European Journal of Law and Technology, Vol 10, Issue 1, 2019

EJLT European Journal of Law and Technology

Children's Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm

Ingrida Milkaite and Eva Lievens[1]

1. Introduction

It has been claimed that an estimated one in three of all Internet users in the world today is below the age of 18 (Livingstone S. et al., 2015; UNICEF, 2017). Digital technologies can provide all children with more information, education, new opportunities and can be a game-changer for children in less developed countries. However, the 2017 UNICEF report on 'Children in a digital world' has revealed that many children from different parts of the world are still not connected to the internet confirming that the digital divide still is a reality (UNICEF, 2017). As research demonstrates that developmental challenges faced by certain regions or countries might have a negative impact on the protection of children's rights overall (Livingstone S, 2014; UNICEF, 2017), questions arise as to what extent children throughout the world can exercise their rights in today's increasingly digital society.

A wide range of children's rights laid down in the United Nations Convention on the Rights of the Child (UNCRC; United Nations General Assembly, 1989) is affected both positively and negatively in the digital realm. Children are offered vast opportunities online, but also might face risks for – among others – their rights to development (article 6), participation (article 12), freedom of expression (article 13) and association (article 15) (Lievens E et al., 2018). Research based on children's own perceptions has found that more and more children use the internet as an entertainment and information source and that they believe that internet access is their right (UNICEF, 2017). They are also often aware of risks they may encounter online.

One of these risks is related to children's online privacy. Throughout their childhood, children share information, photographs and videos with peers, family or – sometimes – strangers online. What is disclosed is, at times, of a private or even intimate nature. When it comes to privacy, studies have revealed that children generally consider themselves as having a right to privacy online from their parents or peers (i.e. 'social privacy') but have a much less developed understanding about the fact that their privacy may also be infringed upon by State or commercial actors (Livingstone S, 2018; Ofcom, 2008; Zarouali B et al., 2017). It is a well-established fact that, when children navigate the internet and use mobile apps and connected devices, data about them is collected both by public actors or governments and businesses, which often operate across the globe (Lupton D and Williamson B, 2017). Children's personal data 'pools' are being filled from the very beginning of their lives, for instance, when pregnancy scans and baby pictures are being uploaded on social media platforms (Children's Commissioner, 2018). Crucially, these extensive

and constantly growing personal data sets are predominantly held or obtained by private companies which may sell the data to advertisers, insurance companies or political parties, leading to unprecedented consequences in the long term. Hence, in the digital world, the right of the child to privacy, laid down in article 16 UNCRC, and the right to protection of personal data are particularly under pressure.

According to article 16 UNCRC, '[n]o child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.' The UNCRC was adopted in 1989, at a time when the use of internet and digital services was not as widespread as it is today. While there is no question about its applicability and relevance today, the way in which the Convention is implemented and interpreted is undoubtedly influenced by this technological and societal change. This is also reflected in initiatives at the UN level, such as the Day of General Discussion on Digital Media and Children's Rights in 2014.

Even though it has been acknowledged for a long time that 'everyone' has a right to privacy and while this is guaranteed by international and national human rights instruments, in practice, 'everyone' is often and without further thought assumed to be an adult. The idea that children merit the same – if not enhanced (Livingstone S, 2018) – protection is not always visible nor lobbied for during law-making processes, even if the best interests of the child, a key UNCRC principle laid down in article 3, requires specific attention and consideration. Moreover, up until now, studies related to children's right to privacy in the digital era have largely focused on Western countries, leading to knowledge gaps in relation to other regions.

That is why this article investigates whether and how the rights of the child to privacy and data protection are protected and integrated in regulatory frameworks in different regions across the world. As such, it aims to map and explore relevant legislation not only in Europe and the United States but also in a selection of countries in Africa and South America, in order to identify whether the implementation of the UNCRC is homogenous in different parts of the world and to detect key regulatory and implementation challenges. As such, its aim is to draw conclusions as to whether countries – both in the global North and South – make similar or diverging decisions in terms of children's data protection and privacy and how this may affect children day-to-day lives in the digital environment.

The focus within this article is on the right to privacy or 'respect for private life', as well as on the right to data protection. Theories on privacy and definitions and typologies (Koops B et al., 2017) thereof have been developed since the end of the 19th century (Warren S and Brandeis L, 1890). The varying conceptualisations and interpretations of both the concepts of 'privacy' and 'data protection' are wide-ranging to the extent they cannot be covered extensively in this article. In short, however, privacy is a broad concept that relates to various aspects of one's individual and personal sphere of life (Fuster GG, 2014). Data protection, on the other hand, is more tightly linked to (automated) processing of personal data, which is any information relating to an identified or identifiable individual (CoE, Convention 108) and the capacity to control the flows of personal information about oneself (Fuster GG, 2014). The complexity of the relationship between these notions, which are not the same but closely linked, is partially reflected in more detail in the analysis below of privacy and data protection regulation in Europe where the regulatory frameworks of both the Council of Europe and the European Union maintain a complementary, yet particular, understanding of the respective rights.

2. The Child's Right to Privacy and Data Protection in Europe

The right to privacy and the right to data protection are ensured both within the Council of Europe (CoE) and within the European Union (EU). The Council of Europe is a regional organisation consisting of 47 Member States. It was established in 1949 and its primary values are the protection and promotion of human rights, democracy and the rule of law in Europe (Council of Europe, 2018). The European Union was established as a regional economic and political organisation which (still) counts 28 Member States that are also members of the Council of Europe. Relying on their respective regulatory frameworks, both the European Court of Human Rights (ECtHR) of the Council of Europe and the Court of Justice of the European Union (CJEU) have issued numerous judgments relating to the right to privacy and data protection. Within this article, the reference to these judgments is confined to a number of cases which shed light on the relationship between privacy and data protection in the broader context of the protection of private and family life. Whereas the child's right to image has been addressed sporadically by the ECtHR, up until now, there have not been any cases dealt with by these courts specifically addressing children's online privacy and data protection.

2.1. Council of Europe

At the level of Council of Europe, the rights to privacy and data protection are enshrined in various documents. First of all, the rights to privacy and data protection are guaranteed by article 8 of the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, ECHR) and the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Both instruments are applicable to all natural persons, and, hence, children as well. The 1981 Convention is the first binding international instrument that protects individuals against abuses which may accompany the collection and processing of personal data, introduces basic principles and safeguards and attributes rights to data subjects. This Convention has recently been modernised (Council of Europe, 2018a). In the context of the different responsibilities of the supervisory authorities, the Convention now explicitly requires the authorities to pay 'specific attention […] to the data protection rights of children and other vulnerable individuals' when it comes to raising (public) awareness (article 15). This, however, is the only explicit reference in the Modernised Convention 108 to children.

The European Court of Human Rights (ECtHR, the Court) has interpreted article 8 of the ECHR on numerous occasions. In the context of that provision, guaranteeing the right to (respect for) private life, the Court has stated that

[t]he concept of 'private life' is a broad term not susceptible to exhaustive definition, which covers the physical and psychological integrity of a person and can therefore embrace multiple aspects of a person's identity, such as gender identification and sexual orientation, name or elements relating to a person's right to their image […]. It covers personal information which individuals can legitimately expect should not be published without their consent (*Axel Springer AG v Germany* (2012), para 83).

In the context of the CoE framework, the right to data protection falls within the scope of article 8 ECHR and is treated 'as a subset of the right to respect for private life' (Brkan M and Psychogiopoulou E, 2017). In its case of *S. and Marper v The United Kingdom* (2008), the ECtHR stressed that

[t]he protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. […] The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned (para 103).

In the 2017 judgment in the case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* the Grand Chamber confirmed that

Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged (para 137).

