6

Digital vulnerabilities and the privacy conundrum for children in the digital age: Lessons for Africa

Hlengiwe Dube

Abstract

In contemporary society, technology has become an indispensable facet of childhood experience, with a growing number of children engaging extensively with digital technologies. Despite this pervasive trend, a significant digital divide and exclusion persists, particularly in the African context, primarily attributed to economic disparities, rendering numerous children devoid of internet connectivity and digital resources. For the connected, the digital age has substantially shaped their experiences, yielding both favourable and adverse consequences. The positive impact is evident in the augmentation of their independent development and other benefits stemming from digital engagement. However, this positive trajectory is accompanied by a concerning dimension wherein children, while utilising and deriving benefits from the internet, are increasingly susceptible to exploitation on online digital platforms. As technology becomes increasingly pervasive and sophisticated, children's vulnerability to online harms escalates concomitantly with their engagement in diverse digital technologies. These online risks encompass child grooming, the improper use of personal information, cyberbullying, sexual exploitation, manifestations of depression and anxiety, exposure to inappropriate content, and the ominous threat of child trafficking. Preserving children's privacy in the digital age emerges as a complex challenge with a nuanced interplay between child protection and autonomy. The paradox inherent in child protection and autonomy presents a nuanced challenge. Conventional wisdom holds that parental guidance serves as the conduit for fostering children's well-being and developmental growth. However, the imperative acknowledgment of children's autonomous existence necessitates careful consideration. Despite the prominence of discourse on children's rights in the Global North, such discussions remain relatively novel in Africa, lacking sufficient attention in Africa. This chapter explores the vulnerabilities experienced by children as active participants in the digital age and elucidates the implications for their privacy.

1 Introduction

Digital and mobile penetration rates are on the rise in Africa, coinciding with the continent's embrace of the fourth industrial revolution (4IR).

According to the International Telecommunication Union (ITU), there was a notable 21 percent increase in the deployment of the 4G networks in 2020. Statistics from the same year reveal that 40 percent of the younger demographic, aged 15 to 24, were using the internet.[1] As the surge of internet penetration continues, children and young people now constitute a significant proportion of the interconnected society. These technological advancements wield a profound impact on children's rights.[2] Notably, children develop a digital identity and digital footprint from very early on, and sometimes preceding their birth.[3] This technology evolution is underscored by children's active social media presence where they have profiles, share their experiences, perspectives and other forms of personal information.

The digital space and technology have many attributes that are beneficial to the development of children. Technologies in this regard encompass the internet, artificial intelligence (AI), robotics, big data, algorithms, information, and communication technologies (ICTs). Considering the demographic prevalence of children in the Global South and Africa, a discernible trend emerges, suggesting a potential surge of children as internet users and assuming a dominant role in shaping the digital landscape.[4] The advent of the COVID-19 pandemic and the imposed lockdowns in response to the pandemic prompted a shift to the digital world and resulted in the escalation of children using digital technologies for recreational and education purposes. Their screen time increased significantly, notwithstanding their limited knowledge of and skills for ensuring their online safety. The United Nations Children's Fund (UNICEF) underscored the potential risks, noting that 'spending more time on virtual platforms can leave children vulnerable to online sexual

[1] International Telecommunication Union 'Measuring digital development: Facts and figures' (2020), https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf (accessed 16 June 2022).

[2] A Third and others 'Recognising children's rights in relation to digital technologies: Challenges of voice and evidence, principle and practice' in B Wagner and others (eds) *Research handbook on human rights and technology* (2019) 378. The digital age is contributing significantly to the hurdles that hinder the fulfilment of the rights of the child: privacy complications; discriminatory emerging technologies such as artificial intelligence (AI); novel forms of sexual abuse and exploitation; Networked participation and education; and many more.

[3] United Nations Human Rights Office of the High Commissioner 'Children's right to privacy in the digital age must be improved' (15 July 2021), https://www.ohchr.org/en/stories/2021/07/childrens-right-privacy-digital-age-must-be-improved (accessed 15 March 2022). Parents or other family members share their images on online platforms.

[4] Third and others (n 2) 376.

exploitation and grooming'.[5] In contrast to Europe, the United States and Canada, most African countries exhibit a comparatively lesser emphasis on issues related to child online safety.

Children engage with a myriad of digital technologies including virtual assistants, wearable devices, smartphones, and interactive toys, thereby significantly influencing their childhood, both positively and negatively. This integration of technologies into their lives fosters their participation, augments learning outcomes, enhances access to information, facilitates social interaction, and also recreational purposes. This multifaceted role of technology in children's experience enables them to explore their creativity and empowers them to freely express themselves. Notably for children with disabilities, technology emerges as a mechanism for dismantling, providing them an avenue to access education among other benefits. However, as children navigate a digitised world and interact with technologies, they are exposed to inherent risks and potential harms that could be detrimental to their well-being and undermine their ability to fully harness the advantages of a networked world.

Children are exposed to violence, harmful and inappropriate content, and manipulation of their personal information.[6] The harmful content encompass that of a sexual nature, non-consensual engagements such as sexting, instances of online sexual abuse and harassment and cyberbullying.[7] Also, in the cyberspace, children are susceptible to radicalisation and exploitation by non-state actors such as terrorist groups and extremists. Through these liaisons, children are prompted to engage in detrimental behaviours including acts of violence.[8] Children may also use technology to utter proclamations that disparage or denigrate others based on unique aspects of their individuality or collective identity such as sexual orientation, religion, nationality, race, economic background, political affiliation, ethnicity and sex/gender. They may also generate or disseminate malicious or spiteful content targeted at particular demographic categories.

[5] UNICEF 'Children at increased risk of harm online during global COVID-19 pandemic – UNICEF' (20 April 2020), https://www.unicef.org/southafrica/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic-unicef (accessed 16 June 2022).

[6] IR Berson & MJ Berson 'Children and their digital dossiers: Lessons in privacy rights in the digital age' (2006) 21 *International Journal of Social Education* 136.

[7] Third and others (n 2) 378. '[T] he internet is generally designed for adults … the internet is age-blind.'

[8] General Comment 25 para 83.

The digital and data economy has undergone exponential growth, resulting in substantial personal information being stored in digitised formats.[9] This underscores the aforementioned vulnerability of children considering their limited knowledge and capacity to control the processing of their personal information. A significant volume of their data is being processed, including collection, storage, transfers and re-purposing, without their knowledge or informed consent. In the African context, data protection mechanisms are still nascent,however, this immature and transitional phase children's vulnerabilities are exacerbated. The right to privacy is a fundamental right that is enshrined in international human rights law and standards. It is not an absolute right and any interference should be proportionate, legitimate, necessary and serve a legitimate purpose. In addition to this international law position, any limitations to children's privacy should be consistent with the principle of data minimisation and prioritise the best interests of the child.[10]

The challenges faced by children infringe on their rights that are enshrined in international human rights law and standards. Ample international human rights instruments and other standard setting documents address children's rights and can also be applied to the digital context. Prominent among these are the United Nations (UN) Convention on the Rights of the Child (CRC)[11] and the African Charter on the Rights and Welfare of the Child (African Children's Charter),[12] serving as the main instruments codifying children rights in Africa. Specifically, on the digital age, UN General Comment 25 on children's rights in relation to the digital environment elucidates the implementation of the CRC and its optional protocols in a digital context. It further provides guidance to ensure compliance with obligations on children's rights.[13] The African Committee of Experts on the Rights and Welfare of the Child (African Children's Committee) also adopted a resolution on the protection and promotion of children's rights in the digital sphere within the African context.[14]

[9] Berson & Berson (n 6) 136.

[10] See General Comment 25 para 69.

[11] United Nations Convention on the Rights of the Child, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (accessed 15 March 2022).

