CERTAIN LEGAL ASPECTS OF CHILDREN'S RIGHT TO PROTECT PERSONAL DATA IN THE CONTEXT OF AI UNDER THE EUROPEAN UNION DATA PROTECTION LAWS

Kamrul Faisal

Abstract

The European Union (EU) legal system provides children with the fundamental right to have their data protected within the ambit of its data protection laws. Article 8 of the Charter of the Fundamental Rights of the EU provides the right for everyone's personal data to be protected, including children. Similarly, Council of Europe (CoE) Convention 108 protects anyone's data in both automatic and non-automatic processing environments.

Children are the most active online user group. Therefore, the protection of children's data is necessary to protect them from related risks and harms. The rationale for providing special protection is that they are less aware of the risks, consequences, safeguards, and rights. The typologies of privacy harms highlight that data subjects lose control over their data in all incidents of personal data compromise. The phenomenon could lead to physical, economic, reputational, psychological, and autonomic harms, breaches of professional secrecy, other social disadvantages, and material and non-material damage such as discrimination, identity theft, fraud, etc. The risks of harm are greater in the artificial intelligence (AI) context. Virtual reality technologies used for gaming purposes, advertising technologies such as Adtech technologies, various Internet of Things (IoT) technologies embedded in smart toys, deploying analytics to derive results from their data, pushing personalised content, etc. are some examples of AI deployment which can process children's data unlawfully online. Therefore, protecting children from unlawful use of their data online in the AI context is obligatory.

Analysing the EU data protection laws in the AI context unfolds certain legal aspects such as default processing situations, the best interests of children, processing based on children's consent and contract, processing based on the transparency principle, automatic decision-making based on children's data and the responsibility of stakeholders to protect children's data. Collectively, they reveal serious shortcomings of law in the area, which may require regulating the area with an exclusive law.

1 Introduction

The European Union (EU) data protection laws provide children with the right to have their data protected. It became a fundamental human right under the EU legal system with the enforcement of the Lisbon Treaty in 2009, as the treaty gave the Charter of the Fundamental Rights of the EU (the Charter) the status of a constitutional treaty within the EU legal system.[1] Consequently, all the rights included in the treaty became directly enforceable throughout the EU.[2] Art. 8 of the Charter provides the right to personal data protection for everyone.[3] When pro-

[1] Kamrul Faisal, *Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective*, vol 28 (Routledge 2023) 68 <https://doi.org/10.1080/10811680.2023.2180266>.

[2] Kamrul Faisal, 'Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions' (2021) 4 Security and Privacy 1, 2 <https://onlinelibrary-wiley-com.libproxy.helsinki.fi/doi/full/10.1002/spy2.157>.

[3] Article 8 of the Charter states:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

cessing[4] the personal data[5] of children, the law requires controller(s)[6] to process such data based on consent or any other lawful basis. Similarly, Council of Europe (CoE) Convention 108 protects everyone's data in both automatic[7] and non-automatic processing environments[8], which often extends across sovereign borders,[9][10] and applies to both public and private sectors.[11] In addition, Art. 8 of the European Convention of Human Rights (ECHR) also protects a natural person's personal data.

Some other national and international important instruments protect children from related privacy harms. To illustrate a few, the United Nations Convention on the Rights of the Child (UNCRC)[12] forbids all types of arbitrary and unlawful interference with children's 'privacy, family, home, correspondence, honour or reputation'.[13] Again, Art. 16(2) UNCRC guarantees that they are entitled to have legal protection against such interferences. The UNCRC further protects children's criminal convictions and offenses data.[14][15] The relevant provisions

---

[4] Article 4(2) GDPR states that processing means any act or set of acts such as collection, storage, erasure, destruction transfer, etc. that is performed on data, or sets of data.

[5] Article 4(1) GDPR outlines personal data as information by which natural persons can be identified directly or indirectly.

[6] According to Article 4(7) GDPR, controller(s) means any natural or legal person, public or private body who jointly or alone determine the purpose(s) of processing personal data.

[7] According to Article 2(c) Convention 108, the term 'automatic processing' refers to certain operations on data that are carried out in fully or partially using automated means, storage of such data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.

[8] Article 2(c), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 1–9.

[9] Preamble, ibid.

[10] Article 1, ibid.

[11] Article 3(1), ibid.

[12] Convention on the Rights of the Child Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49 1989 1.

[13] Article 16, ibid.

[14] Article 40(1), ibid.

[15] Article 40(1) UNCRC states that criminal conviction and offences data include any information related to an alleged, accused of, or convicted information.

urged treating children according to their dignity and human worth through the protection of their rights and freedoms.[16]

The protection of children's data is necessary to protect them from related risks and harms. The most important reason for providing protection is that they are less aware of the risks, consequences, related safeguards, and their rights.[17] The typologies of privacy harms unfold that one thing is common in all cases of personal data compromise – data subjects[18] lose control over their data.[19] It poses a risk to children's right to have their data protected.[20] Such privacy harms could lead to physical, economic, reputational, psychological, and autonomic harms,[21] breach of professional secrecy, other social disadvantages, and material and non-material damage such as discrimination, identity theft, fraud, etc.[22] The risks are greater if children's data including sensitive data such as racial or ethnic origin, political beliefs, religion, genetic data, health, sex life, or criminal convictions) is breached.[23] Putting it differently, if children's sensitive data are breached then it may pose a greater risk to their right to have their data protected.

---

[16] Article 40(1), Convention on the Rights of the Child Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49.

[17] Recital 38, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) 2016 1–119.

[18] Accroding to Article 4(1) GDPR data subject refers to natural persons whose personal data are being processed.

[19] Recital 75, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[20] Recital 75, ibid.

[21] Danielle Keats Citron and Daniel J Solove, 'Privacy Harms' (2022) 102 Boston University Law Review 793, 831.

[22] Recital 75, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[23] Recital 75, ibid.