As the provisions of the ECHR and Convention 108 are applicable to all individuals, it is evident that these instruments are applicable to the younger generations and have an equal, if not a stronger (*K.U. v Finland*, 2008), effect on the protection of their privacy and data, also bearing in mind the specific CoE attention given to children's rights throughout the recent years.

This specific attention to children is especially evident in various recommendations and declarations by the CoE Committee of Ministers. For instance, the 2008 Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet (Committee of Ministers, 2008), the 2014 Recommendation on a Guide to human rights for internet users (Committee of Ministers, 2014) and the 2016-2021 Strategy for the Rights of the Child (Council of Europe, 2016) have acknowledged the importance of protecting children's rights to privacy and data protection in the digital environment. The CoE Strategy for the Rights of the Child explicitly stresses that 'the digital world exposes children to a wealth of opportunities, whether it is through computers, gaming consoles, tablets or smartphones' (Council of Europe, 2016). It also pays attention to the closely intertwined relationship between the positive and negative experiences children may have online by acknowledging that '*access to the Internet and to digital literacy is gradually being considered as dimensions of the rights of the child to freedom of expression, to participation and to education*', but that at the same time '*the digital environment also exposes children to harmful content and its effects, privacy and data protection issues and other risks*'.

The most recent development in this context is the Recommendation adopted by the CoE Committee of Ministers in July 2018 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Council of Europe, 2018b). It provides that, among other responsibilities concerning children,

States must respect, protect and fulfil the right of the child to privacy and data protection. States should ensure that relevant stakeholders, in particular those processing personal data, but also the child's peers, parents or carers, and educators, are made aware of and respect the child's right to privacy and data protection.

It also recommends that States should take particular care ensuring data protection principles with regard to connected or smart devices, such as toys and clothes, and provides that the creation of (digital) profiles of children should be prohibited by law, except for in very specific circumstances (Council of Europe, 2018c).

2.2. European Union

The European Union provides for the protection of both the right to privacy and the right to data protection through its primary and secondary legislation. First, article 16 of the Treaty on the Functioning of the EU provides that '[e]veryone has the right to the protection of personal data concerning them' (European Union, 2012) while article 6 (3) of the Treaty of the European Union states that '[f]undamental rights, as guaranteed by the [ECHR] […], shall constitute general principles of the Union's law' which also include the right to data protection as recognised through the interpretation of the ECtHR (Brkan M and Psychogiopoulou E, 2017). Article 7 of the 2000 Charter of Fundamental Rights of the European Union (CFREU) provides for the protection of privacy and states that 'everyone has the right to respect for his or her private and family life, home and communications'. Article 8 CFREU recognises the particular right to data protection by providing that '[1] everyone has the right to the protection of personal data concerning him or her [and] [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 […]'. Crucially, article 24 CFREU explicitly acknowledges the rights of the child and states, in particular, that '[c]hildren shall have the right to such protection and care as is necessary for their well-being'. Parallel to article 3 UNCRC, article 24 CFREU also emphasises that '[i]n all actions relating to children, whether taken by public authorities or private institutions, the child's *best interests* must be a primary consideration' (authors' emphasis).

In its caselaw, the Court of Justice of the European Union (CJEU) has dealt with both the right to privacy and the right to data protection. The CJEU has recognised the right to data protection in the case of *Promusicae* (2008) even before the CFREU became legally binding through the entering into force of the Lisbon Treaty in 2009 (Fuster GG and Gellert R, 2012; Brkan M and Psychogiopoulou E, 2017). In this case the CJEU took a strong stance and 'seemed to imply that the right to data protection constitutes a part of the right to privacy by stating that the case at hand included "the right that guarantees protection of personal data and hence of private life"' (Brkan M and Psychogiopoulou E, 2017, p.11). Later on, in *Tele2 Sverige AB and Watson et al.* (2016), the CJEU made a clearer distinction between the two rights and decided that 'Article 8 of the [CFREU] concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR' (Brkan M and Psychogiopoulou E, 2017). In general, the CJEU's stance on the interplay between the right to privacy and the right to data protection remains somewhat unclear (Brkan M and Psychogiopoulou E, 2017).

With regard to secondary legislation of the European Union, the Data Protection Directive (DPD) was the main legislative document regulating data protection in the Member States of the EU since 1995. As it had been adopted more than twenty years ago, it, firstly, became inevitably outdated due to technological developments and, secondly, did not provide sufficiently harmonised rules for companies in the Digital Single Market (Robinson N et al., 2009). Hence, in April 2016, the Council and the Parliament of the European Union adopted a new legislative instrument in the context of the EU data protection reform – the General Data Protection Regulation (GDPR) – which became applicable on 25 May 2018. Another element of the new data protection framework, a proposal for a new ePrivacy Regulation, which will replace the 2002 ePrivacy Directive, is currently still on the legislative table.

In general, in comparison to the DPD, the GDPR provides for a wider material and territorial scope, stricter sanctions, and emphasises concepts such as privacy by design and the rights of data subjects, including the right to erasure and the right to data portability. In terms of the discussion on the relationship between privacy and data protection, it is interesting to note that these two

legal instruments refer to both rights (Brkan M and Psychogiopoulou E, 2017). Article 1 (1) of the repealed DPD provided that 'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their *right to privacy with respect to the processing of personal data*' whereas in the GDPR the world 'privacy' or 'private' is not mentioned literally, stating in article 1 (1, 2) that '[the] Regulation lays down rules relating to the protection of natural persons with regard to the *processing of personal data* […] [and] protects fundamental rights and freedoms of natural persons and in particular their *right to the protection of personal data*' (authors' emphasis). Nevertheless, the protection of the right to privacy or 'private life' is inherent in the GDPR reference to fundamental rights.

Unlike the DPD, the GDPR includes a number of provisions that explicitly aim to protect the child data subject's right to data protection. First and foremost, recital 38 GDPR recognises that '[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'. According to the recital, such specific protection is especially warranted in relation to the collection of children's data for the purposes of marketing and profiling.

In addition to the general acknowledgment of the specific need for protection when it comes to personal data of children, article 8 GDPR provides for particular conditions applicable to a child's consent to process data in relation to information society services being directly offered to him or her. This article states that when consent is the ground for data processing, and information society services are offered directly to a child, data processing shall be lawful when the data subject is at least 16 years old. In situations where the child is younger than 16 years old, consent must be given or authorised by the holder of parental responsibility over the child in order for data processing to be lawful under the GDPR. According to para. 2, in this case, the data controller must undertake reasonable efforts to verify the parental consent, taking into consideration available technology. There is no further guidance as to what might constitute an acceptable method for obtaining verifiable parental consent. Crucially, EU Member States have the opportunity to derogate and choose a lower age than 16, provided it is not below 13 years. Preliminary research into the (in a few countries still ongoing) national legislative processes demonstrates that a very fragmented landscape is gradually emerging across the EU (Milkaite I and Lievens E, 2018). This means that the intended harmonisation will not be achieved, and children will be able to consent to data processing at different ages depending on the Member State that they reside in, also in relation to services that are offered throughout the EU. No explanation, however, has been offered by the European legislator as to why the ages between 13 and 16 years were chosen in particular. There are no references to scientific studies or other evidence confirming that such a decision is indeed suitable in terms of the best interest of the child. Moreover, it is not yet clear whether the rules adopted in the country of establishment of a particular service or the country of residence of the child will be applicable in terms of the implementation of article 8 GDPR (Article 29 Working Party, 2018). This leads to legal uncertainty for the many (often globally operating) companies offering information society services in different EU Member States.