[12] African Charter on the Rights and Welfare of the Child, adopted in 1990 and came into force in 1999, https://au.int/en/treaties/african-charter-rights-and-welfare-child (accessed 15 March 2022).

[13] General Comment 25 on Children's rights in relation to the digital environment, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation (accessed 17 March 2022).

[14] African Children's Committee 'Resolution on the Protection and Promotion of

The objectives of this chapter are twofold. The first objective is to highlight the risks encountered by children in online engagements. The second objective is to underscore the intricate privacy conundrum inherent in children's digital interactions. Central to the overarching argument of this chapter is the contention that children's privacy in the digital environment constitutes a critical concern meriting earnest consideration. However, children's privacy should be evaluated from a broader perspective of the digital space that is riddled with hazards that threaten their safety and privacy. In examining the obligations of states, the efficacy of the existing legislation is examined. The initial segment of the chapter examines the vulnerability of children in the digital environment, while the second part considers the privacy aspect, exploring the diverse ways in which the digital environment impacts children's privacy. The third part examines the existing legal frameworks and practices for child protection and privacy. Subsequently, the chapter considers commendable practices from other contexts and examines selected approaches that Africa could potentially adopt. The chapter concludes with proposed recommendations and conclusions designed to enhance online safety of children and enhance their privacy in the African context.

2 Digital risks encountered by children in the digital age

This segment explores the digital risks confronted by children in the digital environment. The focus on the online risks is important as any discourse on children's privacy should also take into account the inherent harms associated with the digital environment, which necessitates a delicate balance between privacy and protection. The digital space has ushered in new avenues for perpetrating violence against children, resulting in dual violation of their rights, both offline and online.[15] Children are also susceptible to online predatory behaviour by online abusers, who are either their peers or adults.[16] Violence against children online manifests in physical and emotional forms and examples include sexual abuse and exploitation, cyberbullying, and the abuse of personal information. Notably, during crisis episodes such as pandemics, networked children's online presence increases and the risk of harm online also escalates.[17]

Children's Rights in the Digital Sphere in Africa' (17 March 2022), https://drive.google.com/file/d/1WhBF7HGfvyTyxWJmkGsHuavnJhZMrDdd/view (accessed 15 March 2022).

[15] Berson & Berson (n 6) 142. See also General Comment 25 para 80.

[16] African Children's Committee (n 14).

[17] General Comment 25 para 80. In response to changes brought about by the COVID-19 pandemic, the African Children's Committee noted that 'countries have adapted to digital learning methods and this may expose children to online child

These risks can 'severely harm their mental and emotional health and physical well-being' and limit a child's development and also potentially affect their adolescence and adulthood.[18] The risks under consideration are related to conduct, content and contact, each impacting on children's safety and privacy.

2.1 Cyberbullying

Exposure of children to bullying is not novel and they experience it as either victims or perpetrators. This chapter considers cyberbullying, denoting bullying which occurs through electronic means.[19] Considered as one of the main threats to children in the digital sphere, cyberbullying may be perpetrated by and among children themselves.[20] Cyberbullying is linked to the way children conduct themselves online, with other children or adults. It can manifest in the use of digital technologies including social media, instant messaging, email or texts, to propagate hurtful behaviour. It involves sending images such as pictures and videos with insults, false information or threats about the targeted victim who may either be included or excluded from the communication. The behaviour can be once-off or recurrent and is necessitated by an existing 'power imbalance between the perpetrator and victim'.[21] Notably, there is a correlation between online and offline cyberbullying, wherein offline incidents and behaviours could migrate to the online space to victimise other children.[22] Due to the electronic medium, cyberbullying has an extensive audience and reach, magnifying its impact.[23] Its consequences can be tragic and there is a higher propensity for victims of cyberbullying contemplating

sexual exploitation and abuse'. See African Children's Committee 'Guidance note on children's rights during COVID-19' (8 April 2020), https://www.acerwc.africa/guiding-note-on-childrens-rights-during-covd-19/ (accessed 18 March 2022). See also African Children's Committee (n 14).

[18] OHCHR (n 3).

[19] RR Calvoz and others 'Constitutional implications of punishment for cyber bullying' (2014) *Cardozo Law Review* 105.

[20] MG Vallejo and others 'Kids and parents privacy exposure in the internet of things: How to protect personal information?' (2018) 22 *Computación y Sistemas* 1196.

[21] UNICEF M Stoilova and others 'Investigating risks and opportunities for children in a digital world' (February 2021) 38, https://www.unicef-irc.org/publications/pdf/Investigating-Risks-and-Opportunities-for-Children-in-a-Digital-World.pdf (accessed 5 April 2022).

[22] Stoilova and others (n 21) 39.

[23] R Slonje & PK Smith 'Cyberbullying: Another main type of bullying?' (2008) 49 *Scandinavian Journal of Psychology* 147-154.

suicide.[24] Although there are no figures for South Africa, there is a significant occurrence of cyberbullying among children in the country.[25]

Cyberbullying exhibits gender-specific variations, with a higher probability of boys being perpetrators and girls being victims.[26] Girls are often targeted on the basis of their physical appearance or sexuality, thereby exerting a profound impact on their reputation and dignity. Such consequences may potentially exacerbate their vulnerability to social exclusion and escalate or perpetuate the ongoing abuse.[27] Due to the appearance based focus, social media becomes a predominant channel for girls' harassment. Conversely, boys experience cyberbullying differently, often associated with playing video games and messaging via mobile phones.

Several factors contribute to the occurrence of cyberbullying including perceptions around violence, a lack of empathy, an exaggerated sense of self-importance and desire for popularity, and diminished self-efficacy tendencies.[28] Vulnerable demographics such as children of single parents, those with disabilities, those who suffer from social anxiety and those from economically disadvantaged school backgrounds are more susceptible to online bullying.[29] The protection landscape against bullying is increasingly becoming more complex. For instance, a child's home usually was their traditional place of safety where they could evade school or neighbourhood bullies. However, in the digital realm, exacerbated by the proliferation of social media presence, bullies transcend the physical barriers of protection, leaving victims without places of solace.[30]

In the context of cyberbullying, the issue of privacy is notably intricate given the possibility of cyberbullying occurring in anonymity or facilitated by use of stolen identities, posing substantial complications to formulating interventions to remedy the victims' situation.[31] In this conundrum, the elusive nature of cyberbullying intensifies the possibility of privacy infringements for the victims due to their susceptibility to

[24] M Laubscher & WJ van Vollenhoven 'Cyberbullying: Should schools choose between safety and privacy?' (2015) 18 *Potchefstroom Electronic Law Journal* 2219.

[25] As above.

[26] Stoilova and others (n 21) 39.

[27] As above.

[28] As above.

[29] As above.

[30] UNICEF 'The state of the world's children 2017: Children in a digital world' (2017) 21, https://www.unicef.org/media/48601/file.

[31] Laubscher & Van Vollenhoven (n 24) 2234.

unwarranted exposure, particularly concerning sensitive information, further compounding the challenges associated with finding solutions to mitigate the far-reaching impact of cyberbullying.

2.2 Exposure to inappropriate content

The content under consideration encompasses discriminatory, sexual, pornographic, hateful, violent or racist expressions. This kind of content can also depict certain behaviours that are detrimental to the well-being of children including instances of self-harm, suicide, eating disorders, gambling, hacking, as well as hurtful and bullying behaviour.[32]

2.3 Sexual risks and Exploitation

Children are increasingly exposed to various sexual activities in the digital space, including engaging in cybersex, and the consumption or exchange of sexual content.[33] Concurrently, the digital environment also exposes them to sexual abuse and exploitation. Cyber sexual exploitation and abuse, a manifestation of digitally-facilitated child sexual abuse entails generating and disseminating child sexual abuse materials; child prostitution; solicitation of sexual acts from minors; threats to a child's reputation; bullying; and the encouragement of children to engage in self-harming behaviours such as suicidal tendencies.[34] Such malevolent acts, typically perpetrated by online sex predators, stem from exploitation of trust established in interactions with minors online. Another disconcerting and prevalent manifestation is online intimate partner violence, a technology-assisted form of violence that manifests in forms of control such as harassment and stalking in the context of a friendship or a pre-existing relationship. Notably higher prevalence of this form of violence is exhibited among teenage girls.[35]

2.4 Exchange of sexual content (sexting)

Sexting is the exchange of sexually explicit content including videos, messages and images through internet-based platforms or mobile phones. While sexting is not inherently risky and can be consensual. It is normal and common behaviour associated with a child's development, particularly during adolescence. At this stage, teenagers engage in sexting as they explore relationships and their sexuality. The initiation and

[32] UNICEF (n 30).