The risks of harm and actual harm are greater in the artificial intelligence (AI) context. The proposed AI Liability Directive refers to AI as a set of enabling technologies, which can contribute to a wide array of benefits to the economy and society. It is associated with technological progress and fosters the growth of new business models in the digital economy.[24]

2 Background

This paper analyses children's right to have their data protected in the context of AI. The existing knowledge on the rights children have about their data being protected in the AI context reveals that this area is highly under-researched, despite the European Commission (EC) addressing the issues in 2011.[25][26]

Children are one of the most active users of online services.[27] According to the UNICEF Annual Report 2017, one in every three network users are children, which makes them the most connected user group.[28] One-third of the US's TikTok customers are children aged 14 years or younger.[29] Children have a right to maintain social relations and grow themselves to become active members of society.[30] But they

[24] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) 2022 1, 15.

[25] The EC said it might be difficult for the parental generation to carry their responsibilities out, because the new technological products and services that are available to their children is less known to them.

[26] Isabella Ferrari, 'Robots for the Family: Protection of Personal Data and Civil Liability' [2018] International Survey of Family Law 297, 310.

[27] Diana S Skowronski, 'COPPA and Educational Technologies: The Need for Additional Online Privacy Protections for Students' (2022) 38 Georgia State University Law Review 1217 <https://www.who.int/news-room/fact-sheets/detail/autism-spectrum-disorders>; Lisa Archbold and others, 'Adtech and Children's Data Rights' (2021) 44 University of New South Wales Law Journal 857.

[28] Federica Persano, 'GDPR and Children Rights in EU Data Protection Law' [2020] European Journal of Privacy Law & Technologies 32, 33.

[29] Samuel M Roth, 'Data Snatchers: Analyzing TikTok's Collection of Children's Data and Its Compliance with Modern Data Privacy Regulations' (2021) 22 Journal of High Technology Law 1, 5–6.

[30] Persano (n 28) 33.

are influenced easily by advertising. Online games, social media, and related technologies may pose negative impacts on their attitude.[31] Therefore, their data need to be protected from the unfair practices perpetrated by online service providers.[32]

The emergence of modern data privacy did not consider children as an interested party at the beginning.[33] The absence of any relevant provision in the Data Protection Directive (DPD)[34] is evidence of that.[35] However, the new law which repealed the DPD – the GDPR included children's data protection provisions. Children's definitions received dynamic and static apprehensions. From a static viewpoint, it is defined based on age, and the dynamic approach focuses on the growing capacities of children.[36] The CoE and UNCRC consider a child to be anyone under 18 years of age.[37] The GDPR considers anyone under the age of 16 to be a child.[38] US law considers 13 years as the demarcation age for children.[39] Concerning dynamic apprehension, the *Gillick competence test*[40] may aid in determining children's

[31] ibid 34.

[32] Skowronski (n 27) 1217.

[33] Ferrari (n 26) 309.

[34] EU Directive 95/46: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data 1995 31–50.

[35] Dorde Krivokapic and Jelena Adamovic, 'Impact of General Data Protection Regulation on Children's Rights in Digital Environment' [2016] Annals of the Faculty of Law in Belgrade International Edition, 2016 205, 206.

[36] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) 2009 1, 3.

[37] Council of Europe, 'Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment' (2018); Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools).

[38] Gerrit Hornung, 'A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012' (2012) 9 SCRIPTed 64; REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[39] Skowronski (n 27); Simran Saini, 'Permission Not Granted: A Domestic and Global Comparative Analysis on Social Media Policies, Privacy Laws and a Proposal for the United States' (2021) 46 Southern Illinois University Law Journal 189.

[40] It is a test that determines children's maturity level by analysing autonomic

maturity before 16 or 13 years old. The rules concerning defining children based on age depict that the definition of children may vary in different jurisdictions.[41] If someone qualifies to be a child, the person is entitled to a high level[42] and special protection[43]. It applies child-specific provisions of the GDPR.[44] Overall, related legal norms are unclear.[45] The lack of legal norms would fail to protect children from related risks and harms.[46]

Virtual reality technologies used for gaming purposes,[47] advertising technologies such as Adtech,[48] and Adsenses, various Internet

---

level in a given context. It is a matter of medical science.

[41] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps' (2017) 26 Information and Communications Technology Law 146, 153.

[42] Simone van der Hof and Sanne Ouburg, '"We Take Your Word For It" – A Review of Methods of Age Verification and Parental Consent in Digital Services' (2022) 8 European Data Protection Law Review 61; Jennifer Dolan, 'Fundamentals for a Child-Oriented Approach to Data Processing' (2022) 8 European Data Protection Law Review 7.

[43] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR); Giangiacomo Olivi, Niccol Anselmi and Claudio Orlando Miele, 'Virtual Reality: Top Data Protection Issues to Consider' (2020) 3 The Journal of Robotics, Artificial Intelligence & Law 141; A Altavilla and others, 'The Secondary Use of Paediatric Data Under GDPR: Looking for New Safeguards for Research' (2019) 3 European Pharmaceutical Law Review 156; Universal Declaration of Human Rights 1948 1.

[44] Olivi, Anselmi and Miele (n 43); Archbold and others (n 27); REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR); Persano (n 28).

[45] Mary Donnelly and Maeve McDonagh, 'Health Research, Consent and the GDPR Exemption' (2019) 26 European Journal of Health Law 97, 119.

[46] Jason Heitz, 'Federal Legislation Does Not Sufficiently Protect American Data Privacy' (2022) 49 Northern Kentucky Law Review 287, 300–301.

[47] Olivi, Anselmi and Miele (n 43) 145.

[48] Archbold and others (n 27) 857.

of Things[49] (IoT) technologies[50] embedded in smart toys,[51] deploying analytics to derive results from their data,[52] pushing personalised content[53] , etc. are some of examples of AI deployment which can process children's data online unlawfully.[54] Therefore, protecting children from unlawful use of their data online in the AI context is necessary.

Controllers are required to take measures that are necessary to protect children's data.[55] The GDPR ensures that related checks and balances are backed by hefty fines and other enforcement mechanisms.[56] Therefore, researching certain aspects of children's right to have their data protected is imminent.

My aim with this paper is to identify the more important legal aspects of children's right to protect personal data in an AI context. To achieve its aim, a traditional doctrinal approach has been deployed. The idea of deploying the method is to situate it within the legal coherence based on existing knowledge. For this paper, a thematic topic modelling approach to analyse data was deployed. While analysing, I have used a data protection lens in the AI context to analyse findings that are novel in this paper. The results help the academic community the most to build further research on top of it. The ambit of the study is limited to the EU data protection laws.