Furthermore, the protection of children's rights is strengthened in the GDPR through the requirement to provide information to children in a concise, transparent, intelligible and easily accessible form, using clear and plain language (recital 58 and article 12), the right to erasure that is also, and even especially, available to children (article 17 and recital 65 which mentions that this right 'is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal

data, especially on the internet'), Data Protection Impact Assessments (recital 75 and article 35) which could or – sometimes even should – be conducted when children's personal data is processed (van der Hof S and Lievens E, 2018), and the drafting of codes of conduct (article 40) which may be used to enhance children's rights by providing more specific protection when children's data is processed, and the application of provisions on Data Protection Authorities' (DPAs) tasks to raise awareness (article 57).

In relation to profiling, the Article 29 Working Party – a former advisory body consisting of all European DPAs which provided guidance on the implementation of the EU data protection law and which has now been replaced by the European Data Protection Board established by the GDPR – has stated that despite the fact that the GDPR does not ban profiling of children completely, data controllers should in general refrain from profiling children for (behavioural) marketing purposes (Article 29 Working Party, 2018). Recital 71 also refers to the fact that solely automated decision-making, including profiling, with *legal* or *similarly significant effects* should not apply to children (authors' emphasis). In any case, when children are the subject of profiling specific protection should be afforded to them (recital 38; Verdoodt V and Lievens E , 2017; Information Commissioner's Office, 2017). As profiling might have a serious impact on a variety of children's rights, these provisions are particularly important. Profiling of children from a young age might result in advertisements, services, products, and information being tailored for and targeted at them, based on their online presence and (previous) behaviour, resulting in 'more of the same' and reducing exposure to new, unexpected or serendipitous ideas. This practice raises concerns related to the right to receive information (article 13 UNCRC), the right to freedom of thought (article 14 UNCRC), and the right to development (article 6 UNCRC), which encompasses experimenting and – especially for adolescents – opportunities to 'explore their emerging identities, beliefs, sexualities and opportunities, balance risk and safety, build capacity for making free, informed and positive decisions and life choices' (United Nations Committee on the Rights of the Child, 2016).

Remaining questions relate to whether or how the implementation of the GDPR will consider the differences in children's social background, context, evolving capacities, and best interests; and how privacy by design and privacy by default mechanisms (article 25 GDPR) will be integrated within current technologies (Milkaite I et al., 2017; Lievens E et al., 2018; Livingstone S, 2018). These questions are of particular importance since the ways in which they will be addressed will significantly impact different children's rights, possibilities and every-day lives in general.

Another piece of the EU data protection puzzle, the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), establishes rules for the processing of personal data in the electronic communications sector. This Directive will be replaced by the ePrivacy Regulation in the coming years. The Regulation, aiming at safeguarding and strengthening privacy and data protection in the field of electronic communications, will update the current rules and introduce additional guarantees for users of such services. The European Commission released its official proposal for a Regulation on Privacy and Electronic Communications in January 2017. The ePrivacy Regulation is supposed to particularise and complement the GDPR in the field of the provision and use of electronic communications services and will thus be a *lex specialis* to the GDPR. Hence, all matters concerning the processing of personal data not specifically addressed by the ePrivacy Regulation would be covered by the GDPR. The proposed ePrivacy Regulation would apply to 'processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users'. Such equipment, in simple words, includes tablet computers, mobile phones, connected Internet of Things and Toys devices, smart

home assistants and many more devices which are increasingly used in proximity to or by children. Therefore, the ePrivacy framework significantly affects digital and online activities by children even though the proposed regulation does not mention children explicitly.

The Commission proposal contains a number of key points that are (also) relevant to children. First of all, the Commission proposal extends the scope of the ePrivacy Regulation to 'Over the Top' (OTT) communication services such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage and Viber. It will also be applicable to the so-called 'Internet of Things' devices, such as internet connected smartwatches, smart toys, connected cars, appliances and health devices, as well as to machine-to-machine (M2M) transmissions, such as between a smart toy and an iPhone or between an Amazon Echo and an iPad. Second, the Regulation strengthens the protection for metadata (such as, for instance, the time of a call and location data which, in case of children, is extremely sensitive), as this type of data may also reveal very sensitive and personal information. In addition, internet users will be better protected in terms of spam by emails, SMS and automated calling machines and will also be able to enjoy more effective enforcement of the provisions (European Commission, 2017). Among the most important further changes to the proposal which made their way into the EP Draft Legislative Resolution (Committee on Civil Liberties, Justice and Home Affairs, 2017) and are relevant for children, are the extension of the principle of confidentiality of communications to data related to or processed by terminal equipment, the prohibition of the so-called 'cookie-walls', the introduction of granular consent and the introduction and promotion of end-to-end encryption.

While the GDPR explicitly recognises children as a vulnerable group of individuals that deserve specific protection when it comes to the processing of their personal data, especially in the context of profiling and (behavioural) marketing, the proposed ePrivacy Regulation does not mention children at all. However, one of the EU Parliamentary Committees put forward proposal for new recitals and articles that also explicitly recognise the need to provide additional protection to children, for instance, with regard to profiling, behavioural advertising and terminal equipment that is intended particularly for children's use (European Parliament Committee on Civil Liberties, Justice and Home Affairs, 2017). These proposed amendments would have had a significant effect on current, especially commercial, practices in relation to children, but, in the end, were not included in the Draft Legislative Resolution of the European Parliament.

3. The Child's Right to Privacy and Data Protection in America

Following the evaluation of the legal framework in Europe, this section focuses on the analysis of the legal framework in the United States, Brazil and Uruguay. While aiming to identify whether children's personal data and the right to privacy are protected in a similar way in countries in different parts of the world, these particular countries were chosen on the basis of the following reasons. Although the United States has not ratified the UNCRC, it has adopted the Children's Online Privacy Protection Act in 1998 and has since built quite extensive experience in implementing it in practice; in Brazil, the new Law on the Protection of Personal Data was adopted in August 2018 which offers a few very specific provisions which are not found in other legal frameworks for children's privacy and data protection; and Uruguay was the first non-CoE country to ratify the CoE Convention 108, and the first South American country.[2]

3.1. United States

Neither the right to privacy, nor the right to data protection is mentioned in the US Constitution. The US jurisprudence nevertheless provides for a certain level of the protection of privacy through the constitutional interpretation of 'the First Amendment (freedom of speech, religion and association), the Third Amendment ([…] privacy of the home […]), the Fourth Amendment (freedom from unreasonable searches and seizures), and the Fifth Amendment (privilege against self-incrimination), as well as […] the Ninth Amendment' (Fuster GG, 2014, p. 28). The attempts to regulate the protection of privacy in the US in general have been considered fragmented. A variety of privacy laws covering different sectors (such as credit reporting, federal agencies, schools, financial institutions, video rental, cable television, health) exists and initiatives are taken at State level (for instance, the 2018 California Consumer Privacy Act), but there appears to be no overarching framework (Gellman R, 2018).

However, in relation to the protection of personal data of children, a specific legislative instrument was adopted early on (Montgomery K and Chester J, 2015). The Children's Online Privacy Protection Act (COPPA) is a US federal law which was adopted in 1998 and became applicable in 2000. COPPA provides that 'a child' is a person under 13 years while 'personal information' is defined as individually identifiable information about a person collected online. The definition of personal information encompasses first and last name, address, e-mail address, telephone number, social security number, screen or user name, a persistent identifier that can be used to recognise a user over time and across different websites or online services, a photograph, video, or audio file, where such file contains a child's image or voice, geolocation information sufficient to identify street name and name of a city or town and other information which could be combined with other pieces of information in order to identify a person (COPPA, 2013; Federal Trade Commission, 2015). Crucially, COPPA imposes certain requirements on operators of websites or online services *directed to* children under 13 years of age, and it is also applicable to operators of other online services that have *actual knowledge* that they are collecting personal information online from a child under 13 years of age (Federal Trade Commission, 2013a; authors' emphasis). The law obliges website or online service providers to provide notice that they are collecting children's personal information, and to collect verifiable parental consent. The main aim of the act is to place parents in control over what personal data is collected from their young children online, although it has been argued that this requirement 'has placed parents in an increasingly difficult position, forcing them to evaluate a company's data collection and marketing practices based on what they read in its privacy policy' (Montgomery K and Chester J, 2015). This, in fact, had a big impact on the subsequent development of terms and conditions of many currently widely used global services, such as Facebook, Google, Instagram, Snapchat, Twitter and other companies. Avoiding obtaining parental consent is one (or the) reason why many online services set 13 years as the minimum age for creating an account or profile (Holloway D and Green L, 2016; Montgomery K et al., 2017). This has a direct effect on children's rights to participation, freedom of expression, association and education.