[33] Stoilova and others (n 21) 45.

[34] General Comment 25 para 81.

[35] Stoilova and others (n 21) 56.

frequency depends on the child's socio-economic status, age, gender and sexual orientation. It is common among teenagers in general and more prevalent among those in the lesbian, gay, bisexual, trans and gender diverse, intersex and queer (LGBTIQ) demographic. Also, the inclination to coerce partners to share sexual content is more pronounced among older children, particularly boys, as compared to the younger ones.[36]

While it is common in digital communication, sexting is inherently associated with risks that include non-consensual transmission of sexual content, sexual bullying harassment and non-consensual dissemination of intimate information.[37] The probability of girls having negative experiences arising from sexting is high, whereas boys' vulnerability is lower.[38] Risks associated with children's experiences while exchanging sexual content online include privacy infringements; compromised online safety; sexual solicitations by adults; sexual grooming; and adverse psychological consequences.[39] For instance, non-consensual sharing of images has detrimental effects on the victim's privacy and reputation, often culminating in stigmatisation or slut-shaming.[40]

2.5 Viewing sexual content online

Engaging with sexual content online involves consumption of sexually-explicit videos or images. Such exposure could be intentional or accidental, with a prevailing curiosity rooted in the quest for sexual knowledge.[41] Notably, there are gender disparities with boys exhibiting more interest in this type of content compared to girls. Although parental involvement can shield children from such exposure, children can circumvent parental control barriers to gain access to explicit content. Additionally, children also exhibit deceptive tendencies and falsify their age information to enable them to access content that is not age-appropriate for them.[42] The ramifications for such exposure, includes engaging in sexting with strangers or unwarranted sexual solicitation by strangers.[43] Consequences

[36] Stoilova and others (n 21) 46.

[37] Stoilova and others (n 21) 45.

[38] As above.

[39] Stoilova and others (n 21) 45.

[40] Stoilova and others (n 21) 46.

[41] Stoilova and others (n 21) 48.

[42] Pew Research Centre A Lenhart and others 'Teens, kindness and cruelty on social network sites' (9 November 2011) https://www.pewresearch.org/internet/2011/11/09/teens-kindness-and-cruelty-on-social-network-sites/ (accessed 26 June 2022).

[43] Stoilova and others (n 21) 48.

are multifaceted and extend beyond the digital sphere, manifesting as psychological effects, social withdrawal during internet disconnection and occasional sleep disturbances.[44]

2.6 Contact with online predators

Online predators adeptly assume deceptive personas and strategically target online platforms commonly accessed by children. The initial encounter with the perpetrator could be either online or conventional offline interactions.[45] Predators establish interactions with minors and cultivate illusions of genuine friendships to foster a sense of trust. There is a perilous possibility of online liaisons culminating in in-person relationships.[46] In these orchestrated liaisons, there is a risk of minors being manipulated into divulging sensitive personal information, including contact details and location data. This surreptitious exchange of information often transpires without the parents' knowledge, thereby impeding their ability to protect their children from potential online threats including those posed by predatory individuals. The prospect and nature of exploitation are contingent upon factors such as a child's age, socio-economic background, gender, and other pertinent considerations.[47]

Online predators manipulate minors to perform sexual acts online.[48] The exposure of children to offline or online abuse, orchestrated by adults or their peers could propel them to engage in more risky activities including communicating with strangers and sharing personal information. Also, children's immersion in online platforms and the nature of their liaisons could potentially steer them towards exploring sexual activities that expose them to abuse and exploitation.[49] Older adolescent girls are more predisposed to victimisation as compared to younger ones, both girls and boys.[50] Additionally, LGBTIQ minors are also susceptible to such risks. While parental guidance and mediation play a crucial role in assisting victimised children, the efficacy of this intervention may be undermined by children's failure to recognise the precarious nature of their situation and consequently refrain from seeking the requisite assistance.[51]

[44] As above.

[45] As above.

[46] General Comment 25 para 81.

[47] As above.

[48] As above.

[49] Stoilova and others (n 21) 51.

[50] Stoilova and others (n 21) 50.

[51] As above.

2.7 Online sexual solicitation of children (child grooming)

Online sexual solicitation of children, commonly referred to as grooming, involves the establishment of inappropriate offline and online relationships between a minor and an adult for the purposes of sexual conduct.[52] This form of child exploitation manifests in various forms including coaxing children to engage in sexual acts or share personal sexual information in virtual platforms such as social media, email or though texting.[53] Predominantly, the targeted children exhibit behaviours such as intense involvement in online gaming, forming friendships with strangers, consuming sexually explicit content, oversharing personal information on the internet, willingly participating in sexting, particularly with strangers, and generally spending extensive periods online, especially during weekends. Notably, a correlation exists between online and offline vulnerabilities, wherein perpetrators may either be acquainted with their online targets or, more commonly, remain strangers.[54] Children who have experienced offline abuse, encompassing sexual exploitation, neglect, physical punishment, or psychological torment, demonstrate an increased susceptibility to succumb to online sexual solicitation.[55] It is crucial to acknowledge the role of social support in mitigating the impact of such abuse, as those lacking such assistance face heightened vulnerability, leading to potential self-harm.

2.8 Sextortion

This involves coercive threats of disseminating sexual images without the owner's consent, is a common issue driven by motives associated with revenge or financial gain and it primarily manifests in pre-existing relationships or friendships. Sextortion exhibits a notable prevalence of male involvement, whether as victims or perpetrators. Furthermore, empirical evidence suggests a disproportionate impact on non-heterosexual individuals, irrespective of their age or racial background.[56]

This section of the chapter extensively explores the adversities confronted by children in their digital experience. As succinctly conveyed by Bush, 'kids are too immature to deal with blackmail, extortion, revenge porn, stalking, being hounded down for nudes, cyberbullying,

[52] African Children's Committee General Comment 7 para 70. Child sexual online grooming is common among children between 13 and 17 years of age, mainly girls.

[53] Stoilova and others (n 21) 51.

[54] Stoilova and others (n 21) 52.

[55] As above.

[56] As above.

being socially excluded, and so much more. Kids can't deal with these issues in the real world, let alone the online world.'[57] The contention posited is that, owing to their inherent immaturity, children struggle to navigate these complex issues in both the physical and digital spheres. The subsequent discussion underscores the intrinsic link between these digital perils and the erosion of trust in technology, thereby prompting parental intervention to safeguard their children. This encroachment on the private online domain of minors is scrutinised in the subsequent segment of this chapter.

3 Privacy implications of children's interaction with technology in Africa

As previously indicated, internet connectivity has significantly improved in Africa, thereby facilitating increased access to social media. Consequently, heightened consideration is warranted for the privacy discourse, given the implications of internet connectivity, particularly concerning children, a focus that has received comparatively less attention.[58] In Africa the discourse on privacy is gaining traction but still is at nascent stages and yet to attain full societal recognition. The inherent complexity of technology, coupled with the omnipotence of technology-based innovations, dundermines individuals' ability to exercise adequate control over their personal information and protect their privacy.