---

[49] Within the scope of this technology, sensors interact with each other in a networked environment to process data in real time.

[50] Roth (n 29).

[51] Maria Cristina Gaeta, 'Smart Toys and Minors' Protection in the Context of the Internet of Everything' (2020) 2 European Journal of Privacy Law & Technologies 118, 118.

[52] Saini (n 39) 207–208.

[53] ibid.

[54] Lisa Collingwood, 'Villain or Guardian? "The Smart Toy Is Watching You Now … ."' (2021) 30 Information and Communications Technology Law 75, 75 <https://doi.org/10.1080/13600834.2020.1807118>.

[55] REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) 2022 (Official Journal of the European Union) 1.

[56] Faisal (n 1) 96.

In the upcoming sections, section 3 is an analysis of the concept of children. Section 4 presents an outline of certain legal aspects of children's right to personal data protection in AI. Section 5 presents a discussion of the topic, followed by the conclusions.

3 The concept of the child in AI

It is difficult to find a uniform definition of a child or children. According to Article 1 of the UNCRC, a child is someone who is under the age of 18 years, unless the person acquires adulthood before that age.[57] It identifies two viewpoints to define a child: static (age) and dynamic (attainment of maturity).[58]

3.1 Static viewpoint

While focusing on the static viewpoint, Convention 108 states that a child is any human who is under the age of 18 years.[59] According to the Children's Online Privacy Protection Act (COPPA) 1998 in the United States, anyone under 13 years of age is a child.[60] According to the GDPR, anyone below 16 years of age is a child with the discretion provided to the Member States for lowering the limit to 13.[61] The discretion that the GDPR provided to the Member States concerning different age limits of the children affected many Member States' long-standing practices. For example, the GDPR set the age limit to

---

[57] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) 3.

[58] ibid.

[59] Council of Europe (n 37) 12.

[60] Gabe Maldoff and Omer Tene, 'Born in the USA: The GDPR and the Case for Transatlantic Privacy Convergence' (2019) 17 Colorado Technology Law Journal 295, 307.

[61] Article 8, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

13, but the Swedish standard practice concerning age was 15 years.[62] The Swedish authority believed that at the age of 15, children usually understand the content and impacts of personal data processing.[63] It not only varies between countries but also across sectors such as consent for research, consent for advertising, etc.[64] For example, Spain considers 14 years of age, and the Netherlands and Hungary consider 16 years to be the age at which children can grant consent.[65] Children in Finland are self-reliant concerning using Internet services related to their school work without the intervention of their guardians.[66] At the age of 16, they tend to avoid age limits by providing false information.[67] That is why the Finnish government fixed the age at which people are considered to be children at 13 years of age for a range of purposes within the meaning of data protection laws.[68] However, the UK takes a slightly different approach. According to the UK Data Protection Act 1998, natural persons can provide consent if they have an understanding of the meaning of exercising the right.[69] Section 66 of the same law assumes that children of 12 years of age or more have such understanding. However, it is inconsistent with the GDPR's 13 years minimum threshold.

It is apparent from the previous analysis that under the EU data protection laws, anyone aged below 16 years is a child. Nevertheless, due to the flexibility that the GDPR provides, the age limit for children is also fixed at the age of 13. Therefore, it can be said that Member States have a wide margin within which to introduce rules related to children's age between 13 and 16.[70] From the static viewpoint, anyone below the age of 13 or 16 years depending on the jurisdiction, is con-

---

[62] Christine Storr and Pam Storr, 'Sweden: Quantitative (but Qualitative) Changes in Privacy Legislation' (2018) 4 European Data Protection Law Review 97, 100.

[63] ibid 100–101.

[64] Macenaite and Kosta (n 41) 152.

[65] ibid 153.

[66] Päivi Korpisaari, 'Finland: A Brief Overview of the GDPR Implementation' (2019) 5 European Data Protection Law Review 232, 234.

[67] ibid.

[68] ibid.

[69] Macenaite and Kosta (n 41) 154.

[70] Krivokapic and Adamovic (n 35) 219.

sidered to be a child. Then what happens with the unborn? Logically, they lie below the 13- or 16-year thresholds, and at least they would have genetic data.[71] Therefore, one valid question remains: is an unborn child considered to be a natural person under the GDPR? The GDPR does not have any explicit provision about it.[72] The European apex courts do not exclude it is possible to consider the unborn child as a data subject.[73]

The area of protecting an unborn child's data is less regulated.[74] The Member States enjoy a remarkable margin of appreciation concerning the matter.[75] The Committee of Ministers of the Council of Europe provided a non-binding recommendation in 1997 concerning the matter.[76] The recommendation afforded the protection of data protection rights to unborn children by recognising their data as children's data.[77] There is no reason to exclude the unborn from data protection laws if the child is alive, although the interpretations of the Data Protection Directive and the Working Party 29 opinion discarded the idea by limiting the protection to living persons.[78]

Relying on a certain age for offering certain rights and loss of protections is an extremely complex matter.[79] The GDPR seems to follow a static viewpoint to define children.

3.2 Dynamic viewpoint

Naturally, children grow over time. Putting it differently, children are members of a unique group that attains physical and psychological maturity over time.[80] According to the static viewpoint of defining chil-

[71] Karl Pormeister and Lukasz Drozdzowski, 'Protecting the Genetic Data of Unborn Children: A Critical Analysis' (2018) 4 European Data Protection Law Review 53, 64.

[72] Pormeister and Drozdzowski (n 71).

[73] ibid 58.

[74] ibid 64.

[75] ibid.

[76] ibid.

[77] ibid.

[78] ibid.

[79] Macenaite and Kosta (n 41) 151.

[80] Opinion 2/2009 on the protection of children's personal data (General

dren, the required level of maturity is attained by them at the age of 12, 13, 16, or 18. Is there a guarantee that the required level of maturity will grow in children at a certain age fixed by law? Do all children grow equally at a particular age? I do not think so. The law seems to assume that the 13 years old may be more competent, in comparison to children aged 12.9 years. Therefore, it is probably one of the biggest flaws of the static viewpoint, which may be supplemented by the dynamic viewpoint of defining children.