Under COPPA, a 'verifiable parental consent' is any reasonable effort, taking into consideration available technology, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorises the collection, use, and disclosure of personal information and the subsequent use of that information *before* the information is collected from that child.

The Federal Trade Commission (FTC), the federal body overseeing the implementation of COPPA,

has approved a number of different verification methods that vary depending on whether the operator is planning to use children's personal information for internal purposes only or whether it plans to disclose children's personal information to third parties, or allow children to make it publicly available. In the latter case the rules are more stringent and include such verification methods as providing a consent form to be signed by the parent and returned via US mail, fax, or electronic scan (the 'print-and-send' method); requiring the parent, in connection with a monetary transaction, to use a credit or debit card, or other online payment system; having the parent call a toll-free telephone number staffed by trained personnel, or have the parent connect to trained personnel via video-conference; or verifying a parent's identity by checking a form of government-issued identification against databases of such information, provided that the parent's identification information is promptly deleted after completing the verification (Federal Trade Commission, 2015). In addition, the FTC approved a number of novel authentication methods, including the Social Security number verification method (Tabor AJ, 2013), the 'facial recognition through parental 'selfies'' method and the 'knowledge-based questionnaire' method which requires a parent to reply to questions a child would usually not know the answer to (i.e. household oriented questions) (Federal Trade Commission, 2013b). A simpler method, the 'email plus' verification is also possible when the information collected from children is only used for internal purposes and is not disclosed to third parties or made publicly available (Federal Trade Commission, 2015).

One of the most important aspects of COPPA is the fact that the parental consent requirement is applicable not only to online websites or services that *direct* their services to children or target them but also the ones who have *actual knowledge* that their services are in fact used by children (Montgomery K et al., 2017). Some specific factors may help companies determine whether their services are considered to be directed to children, such as the subject matter of the service, its visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, whether advertising promoting or appearing on the website or online service is directed to children, audience composition, as well as the intended audience of the site or service and actual knowledge that personal information is collected directly from another website or service which is directed to children (Federal Trade Commission, 2015).

Finally, under COPPA, parents must have access to their child's personal information to review and (or) have the information deleted and they must also have the opportunity to prevent further use or online collection of a child's personal information. The operators are obliged to maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security and they must also retain personal information collected online from a child for only as long as is necessary to fulfil the purpose for which it was collected (Federal Trade Commission, 2015). Although the COPPA rules were updated in 2013 to enhance protection in relation to certain data collection and marketing techniques, such as behavioural advertising, it has been argued that 'major, transformative changes in the digital marketplace' require a fundamental rethinking of COPPA, and, for instance, an extension of its scope to children of 13 years and older (Montgomery K and Chester J, 2015).

3.2. Brazil

In line with international provisions, the Brazilian Constitution not only provides for the right to privacy in general but also for the right to the secrecy of correspondence and telegraphic communications. Aside from the Constitution, the right to privacy and data protection in Brazil used to be mostly protected by sectoral laws covering the spheres of, among others, finances, health and internet. The general legal and political approach towards children was the subject of the Statute of the Child and Adolescent (Law No. 8069/1990) 'making the doctrine of full protection a central pillar of ensuring rights' (ICT Kids Online Brazil: Survey on Internet Use by Children in Brazil, 2017).

The Statute of the Child and Adolescent, which provides for the integral protection of children and adolescents (article 1), considers a child to be a person under twelve years of age, and an adolescent between twelve and eighteen years of age (article 2) (Brazilian Statute of the Child and Adolescent, 1990). The Statute proclaims children's right to respect and the inviolability of their physical, psychological and moral integrity, including the protection of their image, identity, autonomy, values, ideas and beliefs, personal spaces and objects (article 17). Crucially, it also stipulates that as soon as children reach adulthood at the age of 18, their history in social and educational systems must be deleted, since their status in the world of social and legal relations changes (ICT Kids Online Brazil: Survey on Internet Use by Children in Brazil, 2017). This is a very specific provision which could be understood as minimising long-term (unintended) consequences related to childhood data in the digital world where increasing amounts of information are included in databases that might be linked to each other. While much more limited, it appears to be somewhat similar to the European 'right to be forgotten' or 'the right to erasure', laid down in Article 17 GDPR providing that a data subject has the right to have his or her data erased by the controller without undue delay when certain conditions are fulfilled. However, this article does not entail an obligation for certain actors to delete data by default at the moment when children turn 18.

In addition to the Statute of the Child and Adolescent, two recent initiatives concerning the protection of privacy and data protection in Brazil are relevant. In April 2014, the Brazilian Internet Law (No. 12.965) was adopted, laying down principles, guarantees, rights and duties for the use of the internet in Brazil. It established, among others, principles relating to the guarantee of freedom of expression, communication and expression of thought, protection of privacy, protection of personal data, preservation and guarantee of net neutrality (article 3). Moreover, it ascertained the protection of secrecy and confidentiality of communications (article 7, parts II, III), the obligation to provide clear and complete information on the collection, use, storage, treatment and protection of personal data (article 7, part VIII) and the requirement to obtain consent for data processing (article 7, part IX). Children are not explicitly addressed in the Law, other than through a reference to parental control of content that is considered to be appropriate for children by the parents (article 29). The Law also mentions the responsibility of the public authority, together with internet application and service providers and civil society, to promote education and provide information on the use of the computer programs as well as for the definition of good practices for the inclusion of children and adolescents in the digital world.

In October 2015, a Draft Law for the Protection of Personal Data was published. It was approved by the Brazilian Congress on 10 July 2018 while the final Law on the Protection of Personal Data (No. 13.709) was adopted and signed into law by the Brazilian President on 14 August 2018 (Senado Federal, 2018). The Law is the first of its kind in Brazil and is thought to have been inspired by the European GDPR which is evident from some of the new provisions of the Law. The

Law amends the Brazilian Internet Law (No. 12.965) of 23 April 2014 and establishes a comprehensive data protection regime in Brazil which imposes specific rules for the collection, use, processing and storage of personal data, both in electronic and physical forms. Notably, the Brazilian President Temer vetoed a number of important provisions of the Law, including the rules on the national data protection authority, penalties for the infringement of the Law and special transparency requirements for public-sector actors handling personal data (Pallero J and Tackett C, 2018). Nevertheless, the implementation period of the Law has started and will last for 18 months (article 65 of the Law). The Law will come into force on 14 February 2020.

First of all, the new Law is applicable to the processing of personal data, including by digital means, by a natural person or a legal entity of public or private law (article 1). Its definitions, provided in article 5 of the Law, are very similar to the ones in the GDPR. The grounds, or 'scenarios', for data processing are also similar to the ones provided by the GDPR and include, among others, consent and legal, contractual obligations. Under part XII of article 5, consent needs to be free, informed and unambiguous manifestation whereby the data subject agrees to the processing of his or her personal data for a given purpose. The data processing requirements include processing in good faith and compliance with such principles as purpose limitation, suitability, necessity, free access, quality of data, transparency, security, non-discrimination and accountability (article 6). The Law places the burden of proof in terms of showing that consent was obtained on the data controller (article 8 (1)).