Information processing has evolved significantly, advancing in sophistication and occurring at unprecedented speeds. Additionally, the digital ecosystem is predicated on continuous user monitoring and data processing, presenting an imminent threat to privacy. This transformation is enabled by the emergence of big data and other emerging technologies that facilitate the processing of vast datasets through intricate mechanisms designed for the storage, analysis, and manipulation of information. These technological advancements find application in diverse domains such as surveillance, marketing, and profiling.

[57] N Bush 'Cyberbullying, social media and compulsive gaming' (24 March 2022) *IOL*, https://www.iol.co.za/thepost/features/cyberbullying-social-media-and-compulsive-gaming-38e6ca99-f507-4865-91d4-57ebd0d0643c (accessed 26 June 2022).

[58] K Goldstein 'I'm a mom and a children's privacy lawyer: Here's what i do and don't post about my kid online' (17 May 2022), https://www.parents.com/kids/safety/internet/im-a-mom-and-childrens-privacy-lawyer-what-i-do-and-dont-post-online/ (accessed 12 April 2022).

The digital lifestyles entail documenting and sharing experiences and information, extending to the context of children.[59] Also, in contemporary networked societies, routine practices include mandatory identity verification, mass surveillance,[60] profiling, automated data processing, behavioural targeting, and filtering are now ordinary practices.[61] Beyond the realm of families sharing information, public and private institutions actively process children's information. The processed information includes children's emotions, activities, location, relationships, identities, communication, academic performance, gender, race, health and biometric data, all of which can uniquely identify them. This processing is undertaken for purposes related to education, health, and various other societal considerations.[62]

There is a correlation between privacy and the digital risks that have been articulated. Privacy intrusions can impact negatively on the identity and reputation of individuals. Generally, children are not concerned about their digital footprint and the privacy implications in comparison to adults. Consequently, there is a tendency for lower levels of privacy management and the implementation of safety strategies among children. While possessing some requisite skills, children may not consistently apply them.[63] It is imperative to redirect attention towards enhancing privacy management and fostering media and digital literacy among the younger demographic. The illicit processing of information is an indisputable reality, imperilling the privacy of children, a domain that should be held as sacrosanct as that of adults. Of particular concern is the manipulation and non-consensual dissemination of information.

[59] J Gligorijevic 'Children's privacy: The role of parental control and consent' (2019) 19 *Human Rights Law Review* 202.

[60] See General Comment 25 para 75, which states that obligations on mass surveillance and children's privacy require that '[a]ny digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver; nor should it take place without the right to object to such surveillance, in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose'. In the case of tracking devices and monitoring a child's digital activities, such measures should take into account the evolving capacities of the child, serve the best interests of the child and proportionate. See para 76 General Comment 25.

[61] General Comment 25 para 68.

[62] General Comment 25 para 67. Eg, state and private sector surveillance and transactional data collected by commercial actors. See Third and others (n 2) 387.

[63] Stoilova and others (n 21) 31. As a result of their higher levels of vulnerability, girls are more likely to be concerned about their privacy and adopt better privacy behaviour than boys.

Although considerable progress has been made in interpreting the right to privacy, the inclination in the context of children tends to prioritise parental control and child protection, which overshadows the imperative of safeguarding the child's privacy.[64] Globally, incidents of online risks and privacy infringements against children have become prevalent, necessitating an augmented call for prompt intervention.[65] This section of the chapter delves into pivotal facets of privacy in children's online information, encompassing parental responsibility, the phenomenon of "sharenting"; children's online behaviours that pose risks to their privacy; the conundrum of privacy and data protection in the education sector; and the privacy ramifications arising from the advent of emerging technologies such as artificial intelligence (AI).

3.1 Parental guidance in relation to child autonomy and privacy

Parental responsibility is a recognised mechanism that chaperones children throughout their development stages. It includes a broad spectrum of roles such as providing guardianship, care, offering the necessary support and maintaining contact and communication with the child. According to Du Toit, 'parents are key parts of the immediate "eco-system" of a child and are critical in a healthy development of the child, including the functioning and progress of the child'.[66] The concept of parental responsibility is recognised under international human rights. Article 5 of CRC states:[67]

> States Parties shall respect the responsibilities, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention.

Although privacy is a fundamental right, it is not absolute and can be limited. In the context of children, parental responsibility emerges as a potential limiting factor; however, the precise extent of this limitation remains ambiguous. Striking an optimal balance between a child's autonomy and parental responsibility is imperative to prevent parents and guardians from

[64] Gligorijevic (n 60) 202.

[65] Third and others (n 2) 391-403.

[66] T du Toit 'Cyber bullying dilemma: A case for ubuntu', 'https://rm.coe.int/cyberbullying-dilemma-a-case-for-ubuntu-by-thersia-du-toit-smit-nation/1680a30051 (accessed 18 June 2022).

[67] Art 5 CRC; also arts 3, 18 & 19.

exerting absolute control that could impede the child's developmental trajectory. When courts adjudicate matters pertaining to a child's privacy, it becomes essential to elucidate the impact of parental behaviour on the child's privacy. This should be done without reproaching parents for their parenting choices or positioning courts as moral adjudicators arbitrating what constitutes commendable or acceptable parenting practices.[68]

Parental responsibility should be exercised with unwavering commitment to the best interests of the child, a cardinal principle underpinning the safeguarding and advancement of children's rights.[69] In the context of children's privacy within the purview of parental responsibility, there seems to be a *lacuna*. It is generally recognised that children cannot be left entirely to navigate their developmental journey autonomously. Justifiable limitations on their autonomy are crucial to shield them from potential harm, whether directed towards others or themselves.[70] In this regard, as children increasingly access the online sphere, parents assume a 'supervisory and guardianship role'.[71] This Is an indispensable role for regulating a child's digital lifestyle, mitigating the risks of online harms. Parental involvement assumes paramount importance, facilitating a nuanced understanding of their children's online behaviour and offering requisite guidance when feasible.[72] This form of surveillance has become an integral aspect of contemporary parenting in the digital age.

There is a genuine concern for the safety of children that drives parents to infringe on children's privacy and monitor their digital habits.[73] As highlighted earlier, children are susceptible to cyberbullying, exposure to inappropriate content, and exploitation by online predators, including incidents of sexual abuse. Additionally, children may utilise digital channels to engage in illicit behaviour such as drug distribution and

[68] Gligorijevic (n 60) 205.

[69] Art 3 CRC.

[70] Laubscher and Van Vollenhoven (n 24) 2231.

[71] Humanium 'Children's rights and digital technologies: Children's privacy in the age of social media – The perils of "sharenting"' (26 January 2021), https://www.humanium.org/en/childrens-rights-and-digital-technologies-childrens-privacy-in-the-age-of-social-media-the-perils-of-sharenting/ (accessed 26 June 2022).

[72] MacAfee 'America's youth admit to surprising online behavior, would change actions if parents were watching' (4 June 2013), https://www.businesswire.com/news/home/20130604005125/en/America%E2%80%99s-Youth-Admit-Surprising-Online-Behavior-Change (accessed 26 June 2022).

[73] C Null 'I monitor my teens' electronics, and you should too' (27 January 2020) *WIRED*, https://www.wired.com/story/parents-should-monitor-teens-electronics/ (accessed 20 June 2022).

organising of gathering with explicit sexual content, commonly referred to as sex parties. Parents perceive these as serious concerns, thus superseding considerations of privacy. The capacity of children to make regrettable decisions online underscores the necessity of employing monitoring applications and devices as essential tools for ensuring their safety and potentially saving lives.[74]

The paramount motivation behind the monitoring of children's online and offline activities is the ardent desire to safeguard them from potential harm in the digital realm. The perils associated with children's digital experiences have been extensively elucidated in the preceding section of this chapter. Parents and caregivers, grappling with an inherent ambivalence towards the digital space and the myriad risks it poses to children, are inclined towards privacy-intrusive behaviours and heightened restrictions.[75] Parents feel that they have effectively exercised their duty to care in the digitised world when they monitor their children's online activities. The online monitoring is perceived as an extension of the vigilant supervision exercised in offline settings. Consequently, parents find assurance in the belief that they have fulfilled their moral responsibility, thereby ensuring the safety and well-being of their children.