The dynamic viewpoint of defining children defines another term 'mature minors'.[81] Mature minors are entitled to take their own decisions without interference from their parents according to their best interests.[82] The '*Gillick competence test'* may aid in the determination of children's maturity. The test analyses competence level by analysing autonomic level in a given context based on best interests.[83]

Therefore, two major viewpoints are found to define a child:

i. based on age, and
ii. based on maturity.

3.3 Children in AI

There are many examples in the world in which AI is used to abuse children's data. To illustrate a few, the Federal Trade Commission (FTC) in the US found that a website called KidsCom targets children specifically, which ended up collecting children's data in a deceptive and unethical manner.[84] Again, The FTC settled a case with the toy maker VTech to pay USD650,000 for collecting a child's data without their parent's consent.[85] Everything started when a hacker intruded on the VTech-associated app Kid Connect, and VTech failed to provide securi-

Guidelines and the special case of schools) 6.

[81] Mark J Taylor and others, 'When Can the Child Speak for Herself: The Limits of Parental Consent in Data Protection Law for Health Research' (2018) 26 Medical Law Review 369, 372.

[82] ibid.

[83] ibid 370.

[84] Maldoff and Tene (n 60) 307.

[85] Michael L Rustad, 'How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices' (2019) 52 Suffolk University Law Review 227, 251.

ty for those data.[86] On similar grounds, in 2012, FTC settled another case with RockYou for not complying with the COPPA.[87] Moreover, in 2019, the FTC settled a case with contemporary Musical.ly, nowadays known as TikTok.[88] The company failed to take consent from the children's parents while processing their data.[89] Furthermore, TikTok's purposes of collecting data from children do not differ much from the purposes of adults. They provide targeted advertisements, personalised content based on online profiles, deploy analytics, etc. with children's data as well.[90] In addition, the virtual reality (VR)[91] system can know how we move around by analysing our movements and brain waves, it has the potential to infringe data protection laws.[92] The VR techs use sensitive biometric data such as eye-tracking systems, facial recognition systems, fingerprint sensors, voiceprints, different hand geometry, head positioning technologies, etc. to provide a consolidated user experience.[93]

Also, smart toys for children are now equipped with artificial intelligence, which can create an emotional and psychological attachment with children through their interaction capacities.[94] For example, Fisher Price's smart toy (came in the shapes of a bear, monkey, and panda) was able to interact with the children based on smart card themes such as bedtime, break, eating time, today, etc. that a child is supposed to place in front of its nose, and the toy starts communicating according to the theme upon detection.[95] The toy can listen and reply accordingly. Such toys can save their playing behaviour, voice sample, etc., which can be stored outside the scope of the functionality purpos-

---

[86] ibid.

[87] ibid.

[88] Anna Wright Fiero and Elena Beier, 'New Global Developments in Data Protection and Privacy Regulations: Comparative Analysis of European Union, United States, and Russian Legislation' (2022) 58 Stanford Journal of International Law 151, 167.

[89] ibid.

[90] Saini (n 39) 207–208.

[91] According to Olivi et.al.(2020), virtual reality (VR) is a computer-generated environment which is experienced by a user of through a user interface.

[92] Olivi, Anselmi and Miele (n 43) 141.

[93] ibid 142.

[94] Gaeta (n 51) 118.

[95] ibid 125.

es of the toy.[96] These toys are robots connected to the Internet and other IoT, which process children's data with associated risks.[97]

The above-mentioned examples depict that AI can cause harm to children from several data protection perspectives. Within the scope of unethical and deceptive data collection practices, AI-based websites can target children to collect their interests, steal their identities, track their locations, etc. by default. They may process children's data for targeted advertisements, personalised content, and other analytics purposes in a carte-blanch manner without their or their parent's consent, which is unlawful. Moreover, controllers may further fail to provide security for the collected data. Finally, they may process children's sensitive biometric data such as iris scans, voice samples, fingerprints, facial recognition, etc. as well as data concerning their gender, religious views, etc. Such data are categorised as sensitive data and protected especially under Art. 9 GDPR.

Overall, the rapid development of AI-related technologies warrants protecting children from unlawful processing of their data.[98]

4 Certain legal aspects of children's right to personal data protection in AI

According to the EU Charter of Fundamental Rights, children have the right to the protection and care which is necessary for their well-being.[99] Art. 8 of the Charter states:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

…

[96] Collingwood (n 54) 86.

[97] Gaeta (n 51) 118.

[98] Roth (n 29).

[99] Article 24(1), Charter of Fundamental Rights of the European Union 2000 (Official Journal of the European Communities) 1–22.

The law provides the rights to privacy and personal data protection respectively to anyone including children.[100] While processing the personal data of the children, controllers must do so based on consent, or any other lawful basis.

Generally, the GDPR regulates legal norms by default as the most comprehensive law in the area of personal data protection.[101] A child has all the data protection rights that an adult has[102] outlined in Chapter 3 of the GDPR such as the right to access, rectification, erasure, restriction of processing, object, right not to be subjected to automatic decision-making, etc. In addition, Controllers are generally responsible for respecting all provisions of the GDPR.[103]

Apart from default requirements, the GDPR has specific requirements to be met for processing children's data. First, while processing a child's data, the GDPR requires the processing to be conducted according to the transparency principle.[104] Then, the children can never be a subject of a decision made by automatic processing of their data.[105] Finally, the GDPR vests the responsibility to the Member States, controllers, supervisory authorities, EDPB, and the EC to develop and enforce legal matters concerning children's data protection.

Nevertheless, the GDPR outlines certain derogations for the processing of personal data. These include processing in line with freedom of expression and information (includes journalistic, literary, academic, and artistic expression purposes), legal compliance, public interest, under official authority, archiving in the public, scientific, historical research, statistical

---

[100] Council of Europe (n 37) 12–22.

[101] Recital 38, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[102] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) 3.

[103] Article 24(1), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[104] ibid.