Article 9 of the new Law provides two interesting rules on consent. First, it states that when consent is required, it shall be considered void if the information provided to the data subject contains misleading content or was not previously presented in a transparent, clear and unambiguous way. Second, unlike the GDPR, the Law does not prohibit conditional consent. Conditional consent situations are considered to be the ones in which access to a particular service or product is only granted in return of a data subject's consent to data processing. According to the new Law, when the processing of personal data is a condition for the provision of a product or service or for the exercise of a right, the data subject shall be specifically informed of this fact and of the means by which he or she may exercise his or her data subject's rights. The Law also prohibits commercial sharing of health data between data controllers for economic advantage in article 11 (10). Data subjects have the same rights as the ones provided by the GDPR (article 18) and can exercise those rights through complaints to the national data protection authority (yet to be established), consumer-defence entities and courts (individually or collectively) (articles 18 and 22).

Section III of the Law provides the rules for the processing of children and adolescents' personal data. Yet, the Law does not define a child and it is not clear until what age a person is considered a child in this context. First of all, the Law states that children's personal information shall be processed in their best interest (article 14). The first part of the same article provides that the processing of children's personal data shall be carried out with specific and *highlighted* consent ('*consentimento específico e em destaque'* in Portuguese)[3] given by at least one of the parents or the legal representative. There are no further details provided on this rule and it is not completely clear how it will be implemented in the future and whether the parents of all under-18-year-olds[4] would have to provide such consent. The latter case could likely have a negative impact on children's right to information, education, freedom of expression and association (Livingstone S and O'Neill B, 2014; Livingstone S, 2015; Milkaite I et al., 2017; Lievens E et al., 2018; Livingstone S, 2018), depending on its implementation.

The only further addition to the parental consent requirement in the Law is expressed in part 5 of article 14, according to which the controller shall use all *reasonable efforts* to verify that the parental consent was given by the child's representative, *considering available technologies*. This phrasing is similar to parallel provisions in both COPPA and the GDPR. Furthermore, controllers shall not condition the participation of data subjects to games, internet applications or other activities for providing personal information beyond what is strictly necessary for the activity (article 14 (5)).

Finally, the new Law also provides for a specific child transparency provision, stating that information on the processing of children's data shall be given in a *simple, clear and accessible manner*, considering, among others, the intellectual characteristics of the data subject, using audiovisual resources when appropriate, in order to provide the necessary information to the parents or the legal representative and that is appropriate for the children's understanding.

Clearly, certain (but not all) provisions paying specific attention to children appear to be similar to COPPA and GDPR. The similarity also extends to the grey zones and vague notions that are included in the latter documents. In anticipation of the actual coming into force of the Law, the particular methods and results of their implementation in practice in Brazil thus remain to be seen.

3.3. Uruguay

In terms of the legal protection of privacy in Uruguay, the Law on the Protection of Personal Data was adopted in 2008. It regulates the processing of personal information of natural and legal persons in the public and private sectors. The general principles of data protection, according to the law, include legality, purpose of processing, prior informed consent, data security and responsibility (article 5). Moreover, data subjects have such rights as the right of access, right to rectification, update, inclusion or deletion of data (Law on the Protection of Personal Data of Uruguay, 2008). Chapter 4 provides specific protection for certain data, that is sensitive data, health related data, data related to telecommunications, data related to databases created for advertising purposes and data relating to commercial or credit activity.

The law includes principles that appear to be similar to European data protection law (Greenleaf G, 2012). This – at least in part – stems from two additional reasons. First, in 2012 the European Commission has adopted an 'adequacy decision' on the adequate protection of personal data provided by the Eastern Republic of Uruguay with regard to automated processing of personal data. Article 1 of the decision provides that '[f]or the purposes of Article 25(2) of Directive 95/46/EC, the Eastern Republic of Uruguay is considered as ensuring an adequate level of protection for personal data transferred from the European Union' (Commission Implementing Decision, 2012). Such a decision is necessary to allow the transfer of personal data of EU citizens to third countries. Secondly, in 2013, Uruguay became the first non-European state to accede to the 1981 CoE Convention for the protection of individuals with regard to Automatic Processing of Personal Data (Council of Europe, 2013). However, despite having laws which are considered to be 'adequate' and similar to those of Europe, Uruguay does not seem to provide for specific legal protection for the child's right to privacy, other than the general applicability of the Constitution and the Law on the Protection of Personal Data to all individuals.

4. The Child's Right to Privacy and Data Protection in Africa

The privacy and data protection legislation in Ghana and South Africa is the focus of this part of the article. These are two countries among others in Africa (Makulilo AB, 2016) which have

adopted specific legislation for the protection of personal data, including provisions that refer to children's data. Ghana and South Africa were chosen in particular in order to complement the social science research conducted in the context of the Global Kids Online project.[5]

4.1. Ghana

The Constitution of the Republic of Ghana provides for a general right to privacy, stating that '[n]o person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law' (article 18 of the Constitution of the Republic of Ghana, 1992). In 1998, Ghana also adopted the Children's Act (Act 560) which provides for specific rights for children (persons under 18 years of age, according to the law, reflecting the UNCRC). The right to privacy and data protection is not, however, included explicitly in the law (Children's Act of Ghana, 1998).

The main privacy and data protection law in Ghana is the Data Protection Act of 2012. The Act provides eight basic principles which must be followed by data controllers and processors as regards the collection, use, disclosure and care for personal data or information – accountability, lawfulness, specification of purpose, compatibility of further processing with purpose of collection, quality of information, openness, data security safeguards and data subject participation, which are very similar to the data protection principles included in the Convention 108, and the GDPR (Data Protection Act of Ghana, 2012; Data Protection Commission of Ghana, 2018). The Data Protection Act recognises such data subjects' rights as access to personal information, the right to amend one's personal information, the right to prevent processing of personal information, the right to freedom from automated decision making, the right to prevent processing of personal data for direct marketing purposes, the right to seek compensation through the courts and to complain to the Data Protection Commissioner. According to the Act, a person who processes personal data shall ensure that the personal data is processed without infringing the privacy rights of the data subject; in a lawful manner; and in a reasonable manner (article 18 (1)). The definitions, such as of 'personal data', 'special personal data', 'data controllers' and 'data processing', are comparable to the ones established in the EU as well. Finally, the law introduces the Data Protection Commission as an independent statutory body which is responsible for enforcing compliance with the Act (Data Protection Commission of Ghana, 2018).

Interestingly, the Data Protection Act of Ghana refers to children in its chapter on the processing of special personal data. Under article 37, the processing of special personal data is – in principle – prohibited. The two types of 'special personal data' are (1) personal data relating to a child who is under parental control, and (2) personal data relating to religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behaviour of an individual. A number of exceptions to this prohibition is integrated in the second paragraph, including where processing is necessary, or the data subject consents to the processing. It is, however, unclear from the text of the Act whether the latter exception means that a parent, or a child, being the data subject, can consent to the processing of special data. The Act further specifies that the processing of personal information is necessary when it is for the exercise or performance of a right or an obligation, or when it is for the protection of the vital interests of the data subject. Also, special personal data, including children's personal data, shall not be processed unless the processing is carried out for the protection of the *legitimate activities* of a body or association which is established for non-profit purposes, exists for political, philosophical, religious or trade union purposes; relates to individuals who are members of the body or association or have regular contact with the body or association in connection with its purposes, and does not

involve disclosure of the personal data to a third party without the consent of the data subject. The latter provision seems to be applicable in cases when, for instance, schools are processing children's data for their legitimate interest regarding administration.