The digital sphere introduces an additional layer of vulnerability for children, particularly those who are already susceptible, such as those with disabilities. For these children, the access and utilisation of assistive technology signify a transformative experience, rendering achievable what would otherwise be deemed unattainable. The heightened vulnerability of children with disabilities in the digital sphere requires proactive engagement and parental support or those with parental responsibility. For instance, for visually-impaired children, reading social cues could be challenging. Children with intellectual and psychosocial disabilities may encounter the challenge of making appropriate judgments.[76] Moreover, children with albinism generally encounter life-threatening victimisation, such as organ harvesting, a peril that extends to their digital life where they may be targeted by predators. This unique position of children with disabilities in the digital age mandates assisted use of technologies. In undertaking this role, there is the inevitability of encroaching into the child's private space. Effectively managing the vulnerability and disability intersectionality with a child's privacy during the assisted use of technologies becomes a

[74] As above.

[75] Third and others (n 2) 392.

[76] C Kagwiria 'Child online protection for children with disabilities' (10 December 2021), https://www.afralti.org/child-online-protection-for-children-with-disabilities/ (accessed 5 April 2022).

nuanced and delicate task. It is therefore imperative to employ thoughtful approaches to parental guidance, ensuring autonomy, safety and dignity of these children.

Parents use digital and non-digital means to conduct overt or covert surveillance on their children's digital presence. This surveillance extends to monitoring their networking, messaging and browsing history.[77] The expectation of privacy further diminishes when the child uses their parent device, a common scenario in the African context. Such devices are the parent's property, which they routinely inspect. Non-digital monitoring methods include temporary sequestering of children's devices to regulate their screen time and concurrently scrutinise their children's online activities.

Technologies have been developed to enable parents to remotely clone their children's devices and monitor their online behaviour. An example is the Life360 application which offers real-time monitoring of capabilities, including the ability to assess device battery levels and driving speeds.[78] Parents employ these monitoring technologies to not only regulate screen time but also enforce content restrictions, thereby minimising exposure to inappropriate content. Additionally, digital surveillance cameras are also installed in homes to monitor children and sometimes their helpers. The prevalence of technology monitoring extends beyond home settings to educational institutions such as schools and play centres, where it serves as a proactive measure to mitigate security risks.[79] At play centres, for instance, parents can observe their children engaging in various activities and establishing friendships. Notably, the installation of surveillance cameras has become a norm in South African nursery schools and child care centres due to the unfortunate occurrence of child abuse incidents in these institutions.[80] The priority is placed on parental surveillance and the consent of the parent serves as justification for parental intrusions into the child's privacy.

[77] K Mathiesen 'The internet, children, and privacy: The case against parental monitoring' (2013) 15 *Ethics and Information Technology* 263-264.

[78] J Keegan & A Ng 'The popular family safety app Life360 is selling precise location data on its tens of millions of users' (6 December 2021) *The Markup*, https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user (accessed 20 June 2022).

[79] Berson & Berson (n 6) 138-140.

[80] 'Something to ponder: Surveillance cameras to protect our children' (2019) *iAfrica*, https://iafrica.com/something-to-ponder-surveillance-cameras-to-protect-our-children/ (accessed 26 June 2022).

The deployment of monitoring practices has implications on the child's privacy. For instance, the infringement into the child's privacy extends to the child's contacts, primarily composed of children too, and would not have consented to processing of their information by a third party, including communications.[81] Also communications between children take place in the context of friendship, with an expectation of privacy in that relationship.

Parental monitoring presents challenges to children in unique circumstances that require greater levels of privacy. This is particularly pertinent for children experiencing abusive home environments, adolescents seeking autonomy, and those identifying with sexual minorities, as well as individuals in stringent religious communities. In such instances, these children aspire to explore their choices, identities, and circumstances discreetly, avoiding potential embarrassment or surveillance by their parents.[82] Privacy emerges as a critical factor for children with diverse gender and sexual orientations, including trans and queer teens, who rely on it to navigate the intricate process of self-discovery and, eventually, confidently disclose their identities to the public. The imposition of parental surveillance may impede or altogether thwart this exploratory journey. A child's exploration of their identity, manifesting through web searches indicative of being lesbian or gay, may result in harm, particularly for those whose parents harbour strong convictions against individuals with diverse sexual orientations.[83]

In the context of adolescent development, older teenagers may find themselves seeking access to sensitive health-related information pertinent to intimate aspects of their growth. Such inquiries may pertain to matters they are hesitant to discuss with their educators or parents and guardians. Sensitive health information may be collected and processed through online counselling services. Consequently, it becomes imperative for counselling service providers to maintain high standards of confidentiality and data protection. Stringent privacy safeguards should be implemented to govern the handling of information within online counselling platforms. An alternative approach may involve considering an exemption for online counselling services from the mandate requiring parental consent.[84]

[81] C Harrell 'The kid surveillance complex locks parents in a trap' (20 December 2021) *WIRED*, https://www.wired.com/story/the-kid-surveillance-complex-locks-parents-in-a-trap/ (accessed 26 June 2022).

[82] Third and others (n 2) 145.

[83] Mathiesen (n 78) 268.

[84] General Comment 25 para 78.

The pervasive ownership of monitoring applications by companies has resulted in the extensive collection of children's personal information, often lacking essential safeguards to protect such data from potential misuse. Unfortunately, a considerable number of parents remain uninformed about the privacy policies of these companies, some of which explicitly disclose the sharing or sale of data to third parties. The primary focus of parents tends to be on monitoring activities, with a lack of awareness or prioritisation of potential consequences, such as data brokering. Notably, owners of monitoring applications engage in the sale of children's location and other sensitive data to data brokers. For instance, applications like Life360 accumulate location data for children and their families without implementing adequate measures for ensuring the integrity and confidentiality of information security.[85]

Day care centres' use monitoring applications that allow parents to remotely monitor or observe children, raise concern given the risks associated with data collection and sharing when fundamental information security practices and privacy considerations are not accorded due priority. Issues such as securing public cloud buckets hosting children's data, implementing robust cloud server images, embracing end-to-end encryption, and enforcing two-factor authentication become pivotal in mitigating potential risks.[86] The deficiency in proactive disclosure pertaining to information-sharing practices with third parties exacerbates the concerns. There exists a plausible scenario wherein information concerning these preschoolers may be disseminated on social media platforms, such as Facebook, without requisite parental or guardian consent.[87] While the convenience of the monitoring and observation application provides parents with a reassuring sense of remote child monitoring, it concurrently disregards the legitimate concerns surrounding unauthorised access to and utilisation of their child's information by third parties. In the South African context, privacy apprehensions persist despite the perceived security benefits offered by day care centres and camera surveillance. Furthermore, the sharing of passwords used by parents to log into nursery schools or day care facilities with external individuals compounds these privacy concerns.[88] The convenience of the monitoring and observation application affords parents a reassuring sense of ease as they remotely supervise their children. However, this convenience

[85] Keegan & Ng (n 79).

[86] A Hancock 'Parents need to know what's going on inside their day care apps' (23 June 2022) *WIRED*, https://www.wired.com/story/daycare-app-privacy-security/ (accessed 20 June 2022).

[87] As above.