[105] Recital 71, ibid.

purposes, and for the establishment of legal claims, etc. This may entitle the holder to process personal data if any of these applies.[106]

4.1 Default processing conditions for processing children's data

Under default conditions of processing personal data, as per minimum requirements, controllers must apply all the data processing principles outlined in Art. 5 GDPR (lawful, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality), and rely on at least one of the lawful processing grounds outlined in Article 6 of the GDPR. The grounds are outlined as processing is:

- based on the consent of the data subject (Art. 6(1)(a))
- based on a contract in which the data subject is a party (Art. 6(1)(b))
- necessary on behalf of controller(s) for compliance with a legal obligation (Art. 6(1)(c))
- necessary for protecting the vital interests of data subjects, or of another natural person (Art. 6(1)(d))
- necessary for a task carried out in the public interest, or exercise of official authority vested in the controller (Art. 6(1)(e))
- necessary for legitimate interests of the controller(s), or by a third party. In such a situation, the data subject's data protection interests must not override the controllers' or third parties' legitimate interests. This is exactly the case when controllers process children's data. (Art. 6(1)(f))

Children's data may be processed based on consent, contract, or legal obligation vested on the controller(s), to protect the vital interests of the children, for carrying out any task in the public interest, and in situations when controllers pursue their legitimate interests. It is to be noted that when controllers rely on legitimate interests, controllers' processing interests must outweigh children's privacy interests. Otherwise, it would be impossible to rely on it. The GDPR specifies in the context of children that their data protection interests override the controller's legitimate interests. Therefore, the logical interpretation would be that

[106] Recital 65, ibid.

controllers cannot pursue their legitimate interests when processing children's data. In the 'online environment',[107] the service recipients, service providers, and persons affected by unlawful/ illegal content[108] pursue different legitimate interests.[109] For example, the service recipients have the right to protect their freedom of expression and information, the right to respect private and family life, the right to protect personal data, the right to non-discrimination, etc.[110] In addition, the service providers have the right to conduct business and draw up relevant contracts, etc. The affected persons have the right to human dignity, children have their rights online, the right to intellectual property, etc.[111]

Eventually, to process children's data they must rely on other lawful grounds. Ostensibly, certain grounds of processing e.g., while complying with legal obligations, protecting the vital interests of children, or processing children's data for public interests do not instantly lead to complications. One good reason is that these processing grounds may have the potential to consider children's best interests. Consent and contract grounds could also be considered in the same line. But the underlying conditions might create complications. They require action from or on behalf of children. It is even more important when controllers process special categories of personal data. While processing children's special categories of personal data or sensitive data, controllers must rely on the explicit consent of data subjects.[112] Now, one logical inquiry concerning the complication would be whether children are competent to give consent or get involved in contracts.

---

[107] According to the Council of Europe (2018), the online or digital environment refers to the ICTs including the technological devices such as the mobiles in the networked environment, related technological products and services, and contents.

[108] Recital 12 of the Digital Services Act provides the term 'illegal contents' a broad definition to cover many acts of dissemination within its scope. The dissemination of child's pictures concerning children's sexual abuse, sharing of other's private photos non-consensually etc. comprise illegal contents.

[109] Recital 52, REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[110] Recital 52, ibid.

[111] Recital 52, ibid.

[112] Olivi, Anselmi and Miele (n 43) 142.

4.2 Protecting children's best interests

No standard definition of children's 'best interests' can be found. The UNCRC states the best interests of children must be considered when public and private authorities perform any act concerning children.[113] According to the EU Charter of Fundamental Rights, children have the right to the protection and care which is necessary for their well-being.[114] In my opinion, the term 'best interests' refers to those interests of children of which preservation makes the online environment a safe, predictable, and trustworthy place[115] for the children when they are in a vulnerable position[116]. For example, by protecting against the unlawful use of children's data, children's privacy interests are protected. Again, under COPPA, providing incentives such as prizes, etc. to children as a lure to provide more personal information is against children's best interests.[117]

It ensures children's well-being online. Protecting children's best interests is one of the more important principles EU data protection laws rely on for protecting their data.[118]

The law protects children's best interests while processing their data. The present paradigm of children's data protection rights suggests that collecting and processing children's data require controllers to deploy additional resources to protect their rights, development, health, and other well-being connected with their best interests.[119] Chil-

---

[113] Charter of Fundamental Rights of the European Union; REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act); Convention on the Rights of the Child Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49.

[114] Article 24(1), Charter of Fundamental Rights of the European Union.

[115] Recital 12, REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[116] Altavilla and others (n 43) 157.

[117] Heitz (n 46) 294.

[118] Altavilla and others (n 43); Council of Europe (n 37); Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools).

[119] Dolan (n 42).

dren's growing capacity is connected with serving their best interests. Growing capacity refers to their physical and psychological capacity which they attain with time.[120] It is a legal notion of identifying their maturity. In cases in which children did not attain sufficient maturity, parents can take decisions on their behalf to serve their best interests. When parents' and children's interests conflict, children's best interests may prevail,[121] though the courts or the Data Protection Authorities (DPA) should decide such cases.[122] Concerning data protection, parents are the legal representatives of the child, and they must act in the best interests of their children.[123] On the other hand, mature minors are entitled to take their own decisions without interference from their parents according to the principle of the child's best interests.[124]

4.3 Processing children's data based on consent

According to UNICEF, free and informed 'consent'[125] is the best lawful ground for processing children's data.[126] Many allege that the EU adopted laws concerning the protection of children's data from the US COPPA, as the parental consent provisions outlined by the GDPR are identical to those in the COPPA.[127] In the EU, consent is one of the lawful grounds for processing personal data recognised in the Charter and other statutes.[128]

---

[120] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) 6.

[121] Anna Maria Iskül and Kristi Joamets, 'Child Right to Privacy and Social Media – Personal Information Oversharing Parents' (2021) 14 Baltic Journal of Law and Politics 101, 116.

[122] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) 4.

[123] Iskül and Joamets (n 121) 101.

[124] Taylor and others (n 81) 372.

[125] According to Art. 4(11) GDPR, consent refers to any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

[126] Dana Volosevici, 'Child Protection under GDPR' (2019) VI LXX) A Journal of Social and Legal 17, 22.

[127] Maldoff and Tene (n 60) 308.

[128] Macenaite and Kosta (n 41) 156.

The GDPR outlines certain conditions that need to be met if controller(s) would seek to rely on their consent. The consent of a child will be lawful only when controllers offer 'information society services' to a child, and the child is aged 16 years or above.[129] The phrase 'information society service' refers to any service that is given for remuneration at a distance, by electronic means, and at the individual request of the service recipient.[130] Three elements comprise information society service: at a distance, by electronic means, and at individual request. 'At a distance' refers to the phenomenon when the parties in the service are not present simultaneously.[131] 'By electronic means' refers that the service being sent and received using electronic means such as by wire, radio, optical, or any other electromagnetic means.[132] 'At the individual request' of the service recipient means the service provided is based on an individual request.[133] For this paper, information society service must be understood as all those services that are provided at a distance using communication networks at the request of children.