4.2. South Africa

The South African Constitution, adopted in 1996, provides for the protection of the right to privacy, in general, as well as the right to privacy of communications. Crucially, the Constitution of South Africa specifically addresses children's rights (article 28, Chapter 2, the Bill of Rights). It provides that 'children have the same constitutional rights as adults and these include [among others] the right to have their dignity respected, the right to freedom and security and the right to be free of all forms of violence including torture or any cruel, degrading or inhumane punishment' (Constitution of the Republic of South Africa, 1996). It also notes that '[a] child's best interests are of paramount importance in every matter concerning the child' (article 28, part 2).

In terms of legislation specifically providing for the protection of the right to data protection, the South African Protection of Personal Information Act (POPI) was adopted in 2013 (Act 4 of 2013). It is important to note, however, that this Act will only come into force in its entirety[6] by presidential proclamation, on a date which is still to be announced.

The POPI applies to the processing of personal information by automated or non-automated means. In the latter case, in order for the Act to apply, the data records must form a part of a filing system. The Act details the protection of personal information processed by public and private bodies, introduces certain conditions establishing minimum requirements for the processing of personal information, provides for the establishment of an Information Regulator who has the power to enforce the Act (appointed in 2016), provides for the issuing of codes of conduct, sets out the rights of persons regarding unsolicited electronic communications and automated decision making, and regulates the flow of personal information across the borders of the Republic (Protection of Personal Information Act of South Africa, 2013). The Act provides for the conditions required for lawful data processing, which are similar to the ones in the EU, i.e. accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguard, data subject participation (article 4). Notably, the POPI also provides rules on the special processing activities, such as the use of unique identifiers, profiling, direct marketing, unsolicited electronic communications and automated decision making, which might be important for children and their human rights.

Part C of the Act regulates the processing of personal information of children. According to the Law, a child is a natural person under the age of 18 years 'who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him or herself'. Under article 34, '[a] responsible party may […] not process personal information concerning a child' unless such processing is authorised by article 35, the grounds for which are, among others, prior consent, necessity or historical, statistical or research purposes. In terms of consent for data processing, the Act provides that a 'competent person' must consent to the processing of a child's personal data and does not mention any instances in which a child could consent to certain data processing himself or herself.

Parts 2 and 3 of article 35 provide some more information on the exceptional circumstances when children's personal data can be processed. Subject to additional safeguards, the Regulator may, upon application by a responsible party[7] and by notice in the *Gazette*, authorise a responsible party to process the personal information of children if the processing is in the public interest and

appropriate safeguards have been put in place to protect the personal information of the child. The Regulator, however, may impose reasonable conditions in respect of any authorisation granted in such cases. These conditions may include obliging the responsible party to allow the competent authority to review the personal information processed and refuse to permit its further processing; provide notice regarding the nature of the personal information of children that is processed, how such information is processed and information regarding any further processing practices. Crucially, the Act instructs the responsible party, to refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him or herself than is reasonably necessary given the purpose for which it is intended (article 35 (3) (c)). Finally, the responsible party shall establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children (article 35 (3) (d)). Therefore, in cases when the Regulator accepts the application by a party to process children's personal data, it can be done, under specific conditions which, again, establish many requirements for the protection of children's personal information. Once the POPI is published in the *Gazette*, responsible parties will have a one-year transition period to comply with its provisions (article 114).

5. Key regulatory challenges related to the child's right to privacy and data protection in the digital realm

The analysis of privacy and data protection frameworks in selected countries around the world – which, except for the United States, have ratified the UNCRC – shows a fragmented landscape when it comes to the rights of the child to privacy and data protection. Whereas the right to privacy is generally included for all individuals in constitutional documents and most countries have adopted specific data protection acts, the extent to which these documents address children, and the need for the protection of their personal data in particular, differs. In certain countries there is no reference to children, in others parental consent is needed to process children's personal data, and sometimes the processing of such data is in principle prohibited, except in certain circumstances. In some frameworks, differentiations are made according to specific ages, in others, children are considered or appear to be all persons under the age of 18 years. An interesting observation is related to the fact that data protection principles that have been recognised at international level since the agreement on the (non-binding) OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Data in 1980 (OECD, 2011) and the adoption of CoE Convention 108 in 1981 are increasingly included in data protection legislative frameworks across the world. As the digital environment is inherently global, a harmonisation of frameworks in this respect is, although not obvious, a welcome development.

But perhaps harmonisation, especially from a children's rights perspective, should be enhanced even further. Various paths to achieve this could be taken. Although it has been argued that new 'digital rights' should be formulated in respect of children (e.g. the 5rights framework), many agree that - fundamentally - the UNCRC is still fit for purpose in the digital age (Livingstone S et al., 2017; Lievens E et al., 2018). An interesting proposal that could further strengthen and enrich a global approach to children's rights in the digital environment relates to the adoption of 'A general comment on Children's Rights and Digital Media' at the level of the United Nations Committee on the Rights of the Child (LivingstoneS et al., 2017). In relation to privacy and data protection, Livingstone et al. have argued that such a general comment could address:

support for children to understand the nature of privacy online in order to promote the capacity to make safe choices, elaboration of the implications of the digital environment for children's privacy rights, ***development of appropriate legislative and policy frameworks to balance rights to privacy with the need for protection****, raising awareness of the nature of privacy and its breaches online, and the* ***introduction of regulatory frameworks for the industry****, including through international bodies, and consideration of growing potential for surveillance, including by parents, on privacy rights of children* (2017; authors' emphasis).

Moreover, in the context of efforts to ensure that both younger children and teenagers are guaranteed their fundamental right to privacy without infringing on other rights that youth are entitled to, such as their rights to information, education, participation and freedom of expression in the digital world, the idea of adopting worldwide 'Fair Information Principles for Youth in the Global Digital Culture' based on the UNCRC has also been proposed (Montgomery K and Chester J, 2015). Such principles would impose obligations on industry and government bodies 'to ensure that children and adolescents are not subjected to unfair and deceptive surveillance, data collection, and behavioural profiling' and take the unique needs of children of all ages into account (Montgomery K and Chester J, 2015). Indeed, the analysis of the legal frameworks in jurisdictions across the world has demonstrated that the 'age' of a child is often a factor that determines the level of protection that is attributed or the capacity that a child is deemed to have in this context (e.g. to provide consent him- or herself). Two findings are relevant in this respect. First, although a child is anyone under the age of 18 according to the UNCRC, with respect to data protection, the ages that are included in the legislation vary widely, from 12/13 to 18. Often there is little or no explanation as to why a certain age was chosen in a specific country. A question that arises is whether children's capacities in relation to data protection are actually that different across countries, justifying the choice for such different ages? Second, it seems hard to reconcile the use of generic cut-off ages with the evolving capacities of a child. A three-year old, a ten-year old and a sixteen-year old will most likely have a very different understanding of privacy and data protection related issues. Yet, a number of the data protection laws that were examined did not define the notion of a 'child', suggesting that a 'child' means anyone younger than 18 without a distinction as to rights and responsibilities in this area. Whereas for a long time this was lacking, more research about how children understand their right to privacy and data processing practices is slowly emerging (Livingstone S, 2018), and this should be reflected in policy and legislative efforts in the near future.