[88] As above.

supersedes any apprehensions related to possible unauthorised access and use of their child's information.[89]

There are views that there should be a focus shift directing more attention towards developers of inappropriate content that children may encounter online, instead of monitoring children online.[90] While there is merit in this approach, it is much more complex, exceeding the monitoring capabilities of parents themselves. Drawing on Zuboff's insights, practising surveillance on children contributes to the proliferation of surveillance capitalism profiting corporations.[91] Parents are incentivised to buy surveillance devices that enhance the safety of their children online. Zuboff contends that the intensified culture of monitoring stems from a trust deficit towards children by parents, which fosters a climate of suspicion and cultivates the acceptability of the privacy infringements among the younger demographic.

Another oppositional position to monitoring of children's online behaviour is propagated by Mathiesen, who contends that such parental surveillance is paternalistic and deemed 'ethically inappropriate'.[92] Mathiesen advocates for prioritising children's rights to privacy over justifications for parental monitoring.[93] Mathiesen's assertion is underpinned by two crucial two positions. Firstly, Mathiesen argues that 'privacy is necessary in order to respect children's current capacities for autonomy and to foster their future capacities for autonomy'.[94] Secondly, 'privacy is necessary in order to protect children's current capacities for relationships and to foster their future capacities for relationships, this includes their developing the capacity to trust, and be trustworthy'.[95] However, this paramountcy of privacy is not absolute. In instances where the necessity to protect the children is presented, the obligation to protect takes precedence and overrides privacy considerations.[96]

[89] Creche and Nursery Schools for South Africa 'Day-care with cameras', https://creche-nurseryschools.co.za/day-care-with-cameras/ (accessed 20 June 2022).

[90] Harrell (n 82).

[91] See generally S Zuboff *The age of surveillance capitalism* (2019).

[92] Mathiesen (n 78) 263-264.

[93] Mathiesen (n 78) 267.

[94] Mathiesen (n 78) 269.

[95] As above..

[96] Mathiesen (n 78) 271.

The exercise of parental responsibility demands a nuanced distinction between monitoring for protection and intrusive interference.[97] While there is justifiable focus and emphasis for child safety in the digital age, it should be acknowledged that privacy is also important for children's dignity; autonomous development and general psychosocial well-being; their agency, and the general exercise of their rights.[98] It is the anonymity and the ability to operate in private that afford children the opportunity to explore and define their identity and exercise self-determination without being subjected to unwarranted exposure or surveillance compromising their privacy.[99] Also, privacy enables them to cultivate friendships and relationships, integral components of normative child development. Therefore, incursion into privacy should be executed with meticulous consideration and guided by the imperative to shield a child from harm.[100] According to Mathiesen, striking the delicate equilibrium between protecting children from online threats and respecting their privacy entails fostering parent-child interactions that educate children and equip them with the necessary skills to navigate digital challenges.[101] Engaging in such conversations also encourages children to openly discuss their struggles within the digital environment.

3.2 Parents' actions that expose children's personal information

3.2.1 Sharenting

Another aspect that presents complexities in children's privacy is the practice referred to as 'sharenting'. It takes diverse forms, ranging from online diaries chronicling a child's journey to the general dissemination of videos and photographs, and even the establishment of social media

[97] C Popa 'Controlling children's passwords is a flagrant breach of their privacy' (27 August 2020) *The Conversation*, https://theconversation.com/controlling-childrens-passwords-is-a-flagrant-breach-of-their-privacy-141031 (accessed 26 June 2022).

[98] General Comment 25 para 67.

[99] General Comment 25 para 77. 'Many children use online avatars or pseudonyms that protect their identity, and such practices can be important in protecting children's privacy. States parties should require an approach integrating safety-by-design and privacy-by-design to anonymity, while ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, such as cyber aggression, hate speech or sexual exploitation and abuse. Protecting a child's privacy in the digital environment may be vital in circumstances where parents or caregivers themselves pose a threat to the child's safety or where they are in conflict over the child's care. Such cases may require further intervention, as well as family counselling or other services, to safeguard the child's right to privacy.'

[100] Mathiesen (n 78) 271.

[101] Mathiesen (n 78) 272.

accounts dedicated to children.[102] The information is shared either with close family and friends or with a broader digital network.[103] Sharenting is facilitated by power dynamics inherent in child-parent relationships, particularly in early childhood when parents wield absolute control and authority over the child's information. At that stage, cognitively, children lack the capacity to comprehend the intricacies of their lives, including consent.[104] In this context, the emphasis on the child's individual autonomy and control is notably diminished. Sharenting results in digital documentation of children's lives on digital platforms, coining the term 'generation tagged' to describe this prevalent reality.[105] Consequently, children reach adulthood with an already developed digital identity and footprint.[106]

Motivational factors behind sharenting include perceived benefits such as creating memories, updating family and friends and sharing parental experiences or soliciting for support in the parental journey.[107] However, despite these benefits, there are privacy implications.[108] The showcasing through sharenting relegates to secondary position pertinent aspects such as dignity and privacy of the child. While some parents may be aware of the privacy risks associated with sharenting and discontinuing the practice, the tendency to share children's images on social media platforms remains prevalent and the trend continues to escalate with the emergence of additional social media platforms and the unprecedented increase of online and social media users.[109]

Privacy and digital identity development are at stake when considering the impact of sharenting. The paramountcy of privacy implications heightens, notably at adolescence, a transitional stage when children start development of their independent digital identity.[110] When parents

[102] K Kopecky and others 'The phenomenon of sharenting and its risks in the online environment: Experiences from Czech and Spain' (2020)110 *Children and Youth Services Review* 2.

[103] Gligorijevic (n 60) 202.

[104] Gligorijevic (n 60) 204.

[105] E Nottingham 'Sharenting in a socially distanced world' (12 August 2020), https://blogs.lse.ac.uk/parenting4digitalfuture/2020/08/12/sharenting-during-covid/.

[106] Berson & Berson (nn 6) 141.

[107] G Ouvrein & K Verswijvel 'Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management' (2019) 99 *Children and Youth Services Review* 320.

[108] As above.

[109] E Nottingham 'Sharenting in a socially distanced world' (12 August 2020), https://blogs.lse.ac.uk/parenting4digitalfuture/2020/08/12/sharenting-during-covid/.

[110] Ouvrein and Verswijvel (n 107) 325.

share content they deem sensitive and inappropriate, it negatively affects their reputation and the digital identity they aspire to cultivate. Also, the 'permanence of online information' creates even greater challenges for the child in the later years when their sensitive information remains permanently online.[111] The inappropriate and sensitive content could also contribute to problems for the child, such as future humiliation, impersonation, cyberbullying and inappropriate use of the child's content by paedophiles and sex predators.[112] Parents do not always have control over the information that they share although they endeavour to keep the context within selected spheres. The content may inadvertently transcend the initially envisioned boundaries.[113]

Beyond the basic sharing of children's personal information for social reasons, there is a commercial dimension. The digital economy has given rise to online working modalities including the emergency of influencers on social media platforms. Children feature substantially on their parents' platforms who are influencers. The use of children's information for developing social media content also exacerbates oversharing of children's personal information, as previously highlighted. The oversharing is perceived as exploitative and could potentially expose children to online harms such as cyberbullying and unsolicited attention by online predators.[114] Social media accounts created by parents on behalf of children are proving to be a conduit for exposing children's privacy, particularly in situations where they lack the capacity to provide informed consent or object to the dissemination of their images. The UK's Digital, Culture, Media and Sport Committee published a report on the harms encountered by children assuming roles as influencers on social media platforms.[115] The report underscores:

> Posting content about children online can affect their privacy, which brings security risks. For example, checking-in to venues on social media posts or posting images of the child's home could expose their location. Some child influencers, like child stars, have amassed a significant fan base, which could

[111] Humanium (n 72).

[112] Kopecky and others (n 104) 5.

[113] As above.

[114] See Sarah Adam's TikTok account (@mom.uncharted), in which she interrogates the role of parents in creating a digital footprint for their children by posting their personal information over which they do not have control, https://www.tiktok.com/@mom.uncharted/video/7062434975810931974?is_from_webapp= 1&sender_device=pc&web_id6891301529808209413 (accessed 4 July 2022).

