that reaffirmed an individual's right to choose how to live with the support needed in the community[57].

The declared aim of SDM, indeed, is to empower people to make their own decisions, to the maximum extent possible, to increase their self-determination. Mostly, SDM is seen as a valuable alternative to the traditional overly restrictive instruments of guardianships or substitute decision making regimes, to which usually certain categories of people (for example mentally or cognitive disabled people or older adults) have been relegated to by the law so far[58].

The key element of SDM is, therefore, the protection of the person at her highest expression, namely, self-determination which is what leads people to live *meaningfully* their life in a certain community. And it is exactly in this perspective that we see the connection with vulnerability and, in particular, with the case of children's vulnerability and the use of smart toys.

F. Ways forward and conclusions

What we have tried to do in these pages is to explore how the concept of vulnerability could be declined in the specific situation of children playing with smart toys and what coordinates – if any – we could identify to avoid or, at least, limit that situation of vulnerability. The risks and the threats that we acknowledged led our analysis to look for the reasons behind those risks but, mainly, for the responses that legal systems and institutions have already given or, possibly, could still give.

One fundamental element that is critical to underline is that the answers we considered, namely the UK and the California Age-Appropriate Design Codes, as well as the EU initiatives together with the *supported decision-making agreement*, are not pathogenic responses. According to what Goodin says, as a matter of fact in this specific case, these are all *pro-active*

57 *Ross and Ross v. Hatch*, Case No. CWF-120000426 (Circuit Court of Newport News, 2013). Some of the material can also be found at <https://jennyhatchjusticeproject.org/justice-project/trial-information/> accessed September 2023.

58 See Anna Arstein-Kerslake, 'An empowering dependency: Exploring support for the exercise of legal capacity' (2016) 18(1) Scandinavian Journal of Disability Research 77; Anna Arstein-Kerslake, Michelle Browning, Joanne Watson, Jonathan Martinis, Peter Blanck, 'Future directions in supported decision making' (2017) 37(1) Disability Studies Quarterly; Peter Blanck, *eQuality: The struggle for web accessibility by persons with cognitive disabilities* (Cambridge University Press 2014).

proposals that, implicitly or explicitly, recognize the necessity to distinguish the actual or potential situations of vulnerability and try to fill in the gaps, practically (establishing the set of standards in the codes and with the support of the community in the SDM).

It is true that there are still many Caylas and i-Que Robots on the global market, also because e-platforms make it possible to sell repeatedly world widely even products not 'officially' on the market anymore.

At the same time, tough, there is also Roybi Robot, the 2021 winner of the Smart Companion category in the Smart Toy Awards, the event organized by the World Economic Forum in collaboration with UNICEF and its AI for children project[59], together with some companies such as PWC, Dell tech and the University of Berkley. The aim of this event was to find the most promising smart toys for children that promoted safe, trustworthy, ethical, and responsible use of AI. The idea is to encourage the use of technology to increase and improve the enormous potential and opportunity in education that these tools could bring with them.

Roybi represents precisely the example of how smart toys can actually be a source of safe learning, safe design and conscious use for the children. Indeed, beyond providing kids with a private tutoring experience that uses Artificial Intelligence, Roybi Robot introduces them to technology, math, science, and multiple languages**.** This smart toy explicitly refers to age-appropriate design features, is considered 'child-friendly A.I.' and indeed provides educational content[60]. Finally, Roybi's award is the result of the evaluation of experts and children: this confirms, once again, that participation and, mostly, participation by the subjects who should be the final user (potentially, at least, vulnerable users) is essential.

In this respect our analysis pointed out that the vulnerability condition of children in the digital environment, when using smart toys, needs to be declined taking into consideration: the taxonomy we described regarding the inherent/situational and dispositional/occurrent distinction and the

59 The Office of Global Insight and Policy is leading a two-year project to better understand how Artificial Intelligence (AI) systems can protect, provide for, and empower children<https://www.unicef.org/globalinsight/featured-projects/ai-children> accessed September 2023. UNICEF worked together with the Government of Finland, and collaborated with the IEEE Standards Association, the Berkman Klein Centre for Internet & Society, the World Economic Forum, the 5Rights Foundation and other organizations.

60 About the innovative features of this smart toy, see <https://roybirobot.com> accessed September 2023.

principles of the Convention on the rights of the child, namely the best interest and the evolving capacities of the child.

In this perspective, the result we get is in accordance with the very essence of childhood itself: being in progress, *in fieri*. This is the reason why we chose to employ that specific type of taxonomy on vulnerability together with the intersectionality approach. As we argued at the beginning that the ultimate goal must always be the promotion and the protection of the human dignity, the case of smart toys showed how easy it is to deviate from this goal, if all the actors involved do not pay enough attention and do not commit to this aim[61]. The risk is that what Rodotà[62] called "corpo elettronico" - that is all the information that make our identity - could not be reunited with the "corpo fisico". This is, instead, where the value of dignity becomes *the* critical element: it avoids that the person becomes just a source for profiling, selling data or an object of surveillance.

Institutions and civil society, then, have a precise responsibility towards the rest of the community in guaranteeing that this will not happen and to put in place actions that actually empower people, reducing or eliminating their vulnerability, not simply eliminating the problem, as in the case of Cayla and i-Que, that were just removed from the market.

As the case of smart toys have clearly demonstrated, the empowerment of children not only is possible but could represent a valid and appropriate

61 On the matter of responsibility, and in particular on the necessity for the institutions of taking a straightforward position, particularly interesting is the testimony that Prof. Woodrow Hartzog, from Boston University School of Law, gave on September 12, 2023 during the hearing, before the US Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, on "Oversight on A.I.: Legislating on Artificial Intelligence". Prof. Hartzog stressed the point that the policy-approaches of the last few years, tough significant, are not enough. He then stated that "To bring AI within the rule of law, lawmakers must go beyond half measures to ensure that AI systems and the actors that deploy them are worthy of our trust". He also underlined that "trust and relational vulnerability are the critical lenses through which to view issues of privacy, data protection, and civil rights in the digital age". The text of the testimony is available at <https://www.judiciary.senate.gov/imo/media/doc/2023-09-12_pm_-_testimony_-_hartzog.pdf> accessed September 2023. See, also, Solon Barocas, Andrew Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671; Andrew Selbst, Solon Barocas, 'Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law' (2023) 171 University of Pennsylvania Law Review 1023; Woodrow Hartzog, *Privacy's blueprint the battle to control the design of new technologies* (Harvard University Press 2018); Woodrow Hartzog, 'Unfair and Deceptive Robots' (2015) 74 Mar. L. Rev. 785.

62 See Stefano Rodotà, *Il Diritto di avere diritti* (Laterza 2016), 197.

suggestion to limit their vulnerability. Making the children more digitally literate[63] - their selves or through the intervention of their parents or guardians or agreed supervisor, in the case of the supported decision-making agreement - much more aware of their rights and, finally, realize what should always be the ultimate goal: pursuing their best interest.

63 See, also, the initiatives recently taken by the Italian data protection authority that aim at protecting minors online through an intense activity of dissemination about the digital environment. Particularly relevant the last publication by one of the members of the Authority, Agostino Ghiglia, of the book entitled *Educazione Civica Digitale* (Roma, 2023). More generally, on the commitment of the Authority, see <https://www.garanteprivacy.it/temi/minori> accessed September 2023.