6. Conclusion

Regardless of concrete harmonisation efforts, it is our view that it is not only timely, but also urgent, to ensure that the child's right to privacy and data protection in the digital realm is on top of international, regional and national policy agendas. Whereas most countries have acknowledged every individual's right to privacy through the ratification of general international human rights documents, and every child's right to privacy through the ratification of the UNCRC, it would be helpful in today's digital society if the UN Committee on the Rights of the Child would provide more guidance on how this right to privacy is impacted by the presence of technology in children's lives across the world. This could happen through the adoption of a General Comment with guidance for states both in the Global North and South. Such a document – along the same vein as the July 2018 CoE Recommendation on Guidelines to respect, protect and fulfil the rights of the child in the digital environment for Europe – could also provide for an impetus to be more specific about the child's right to data protection in regulatory frameworks. Where national data

protection frameworks do not explicitly take the child's best interests into account, states could be motivated to take this up, and in countries where the data protection frameworks already do refer to children, states could be encouraged to evaluate whether the framework is adequate in light of the recent changes in society. As both private and public actors are collecting children's personal data from birth onwards (and sometimes even before) in all parts of the world and globally used technology is facilitating the creation of big data-sets, the development of extremely accurate profiles and automated decision-making, sufficiently detailed regulatory frameworks that include strong safeguards, rights and enforcement mechanisms for children of different ages, should be adopted. Especially with regard to intrusive data processing practices, such as profiling for commercial, political or other reasons that might have a significant and long-term impact on the well-being and rights of the child, restrictions should be considered. Such restrictions should take into account existing evidence, as well as consideration of the precautionary principle, which compels society to act cautiously if there are certain – but not necessarily absolute – scientific indications of a potential danger and if not acting upon these indications could inflict harm (Lievens E, 2010).

Our analysis has shown that data protection frameworks around the world currently still leave considerable room for interpretation for parties processing data as regards their specific obligations towards child data subjects. This leaves an important task to Data Protection Authorities, who should offer guidance to those public and private organisations, as well as provide information to child data subjects and their parents. In a similar vein, child rights ombudsmen or children's rights commissioners could play an important role in helping to ensure that children's rights, including the right to privacy and data protection, are honoured and put into practice, also in relation to the digital environment.

At the same time, measures that aim to protect children's privacy or right to data protection may in certain instances have unforeseen consequences for other rights, such as their right to freedom of expression and association (Lievens E et al., 2018). An example thereof is a situation where teenagers cannot become a member of online communities that might be valuable to them without the consent of their parents for the processing of their data. Therefore, we advocate for a holistic child-rights-oriented approach. This entails that when adopting a new legal or policy measure in the area of privacy and data protection, the impact thereof of on the broadest spectre of children's rights is assessed, for instance through a child rights impact assessment. An essential part of such an assessment consists of the consideration of the child's best interest and the evolving capacities of the child, as prescribed by the UNCRC. Such an approach will underpin forward-looking policymaking that addresses the opportunities and risks for childhood and youth in the digital realm.

7. Bibliography

Article 29 Working Party (2018), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Retrieved from http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

Article 29 Working Party. (2018, April 10). Guidelines on Consent under Regulation 2016/679. Retrieved from http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

Brazilian Statute of the Child and Adolescent 1990, Law No 8069. Retrieved from http://www.planalto.gov.br/ccivil_03/leis/L8069.htm.

Brkan, M and Psychogiopoulou, E (2017), Courts, Privacy and Data Protection in the Digital Environment (Cheltenham: Edward Elgar Publishing).

Children's Act of Ghana 1998, Act 560. Retrieved from

http://www.unesco.org/education/edurights/media/docs/f7a7a002205e07fbf119bc00c8bd3208a438b37f.pdf.

Children's Commissioner. (2017). *Growing up Digital. A report of the Growing Up Digital Taskforce*. Retrieved from https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf.

Children's Commissioner. (2018). *Who knows what about me?* Retrieved from https://www.childrenscommissioner.gov.uk/publication/who-knows-what-about-me/.

Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (C(2012) 5704). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:227:0011:0014:EN:PDF.

Committee of Ministers (2008), Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet. Retrieved from http://childcentre.info/public/protecting_children_on_the_internet.pdf.

Constitution of the Republic of South Africa 1996. Retrieved from http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN005172.pdf.

Council of Europe (2013), Personal data protection: Uruguay becomes first non-European state to accede to 'Convention 108'. Retrieved from https://www.coe.int/en/web/portal/view/-/asset_publisher/vn2ojsz0tUaf/content/personal-data-protection-uruguay-becomes-first-non-european-state-to-accede-to-convention-108-.

Council of Europe (2014), Recommendation CM/Rec (2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users. Retrieved from http://www.azlp.gov.ba/propisi/default.aspx?id=1014&langTag=bs-BA.

Council of Europe (2016), Strategy for the Rights of the Child (2016-2021). Retrieved from https://rm.coe.int/168066cff8.

Council of Europe (2018), Values. Retrieved from https://www.coe.int/en/web/about-us/values

Council of Europe (2018a), Modernisation of Convention 108. Retrieved from https://www.coe.int/en/web/data-protection/convention108/modernised.

Council of Europe (2018b), New Recommendation adopted on children's rights in the digital environment. Retrieved from https://www.coe.int/en/web/children/newsroom/-/asset_publisher/6ZtVCaG3cc7i/content/new-recommendation-adopted-on-children-s-rights-in-the-digital-environment.

Council of Europe (2018c), Recommendation CM/Rec (2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Retrieved from https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808b79f7.

Court of Justice of the European Union (2008), Productores de Música de España (Promusicae) v Telefónica de España [29 January 2008] ECJ C-275/06 ECLI:EU:C:2008:54.

Court of Justice of the European Union (2016), Tele2 Sverige AB [21 December 2016] ECJ C-203/15 and C-698/15, ECLI:EU:C:2016:970.

Data Protection Act of Ghana 2012. Retrieved from https://www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843%29.pdf.

Data Protection Commission of Ghana (2018), Data Protection Act. Retrieved from https://www.dataprotection.org.gh/data-protection-act.

European Court of Human Rights (2008), K U v Finland [2 December 2008] ECtHR Application no 2872/02.

European Court of Human Rights (2008), S and Marper v United Kingdom [4 December 2008] ECtHR Application nos. 30562/04 and 30566/04.

European Court of Human Rights (2012), Axel Springer AG v Germany [7 February 2012] ECtHR App no 39954/08.

European Court of Human Rights (2017), Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland [27 June 2017] ECtHR Application no. 931/13.

European Court of Human Rights (2017, September). Factsheet on the right to the protection of one's image. Retrieved from https://www.echr.coe.int/Documents/FS_Own_image_ENG.pdf.

European Commission (2017), Proposal for an ePrivacy Regulation. Retrieved from

https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

European Parliament Committee on Civil Liberties, Justice and Home Affairs (2017), Draft Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Retrieved from

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-606.011%2b01%2bDOC%2bPDF%2bV0%2f%2fEN

European Parliament Committee on the Internal Market and Consumer Protection (2017), Opinion on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Retrieved from

http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0324&language=EN.

European Union (2007), Consolidated version of the Treaty on European Union.

European Union (2012), Consolidated version of the Treaty on the Functioning of the European Union.

Federal Trade Commission (2013a), Children's Online Privacy Protection Rule ('COPPA'). Retrieved from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

Federal Trade Commission (2013b), FTC Grants Approval for New COPPA Verifiable Parental Consent Method. Retrieved from https://www.ftc.gov/news-events/press-releases/2013/12/ftc-

grants-approval-new-coppa-verifiable-parental-consent-method.

Federal Trade Commission (2015), Complying with COPPA: Frequently Asked Questions. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

Fuster, G G and Gellert, R (2012) The fundamental right of data protection in the European Union: in search of an uncharted right, International Review of Law, Computers & Technology, 26(1), 73-82.

Fuster, G G (2014), The Emergence of Personal Data Protection as a Fundamental Right of the EU (Cham: Springer International Publishing).

Gellman, R (2018), The long and difficult road to a US privacy law. Part 1. Retrieved from https://iapp.org/news/a/the-long-and-difficult-road-to-a-u-s-privacy-law-part-1/.