[115] UK Parliament 'Influencer culture: Lights, camera, inaction?' (9 May 2022), https://publications.parliament.uk/pa/cm5802/cmselect/cmcumeds/258/report.html#heading-4 (accessed 30 June 2022).

> expose them to additional attention when they travel or run fan meet-and-greets.[116]

Although this is a UK-focused report, it is imperative to recognise that the concerns elucidated are equally pertinent in the African context.

The subject of consent in processing personal information is paramount, but is a complex terrain, generally, and more complicated in the context of children's rights. In the case of a child, it 'neither necessarily expresses a child's autonomy nor protects it, particularly where power imbalances exist'.[117] Simultaneously, parental consent may not invariably be the appropriate option as it may not represent the best interests of the child. According to UN General Comment 25 on children's rights in relation to the digital environment, consent should be informed and freely given by either the child or the parent or caregiver. The age and evolving capacity of a child determines the appropriate consenting party prior to processing of data. Data controllers or processors should ensure and validate the acquisition of informed and meaningful consent.[118] In Africa, data protection laws mandate the consent of the responsible adult for processing children's personal information, a stance echoed in the legislation of South Africa, Ghana, and Zimbabwe. However, the practical application faces challenges due to the inherent complexities that characterise this domain.

4 Children's actions that compromise their privacy

4.1 Children as online content creators and sharing of personal information

Children actively shape their digital identity and leave a lasting footprint through content creation and dissemination on digital platforms, thereby unconsciously compromising their privacy. The dichotomy between public and private is distorted in the context of the screen-driven culture, compelling children to share content that would otherwise be considered intimate and private, and not intended for public consumption. The propensity to share content online has evolved into a global phenomenon

[116] As above.

[117] Human Rights Council Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci 'Artificial intelligence and privacy, and children's privacy' (July 2021) para 120, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement (accessed 31 March 2022).

[118] General Comment 25 para 71.

among the young demographics.[119] Parents may not be aware of the nature and extent of content creation and dissemination by their children, particularly adolescents. Teenagers perceive online platforms as safe spaces for sharing personal information, including about their dating life.[120] The South African case presents a quintessential illustration of children overly disclosing intimate personal information. Teenagers as young as 14 years, actively participated under the hashtag #TheRiskITook, which gained popularity on TikTok and other social media platforms. They shared information about reckless sexual conduct that resulted in pregnancy at a young age.[121] The testimonies include images of themselves and their babies. While the hashtag raised awareness on teenage pregnancy it also had privacy implications. They are driven by peer pressure and suboptimal digital hygiene practices reflective of inadequate levels of digital literacy.

For instance, adolescents in South Africa actively participate in the dissemination of sexually explicit material, engaging with both their romantic partners and strangers whom they encounter and form relationships with online.[122] While the sharing of content occurs with an expectation of privacy, the originator inadvertently relinquishes control over the recipient's subsequent actions with the shared information. Regrettably, instances have arisen where intimate images are disseminated without consent or manipulated into explicit content when relationships turn adversarial.[123] The enduring online footprint of these occurrences has the potential to detrimentally impact individuals' reputations, both during their formative years and later in adulthood.

The digitised world is creating new manifestations of child labour where children participate in the digital economy, and assume social media roles as influencers, including on YouTube, Instagam TikTok and generate income for both themselves and their families. They are commonly referred to as 'child influencers' and their cultural currency hinges on popularity which is determined by continuously churning out content to captivate audiences. However, it is within the realm of content creation that the privacy of these children becomes compromised, as they divulge

[119] J Orlando 'Online and out there: How children view privacy differently from adults' *The Conversation* (14 April 2015), https://theconversation.com/online-and-out-there-how-children-view-privacy-differently-from-adults-38535 (accessed 26 June 2022).

[120] MacAfee (n 73).

[121] LMMM Rantao '#TheRiskITook on sex and pregnancy: Where do we draw the line?'(12 June 2022) *IOL*, https://www.iol.co.za/sundayindependent/news/africa/theriskitook-on-sex-and-pregnancy-where-do-we-draw-the-line-73879ded-3c6d-4182-922d-0c666bc4568a (accessed 26 June 2022).

[122] Bush (n 58).

[123] As above.

sensitive information, including location details and other personal data. This is exemplified in the South African context, particularly observed in children's behaviour in photo-sharing applications and related platforms.[124]

4.2 Sharing of passwords

Younger children, typically characterised by a propensity to share possessions and establish minimal boundaries, exhibit a parallel behaviour in the digital world. Among the various privacy-infringing behaviours observed in children, the act of sharing passwords with friends or romantic partners stands out prominently. This conduct is primarily rooted in trust among friends or signifies the intimacy within a romantic relationship.[125] However, such sharing compromises the inherent secrecy of a password, a crucial element that preserves the exclusivity of online accounts and acts as a deterrent against unauthorised access. The act of sharing passwords blurs the line between the legitimate account owner and other users with access to the password, potentially distorting the child's unique digital identity.[126] The termination of friendships or romantic liaisons further exposes password owners, rendering them susceptible and vulnerable.

Besides the imprudent practice with passwords, parents also exercise some degree over a child's digital life by retaining access to their passwords. While it is justifiable for the parents to exercise some degree of control, children should be given the 'freedom to control their own passwords', thereby fostering a deeper understanding of concepts related to privacy and identity, empowering children to navigate the digital landscape responsibly.[127]

4.3 Children Strategies to circumvent parental oversight

In light of their status as digital natives, most adolescents exhibit an advanced technological proficiency surpassing that of their parents and guardians. Leveraging this knowledge, they employ privacy-enhancing measures, denoted as 'monitoring escape action' by Vallejo and others, to

[124] 'Teens are flocking to new photo-sharing apps. Are they safe?' (22 May 2022) *IOL*, https://www.iol.co.za/lifestyle/family/parenting/teens-are-flocking-to-new-photo-sharing-apps-are-they-safe-07cb76f5-f8e3-41fd-9864-e2ecd88f48ce (accessed 26 June 2022).

[125] Pew Research Centre: A Lenhart and others 'Teens, kindness and cruelty on social network sites' (9 November 2011), https://www.pewresearch.org/internet/2011/11/09/teens-kindness-and-cruelty-on-social-network-sites/ (accessed 26 June 2022).

[126] Popa (n 97).

[127] As above.

counteract parental surveillance.[128] These measures include the strategic selection of applications perceived as 'safe' from parental scrutiny, the activation of privacy settings and messaging controls designed to restrict parental access to online activities, and a discerning approach to friend selection that typically excludes parents or guardians.[129] They may also resort to creation and dissemination of content on platforms unknown to their parental figures and configure profiles as private, limiting access exclusively to friends. The activation of privacy settings allows for the discreet concealment of profile information, activities, likes, and interests, albeit with certain basic details such as name, profile image, and gender potentially remaining accessible by default.[130] It is also common for pre-adolescents to employ stratagems such as falsifying their ages to gain access to social media platforms that impose age restrictions exceeding their actual age, such as Facebook, Instagram, Pinterest, and X (formerly Twitter).

Notwithstanding the privacy measures implemented to circumvent parental scrutiny, these efforts do not constitute a foolproof shield against potential exploitation. While children may skillfully navigate away from parental scrutiny, their actions position them in situations inherently fraught with the risk of exposure to abuse in the course of online interactions, particularly with strangers harbouring malicious intentions, such as sexual predators targeting teenagers and young adults.

5 Emerging technologies and processing of children's personal information

The advent of emerging technologies, particularly AI, has become a cornerstone of the 4IR, exerting a profound influence on individuals' lives, notably those of children. This transformative impact is evident in the digitisation of children's toys, which are integrated with digital assistants like Alexa and Google Voice.[131] Consequently, emotional and cognitive expressions of children may permeate the structures of toy manufacturing businesses.[132] AI's influence is evident in its potential to combat violence against children, particularly in tracking down predators.[133] However,

[128] Vallejo and others (n 20) 1197.