For those below 16 years of age, the services can be offered only if consent is provided by the parental authority over the child.[134] The Member States may lower the age threshold to 13, but not below that.[135] It is the responsibility of the controller(s) to make all reasonable efforts using available technology to verify whether consent is given by a child aged 13, 16, or older (depending on a Member State's law), or

---

[129] Article 8(1), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[130] Article 1(2), DIRECTIVE 98/48/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations 1998 (Official Journal of the European Communities) 18.

[131] Article 1(2), ibid.

[132] Article 1(2), ibid.

[133] Article 1(2), ibid.

[134] Article 8(1), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[135] Article 8(1), ibid.

the parental authority over the child.[136] Anyone who provided consent for processing must be empowered to revoke the same at any time.[137]

According to Article 29 Working Party, consent must be an indication of the wishes of the data subjects, freely given, specific, and informed.[138] The term 'freely given' can be analysed from the real choice principle when the consent provider has an option. The Swedish DPA imposed an administrative fine of SEK 200,000 (approximately EUR 20,000) on the Secondary Education Board of Skellefteå municipality for not relying on consent or any other data general processing derogations properly. They deployed facial recognition technology (FRT) via a camera in a school in northern Sweden[139] to check the attendance of students.[140] The DPA said that this act violated multiple provisions of the GDPR.[141] In addition, privacy literacy has something to do with freely given consent. Very low privacy literacy may lead to unsustainable consent propositions.[142]

For consent in information society services, one of the biggest practical problems is to determine whether the user is a child or not[143] and/or whether consent is collected from the child or parental authority.[144] Therefore, it requires dealing with several legal issues proactively.[145] One study depicts that digital services targeted at children do not meet their obligations concerning age verification and parental consent, despite deploying new methods of verification.[146] Different

---

[136] ibid; Council of Europe (n 37).

[137] Council of Europe (n 37) para 34.

[138] Macenaite and Kosta (n 41) 156.

[139] European Data Protection Board (EDPB), 'Facial Recognition in School Renders Sweden's First GDPR Fine' (2019) <https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv> accessed 6 April 2023.

[140] Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students (2019) 1 1, 2.

[141] ibid.

[142] Olivi, Anselmi and Miele (n 43) 141.

[143] ibid 145.

[144] Olivi, Anselmi and Miele (n 43); Hof and Ouburg (n 42).

[145] Olivi, Anselmi and Miele (n 43) 145.

[146] Hof and Ouburg (n 42) 71.

age verification and parental consent methods are found in different case studies. They include self-declaration, entering the date of birth, linking the child's account with that of the parents, date of birth along with photographs, images of a school ID or pass, short videos with spoken random words, restriction of services, asking for additional information in case of suspicion, and reporting possibilities.[147] Sometimes parental authority is sought by apps by default, etc.[148] To regulate the area more efficiently, more empirical research is needed involving parents, children, and policymakers.[149] For now, the Member States, supervisory authorities (SAs), the Board, and the European Commission will encourage controllers to draw up a code of conduct that ensures the application of the GDPR appropriately.[150] The initiation of a code of conduct comprises *inter alia* how the required information is provided, protection is provided, and of obtaining consent from children or parental authority.[151]

4.4 Processing children's data based on contract

Relying on a contract for processing personal data is one of the lawful bases outlined by the GDPR. In a contract, there are usually two parties between whom it is executed. The rules related to consent do not affect the provisions of contract laws of the Member States.[152] While exercising their right to business, the information society service providers have legitimate interests to initiate contracts.[153] But do children have the legal competence or capacity to enter into contracts with control-

[147] ibid 66–67.

[148] ibid 68.

[149] Macenaite and Kosta (n 41) 196.

[150] Article 40(1), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[151] Article 40(2)(g), ibid.

[152] Article 8(3), ibid.

[153] Recital 52, REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

ler(s)? Certainly not. By competence, I mean whether they understand the risks involved in providing consent to process their data in a particular context. Again, by capacity, I refer to whether they have reached a certain age threshold that enables them to enter into contracts freely. These questions and related aspects pose significant complications in settling legal norms, which require further research.

4.5 Transparent processing behavior

To provide children with specific protection, the GDPR stresses processing their data according to the transparency principle.[154] The principles require controllers to

i. communicate certain information to the children, and
ii. communicate the information in concise, easily accessible, and easy-to-understand forms.

What information do they communicate? Information concerning the collection of data, data protection rights[155], and any possible data breach notifications.[156] It is the responsibility of the controller(s) to provide certain information when the data are or are not directly collected from children.[157] The information includes the identity and contact details of the controller, the contact details of the data protection officer, the purpose and legal basis of processing, the legitimate interests pursued by controllers, the recipients of the data, whether or not the controller intends to transfer the data to a third country, or international organisation along with the existence or absence of adequacy decision from the European Commission (EC), appropriate safeguards,

---

[154] Recital 58, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[155] Article 8, Convention 108+ Convention for the protection of individuals with regard to the processing of personal data 2018 (European treaty series) 1.

[156] Article 12, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[157] Article 12, ibid.

ways of obtaining a copy, or otherwise making them available. In addition, the controllers would inform about the duration of storing the data along with the determination standard, the existence of data protection rights[158], the possibility of withdrawing consent, the right to file a complaint with the concerned supervisory authority, the possible existence of automatic decision making based on profiling, all the initial and subsequent data processing purposes.[159] Furthermore, the controllers must inform the children of any possibility of high risk to their data protection right in the event of a personal data breach under Art. 34 GDPR.[160] While doing so, they are required to inform about the nature of the data breach.[161] However, it is to be noted that the obligation to notify a breach only arises if it may result in a high risk to children's rights and freedoms.[162]

The transparency principle further requires controllers to communicate in plain and easy language to the children so that they understand who and for what purposes their data are being collected. Only then it may qualify as transparent processing concerning children. For this, clear, plain language (child-friendly[163]) and visualisation (if appropriate) tools may be used.[164] As per another legal rule, everything can be used in electronic form that can be integrated into websites.[165] Child-friendly formats are difficult to find. Controllers need to find suitable approaches that may involve comics, cartoons, pictographs, animations, or something else that is suitable for them.[166] Children

---

[158] Article 15–22, ibid.