Global Kids Online (2018), Global Kids Online | Children's rights in the digital age. Retrieved from http://globalkidsonline.net/.

Greenleaf, G (2012), 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108', International Data Privacy Law *2*(2), 68–92.

Holloway, D and Green, L (2016), 'The Internet of toys', Communication Research and Practice *2*(4), 506–519.

ICT Kids Online Brazil: Survey on Internet Use by Children in Brazil 2016 (2017) (Sao Paulo). Retrieved from

http://cetic.br/media/docs/publicacoes/2/TIC_KIDS_ONLINE_2016_LivroEletronico.pdf.

Information Commissioner's Office (2017), Consultation: Children and the GDPR guidance. Retrieved from https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf.

Koops, B J, Newell, B C, Timan, T, Škorvánek, I, Chokrevski, T and Galič, M (2017), 'A Typology of Privacy', University of Pennsylvania Journal of International Law 38(2): 483-575 .

Law on the Protection of Personal Data of Uruguay 2008. Retrieved from

http://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html.

Lievens, E (2010) Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments (Leiden / Boston: Martinus Nijhoff Publishers).

Lievens, E, Livingstone, S, McLaughlin, S, O'Neill, B, and Verdoodt, V (2018), Children's rights and digital technologies, 1–27, in: Kilkelly, U and Liefaard, T. (Eds) International Human Rights of Children (Singapore: Springer).

Livingstone, S (2014), Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile. Retrieved from http://eprints.lse.ac.uk/60513/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU%20Kids%20Online-Children%27s%20online%20risks_2014.pdf.

Livingstone, S (2015), No more social networking for young teens? Retrieved from http://blogs.lse.ac.uk/mediapolicyproject/2015/12/18/no-more-social-networking-for-young-teens/.

Livingstone, S (2018), 'Children: A Special Case for Privacy?', InterMEDIA Vol 46 (2). Retrieved from http://www.iicom.org/intermedia/intermedia-july-2018/children-a-special-case-for-privacy.

Livingstone, S, Carr, J and Byrne, J (2015), One in Three: Internet Governance and Children's Rights. Global Commission on Internet Governance, Centre for International Governance Innovation and the Royal Institute of International Affairs. Retrieved from https://www.cigionline.org/sites/default/files/no22_2.pdf.

Livingstone, S, Lansdown, G and Third, A (2017), The Case for a UNCRC General Comment on Children's Rights and Digital Media. Children's Commissioner for England. Retrieved from https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Case-for-general-comment-on-digital-media.pdf.

Livingstone, S and O'Neill, B (2014), 'Children's rights online: challenges, dilemmas and emerging directions', 19–38, in van der Hof, S, van den Berg, B and Schermer, B, (eds) Minding Minors Wandering the Web: Regulating Online Child Safety (The Hague: Springer with T. M. C. Asser Press).

Lupton, D and Williamson, B (2017), 'The datafied child: The dataveillance of children and implications for their rights', New Media & Society 19(5), 780–794.

Makulilo, A B (Ed.) (2016), African Data Privacy Laws (Cham: Springer International Publishing).

Milkaite, I and Lievens, E (2018), GDPR: updated state of play of the age of consent across the EU, June 2018. Retrieved 11 July 2018, from

https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751.

Milkaite, I, Verdoodt, V, Martens, H, and Lievens, E (2017), The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society. Roundtable Report. Retrieved from https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf.

Montgomery, K C and Chester, J (2015), 'Data Protection for Youth in the Digital Age: Developing a Rights-based Global Framework', European Data Protection Law Review 1(4), 277–291.

Montgomery, K C, Chester, J and Milosevic, T (2017), 'Ensuring young people's digital privacy as a fundamental right', 85–102, in De Abreu, B S, Mihailidis, P, Lee, A Y L, Melki, J and McDougall, J (eds) International Handbook of Media Literacy Education (New York: Routledge).

Ofcom (2008), Social Networking. A quantitative and qualitative research report into attitudes, behaviours and use.

OECD (2011), Thirty years after the OECD privacy guidelines. Retrieved from http://www.oecd.org/sti/ieconomy/49710223.pdf.

Pallero, J and Tackett, C (2018), Brazil president approves data protection bill — but vetoes key accountability measures. Retrieved from https://www.accessnow.org/brazil-president-approves-data-protection-bill-but-vetoes-key-accountability-measures/.

Protection of Personal Information Act of South Africa (2013). Retrieved from http://media.mofo.com/files/PrivacyLibrary/3789/Protection-of-Personal-Information-Act-4-of-2013.pdf.

Robinson, N, Graux, H, Botterman, M and Valeri, L (2009), Review of EU data protection directive: summary. Information Commissioner's Office. Retrieved from https://ico.org.uk/media/about-the-

ico/documents/1042347/review-of-eu-dp-directive-summary.pdf.

Roos, A (2016), 'Data Protection Law in South Africa', 189–227, in Makulilo, A B (ed) African Data Privacy Laws (Cham: Springer International Publishing).

Senado Federal (2018), Brazilian General Data Protection Act No 13.709 of 14 August 2018. Retrieved from http://legis.senado.leg.br/legislacao/DetalhaSigen.action?id=27457334.

Tabor, A J (2013), Imperium, LLC Proposed Verifiable Parental Consent Method Application. Retrieved from https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf.

UNICEF (2017), The State of the World's Children 2017. Children in a Digital World. Retrieved from

https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf.

United Nations Committee on the Rights of the Child (2016), General comment No. 20 on the implementation of the rights of the child during adolescence, https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f20&Lang=en.

United Nations General Assembly (1989), Convention on the Rights of the Child, Treaty Series, Vol. 1577, p. 3.

van der Hof, S, & Lievens, E (2018), 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(1). Retrieved from https://papers.ssrn.com/abstract=3107660.

Verdoodt, V, & Lievens, E. (2017), Targeting children with personalised advertising: how to reconcile the best interests of children and advertisers. In G. Vermeulen & E. Lievens (Eds.), Data Protection and Privacy Under Pressure: Transatlantic tensions, EU surveillance, and big data (Antwerp: Maklu).

Warren, S and Brandeis, L (1890), The right to privacy, Harvard Law Review, 4(5), 193-220

Zarouali, B, Ponnet, K, Walrave, M and Poels, K (2017), "Do you like cookies?" Adolescents' sceptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing, Computers in Human Behavior, 69, 157-165.

Acknowledgement

This article presents research findings from the project "A children's rights perspective on privacy and data protection in the digital age: a critical and forward-looking analysis of the General Data Protection Regulation and its implementation with respect to children and youth" (Ghent University, Special Research Fund).

---

[1] Ingrida Milkaite (Law & Technology, Ghent University) and Eva Lievens (Law & Technology, Ghent University)

[2] In addition, it can be noted that the countries that have been investigated are also included in the Global Kids Online research project. Global Kids Online is an international research project which collects international evidence on children's internet use and relies on a global network of researchers and experts (Global Kids Online, 2018). The research data provide academics, policy makers and industry stakeholders with an evidence base on the opportunities, risks and protective factors of children's internet use. For more information, see http://globalkidsonline.net/.

[3] An (unofficial) English version of the Brazilian Law was used by the authors and can be found at https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf

[4] Provided that a child (or an adolescent) is considered any person under 18, as defined by the Brazilian Internet Law No. 12.965 of 23 April 2014 or by the United Nation Convention on the Rights of the Child (article 1), which Brazil ratified in 1990.

[5] Cf. footnote 1.

[6] The sections of the Act that have come into force are the ones concerning the definitions of the law, the establishment of the Regulator, the provisions granting the Minister the authority to adopt regulations and procedures for making regulations (Roos, 2016).

[7] The responsible party is defined by the Act as a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information (Chapter 1, definitions).