[159] ibid.

[160] Article 12, ibid.

[161] Article 34(2), ibid.

[162] Article 34(2), ibid.

[163] Convention 108+ Convention for the protection of individuals with regard to the processing of personal data para 68.

[164] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[165] Recital 58, ibid.

[166] Eva Lievens, 'Dutch DPA Fines TikTok for Not Offering Understandable Information to Children' (2021) 7 European Data Protection Law Review 423, 428.

aged 9–12 years, particularly like interactive things like mind-maps, games, quizzes, vlogs, animations, etc. through which to be communicated with.[167] Moreover, we can look into the business models of giant companies such as TikTok. This controller received huge business success with its diversified contents which include dances, lip-syncs, comedy shorts, etc.[168] Therefore, they can be used to communicate with the children. Anything that is associated with the things they do and knows works better in communicating with them.

4.6 Automatic decision-making based on children's data

Processing children's data for 'automatic decision-making'[169] purposes based on their online profiles is incoherent with their best interests and the special protection[170] that the EU data protection laws seek to provide. Targeting advertising for children is more profitable than that aimed at adults as they have a limited understanding of the differences between content and advertisements.[171] While providing targeted advertisements, the marketers may process children's location, behaviour, interests, emotions, etc. in a pervasive manner.[172] That is why it is important to know the law that applies in the area.

While expressing their concerns – the UNCRC, the Charter and many national constitutions state that profiling-based advertisements

---

[167] ibid.

[168] Roth (n 29) 2.

[169] Recital 71 GDPR states that automatic processing of personal data is a mechanism which analyse personal aspects of natural persons such as health situation, interests, preferences, behavior, location, movement etc. based on someone's profile to take certain decisions about them without human interventions.

[170] Dolan (n 42) 13.

[171] Aleksandra Popova, 'The Fine Line between Identifiers Capable of Identifying and Identifiable Information' (2018) 24 Suffolk Journal of Trial & Appellate Advocacy 255, 267.

[172] Eva Lievens, 'Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights' (2021) 39 Nordic Journal of Human Rights 128, 128 <https://doi.org/10.1080/18918131.2021.1992951>.

manipulate children unlawfully.[173] The CoE also recommends prohibiting online profiling of children completely.[174] Generally, processing children's data for automatic decision-making purposes is banned, though EU laws may allow such a thing in a limited manner.[175] Under exceptional circumstances, processing for automatic decision-making might be allowed. In such cases, the GDPR requires controllers to comply with notice obligations, enforce children's data protection rights, perform data protection impact assessment (DPIA) mandatorily[176], maintain a code of conduct,[177] etc. The newly enacted EU Digital Services Act (DSA) also generally bans advertising based on profiling children.[178] While favouring controllers' advertise-based business models[179], the online services providers should not advertise to the children based on profiling using their data.[180] To make it happen, they should take the necessary steps to determine the age of the users.[181] Collecting age is not an option for that.[182] In addition, large service providers should provide the targeting and delivering criteria to minors.[183] The new rules are not without loopholes. It neither specifies those exceptional grounds when processing children's data for the automatic decision-making that might be lawful nor provides a unified way to identify children's age. Therefore, the EC and the EDPB should outline the standards of targeted measures online.[184]

In my opinion, controllers should not make the children subject to automatic decision-making by processing their data. However, contemporary practice by the controllers suggests quite the opposite. Many

---

[173] ibid.

[174] Council of Europe (n 37) para 37.

[175] Hornung (n 38) 75.

[176] ibid 77.

[177] Recital 104, REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[178] Article 28(2), ibid.

[179] Recital 79, ibid.

[180] Recital 71, ibid.

[181] Recital 71, ibid.

[182] Recital 71, ibid.

[183] Recital 95, ibid.

[184] Article 44(1)(j), ibid.

companies operate through default businesses using a corporate surveillance model,[185] which is not a standard practice. But do advertising companies have mechanisms deployed to filter children out and make automatic profiling systems disapplied? I doubt it. In *re Nickelodeon Customer Privacy Litigation* case, the plaintiff's children (younger than 13 years old) sued Viacom and Google for collecting the data that included their internet browsing habits unlawfully and selling them for targeted advertisements based on those data.[186]

4.7 Responsibility of the enforcers to protect children's data

In different GDPR provisions, the EU Member States, supervisory authorities, individuals, controllers, processors, third-party watchdogs, the European Data Protection Board, and domestic courts are identified as the enforcers of the GDPR. Each enforcer has a different role in the duties and responsibilities spectrum. Some outline the laws and related rules, some interpret, some exercise rights, and some ensure compliance. The GDPR introduces certain ex-ante and ex-post enforcement mechanisms. To illustrate a few ex-ante mechanisms – data protection by default and by default, prior consultation with supervisory authorities, a record of processing activities, designation of data protection officers, requirements of data protection impact assessments, etc. In addition, some examples of ex-post enforcement mechanisms are – administrative fines, definitive or permanent bans on processing, suspension of automatic exchange of information, auditing, breach notifications, the right to be forgotten[187], etc.

---

[185] Simone van der Hof, 'I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2016) 34 Wisconsin International Law Journal 409, 444.

[186] Popova (n 171) 266.

[187] Recital 65, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

Being the classical enforcement authorities, supervisory authorities have investigative, corrective, and advisory powers.[188] They must promote public awareness concerning the risks, rules, safeguards, and rights related to personal data processing with special reference to children.[189] In addition, they are responsible for promoting public awareness of their powers and functions, rights of data subjects and exercise of those rights, and awareness of controllers and processors about their responsibilities.[190] But what are the specific acts they are required to perform to attain specific objectives? Do they have the tools and resources to make the public aware of those matters? Providing special protection may require attaining special competence by the SAs. To be able to identify relevant aspects, further research is necessary. For now, to situate with the legal coherence concerning such matters, the GDPR suggests turning to the CoE Convention 108 to look for guidance.[191]

In all, the EU data protection laws do not incorporate an exclusive data protection instrument that protects children's right to have their data protected. Within the scope of different laws (such as the Charter, the UNCRC, the CoE Convention 108 and its updated version, the GDPR, the Digital Services Act, the proposed AI Liability Directive, etc.), the legal norms concerning the matter may appear chaotic. Though children receive special high-level protection of their data, the EU legal system does not have a special law to ensure it. Collectively, they reveal certain legal aspects that require further research to under the area better in the context of AI.

Concerning AI aspects, the GDPR does not regulate AI-related aspects directly. It does not contain the phrase 'artificial intelligence' (AI) a single time. Nevertheless, it contains certain provisions concerning the automatic processing of personal data which is related to the functionality of AI. In terms of automatic personal data processing, data subjects have the right to know the logic behind such process-

[188] Article 58, ibid.

[189] Article 57(1)(b), ibid.

[190] Article 15(2)(e), Convention 108+ Convention for the protection of individuals with regard to the processing of personal data.

[191] Recital 105, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

ing.[192] However, the right must not interfere with others' rights and freedoms, trade secrets, copyright, or any other intellectual property rights.[193] The proposed AI liability Directive seeks to promote trustworthy AI to exploit its benefits within the scope of the law.[194] The AI liability Directive appears to be consistent with the EU data strategy,[195] as it complements other AI policy-based regulatory instruments such as the GDPR, the DSA, etc.[196] Nevertheless, deep insights into the Directive are not the subject matter of this paper.

5 Discussion and conclusions

The legal aspects of the EU data protection laws reveal that the laws collectively protect children's right to have their data protected in a to-and-fro manner. For example, the GDPR analysis elicits that child-specific provisions concerning data protection emerged in several places. Articles 8, 12, 13, 14, and Recitals 38, 58, etc. deal with children exclusively. This phenomenon can also be discussed from a special protection viewpoint. It has already been clarified that the GDPR provides special protection to children. While doing so, the law may have introduced child-specific provisions in addition to general provisions from time to time whenever the legislators deemed it necessary.

Protecting children's right to protect personal data in AI is a complex matter. The laws concerning protection reveal that to be able to provide protection first, it is necessary to determine whether the concerned data subject is a child. The EU data protection laws favour the static approach to defining a child. This viewpoint has the potential to protect unborn child's rights. However, I believe it may not be enough, since in fixing the age at which to define a child, it may be incorrect to assume whether a child possesses the required amount of maturity or not. A dynamic approach is necessary to compensate for the static

[192] Recital 63, ibid.

[193] Recital 63, ibid.

[194] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) 2.

[195] ibid 4.

[196] ibid 10.

approach in a particular context to help settle a case by identifying whether a data subject is a child or not. At least this may be relevant in courtrooms where legal issues are usually challenged. The dynamic approach cannot protect the unborn child's data protection. Therefore, both approaches to defining children should be used. They complement each other. In the AI context, the main challenge is to determine whether a user is a child and apply related rules. The situation is less complicated in the products and services which are directed towards children exclusively. Nevertheless, it is more complicated when products and services are directed to anyone. Despite different controllers deploying innovative ways of verifying age, measures are not enough to identify children conclusively in an AI context. Further research is necessary in this regard. Identification of children is important as it helps to apply the children's specific legal rules e.g., providing special protection within the girth of data protection laws.

Child-specific provisions declare certain legal aspects of protecting children's data online. The list of identified aspects is not exhaustive but surely comprises the most important ones.

The legal aspects reveal unprecedented shortcomings of legal norms concerning children's right to have their data protected. The default data processing norm under the GDPR states that for processing children's data, controllers should rely on consent, controller obligation, children's interests, or public interests, as relying on other grounds may be impossible while processing children's data. They may not have the competence to be a part of a contract, and their privacy interests may always override the controller's legitimate interests. In addition, relying based on consent is not without challenges. According to GDPR and Member States' laws, controllers must attain consent from their parents if children are below 13 years of age. But children may provide consent if they are 13 years or older. However, there is a lack of unified rules that help controllers verify whether consent can be given by a child of 13 years or older (depending on MS laws) or the parental authority over the child. The EDPB needs to provide specific guidance concerning the matter. Again, children are entitled to be treated in a manner that serves their best interests. They have a right to participate[197] and to be represented by their parental au-

[197] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) 6.

thorities[198] according to the principle of their best interests. The law must define the best interests to ensure consistent compliance.

Moreover, there is no guarantee that parents always understand the underlying risks when they consent on behalf of their children. It is to be noted that the rights belong to children and parents merely assist them to exercise those rights. That is why less concerned and overprotective[199] types of parents may both end up restricting children's rights. Providing mandatory pieces of training to parents at different stages of their lives, such as before having a child, before admitting them to school, etc. might be a solution to the problem.[200]

Next, to comply with the transparent data processing principle, it is seen that the controller struggles to find ways to communicate certain information with children in a way that makes them understand the associated risks. The reasons behind successful business initiatives that target children in particular, children's likes, dislikes, interests, etc. can be inquired to find some solutions. Further, the existing legal norms concerning automatic decision-making using children's data need to be clarified to identify the circumstances in which it may be allowed. Finally, SA's role in creating public awareness needs to be settled.

Considering the shortcomings in the EU's data protection laws, it can be said that it is high time the EC enacted an exclusive data protection law for children to protect them from related risks and harms of the digital playground which include robots and AI.[201] The EU did not enact a special law that protects children's data exclusively.[202]

Acknowledgments

This work is funded by the University of Helsinki's Generation AI project under contract number 01331393. The author thanks Susanna Lindroos-Hovinheimo, Professor of Public Law, University of Helsinki, and Päivi Korpisaari, Professor of Communications Law, University

[198] ibid 5.

[199] Hof (n 185) 443.

[200] Ferrari (n 26) 319.

[201] Gaeta (n 51) 135.

[202] Kai Feng and Sylvia Papadopoulos, Student (K-12) Data Protection in the Digital Age: A Comparative Study, vol 51 (2018) 265.

of Helsinki for commenting on the draft of this paper. The author also thanks the in-house language revision services.

Disclosure Statement

The author reports that there are no competing interests to declare.

ORCID

Kamrul Faisal http://orcid.org/0000-0002-0691-6146