[129] Lenhart and others (n 125).

[130] As above.

[131] S Steinberg 'Ethical AI? Children's rights and autonomy in digital spaces' (28 April 2021), https://blogs.lse.ac.uk/parenting4digitalfuture/2021/04/28/children-and-ai/ (accessed 28 March 2022).

[132] UNICEF (n 30) 32.

[133] Steinberg (n 132).

the use of AI presents ethical concerns, as its deployment may have adverse implications for children's rights, with a particular focus on privacy considerations. The advent of big data similarly yields a dual impact, in that it expedites seamless data retrieval yet concurrently gives rise to substantial privacy concerns. This is especially pronounced when the ethical management of extensive datasets is either disregarded or mishandled.[134] Additional considerations involve the adept management of sensitive data, particularly health information, and the crucial subject of informed consent. However, despite the growing interest in the intersection of AI and children, the efficacy of this strategic focus is compromised by the inadequate emphasis and scholarly attention directed towards this burgeoning discourse.[135]

6 Existing frameworks in Africa for children's privacy and child protection online

Given the identified risks that children encounter in the digital sphere and the associated privacy challenges, it is imperative to examine the framework designed to safeguard children online, including their privacy. This section highlights the international framework as provided by the UN and the regional and sub-regional framework in the African context. While this framework fundamentally ensures the protection of childre''s rights, it should be acknowledged that the initial instruments were not designed with the digital environment in consideration. Consequently, treaty-monitoring bodies are presently engaged in formulating standards to address the protection and advancement of children's rights in the digital age. Instruments under consideration are the UN CRC; the African Children's Charter, the African Union Convention on Cyber Security and Personal Data Protection (the (Malabo Convention); the UN General Comment 25; and General Comment 7 and its Resolution on the Promotion of Children's Rights in the Digital Sphere of the African Committee of Experts on the Rights and Welfare of the Child (African Children's Committee).

6.1 International and regional framework

6.1.1 United Nations Convention on the Rights of the Child

The UN CRC is the international child rights instrument. Adopted in 1989, it contains provisions on the protection of children against various forms of human rights violations. Regarding privacy, article 16 stipulates

[134] As above..

[135] As above.

that a child's privacy should not be subject to unlawful and arbitrary infringements, emphasising the need to safeguard their right to privacy through legal means.[136]

6.1.2 UN General Comment 25 on children's Rights in relation to the digital environment

This General Comment, adopted by the Committee on the Rights of the Child in 2021, is specifically tailored to address the promotion and safeguarding of children's rights within the digital context. The Committee recognises that 'innovations in digital technologies affect children's lives and their rights in ways that are wide-ranging and interdependent, even where children do not themselves access the internet'. Based on this position, the Committee sought to guide states on the application of CRC to the digital environment, urging them to enact legislative and other measures. It emphasises the need to respect the perspectives of children; prevention of discrimination; upholding the right to life; ensuring survival and development; and acknowledging the evolving capacities of the child; and prioritising their best interests.[137]

6.1.3 African Charter on the Rights and Welfare of the Child

The African Charter on the Rights and Welfare of the Child (African Children's Charter) is the continental instrument on the rights of the child.[138] The Charter imposes binding obligations on states concerning the safeguarding of children. Specifically, section 10 underscores the imperative to safeguard the right to privacy. It stipulates that:

> No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.[139]

[136] Art 16: '(1) No 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. (2) The child has the right to the protection of the law against such interference or attacks.'

[137] UN General Comment 25 generally.

[138] African Charter on the Rights and Welfare of the Child, https://au.int/en/treaties/african-charter-rights-and-welfare-child (accessed 5 March 2022). It was adopted in 1990 and came into force in 1999 (African Children's Charter).

[139] Sec 10 African Children's Charter.

6.1.4 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention

Adopted in 2014, the AU Convention establishes a framework for addressing cyber security, the prevention of cybercrimes, and the safeguarding of personal data. Notably, the Convention incorporates specific provisions on child protection. In this regard, article 29(3) focuses on content-related offences, imposing a legal obligation on member states to criminalise activities related to child pornography, including its production, distribution, registration, transmission, importation, and possession.[140]

6.1.5 African Children's Committee General Comment 7 on article 27 of the African Charter on the Rights and Welfare of the Child on Sexual Exploitation[141]

The General Comment expounds on article 27 of the African Children's Charter, specifically addressing the multifaceted issue of child sexual exploitation and abuse.[142] It extensively covers child sexual exploitation online and presents an opportunity to extend the understanding of the implications of article 27 of the African Children's Charter to the digital world of exploitation and abuse.[143]

6.1.6 Resolution on the promotion of children's rights in the digital sphere

The Resolution was also adopted by the African Children's Committee in recognition of the negative encounters that children experience in the digital environment.[144] The Committee recognised the need to protect

[140] African Union Convention on Cyber Security and Personal Data Protection, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 5 March 2022).

[141] African Children's Committee General Comment 7 on art 27 of the African Charter on the Rights and Welfare of the Child on Sexual Exploitation (2021), https://www.acerwc.africa/wp-content/uploads/2021/09/General-Comment-on-Article-27-of-the-ACRWC_English-1.pdf (accessed 5 March 2022).

[142] Art 27 provides: '1. States Parties to the present Charter shall undertake to protect the child from all forms of sexual exploitation and sexual abuse and shall in particular take measures to prevent (a) the inducement, coercion or encouragement of a child to engage in any sexual activity; (b) the use of children in prostitution or other sexual practices; (c) the use of children in pornographic activities, performances and materials.'

[143] African Children's Committee General Comment 7 para 10.

[144] African Children's Committee Resolution on the Promotion of Children's Rights in the Digital Sphere, https://drive.google.com/file/d/1WhBF7HGfvyTyxWJmkGsHuavnJhZMrDdd/view (accessed 5 March 2022).

and promote children's rights to privacy as provided under the African Children's Charter and other instruments such as the Malabo Convention.

6.2 National frameworks

Drawing from the regional and international frameworks,states have an obligation to adopt measures for the lawful processing of personal information including that of children. States are mandated to design regulations for children that are suited for the digital environment, taking into consideration the best interests of the child principle, child protection and privacy as primary considerations. Infringements into children's rights should only be for legitimate reasons and prescribed by the law. Currently, over 30 African countries have adopted specific data protection laws while others have taken a sectoral approach. This section highlights the South African and Rwandan contexts on the protection of children's information and the promotion of digital literacy.

6.2.1 Protection of Personal Information Act

South Africa's Protection of Personal Information Act (POPIA) serves as the framework for regulating the processing of personal information including children's personal information. Section 34 prohibits the processing of children's personal information and mandates responsible parties processing children's information apply for authorisation from the Information Regulator. Upon meeting the requisite criteria, additional conditions are imposed to ensure compliance.[145] The Act also mandates that the processing of a child's personal information should be undertaken with explicit consent of a competent person. Such processing should be deemed a requisite measure for defending or exercising a right, or fulfilling a legal obligation.

Furthermore, processing may be permissible for research, statistical, or historical purposes, provided it serves a public interest. It is imperative that adequate safeguards be implemented to ensure the child's privacy, even in situations where obtaining the required consent is unattainable.[146] A child's personal information may also be processed if it is already consciously in the public domain, with the consent of a competent person. The processing may be authorised if the responsible authority has established adequate safeguards for the protection of children and that there exists a compelling public interest justification for the processing. In terms of the law, an individual with competence may withdraw content or

[145] Sec 35 POPIA.

[146] As above.

seek a review of a child's personal information. Responsible parties may be required to provide notification detailing their processing practices, the amount of information being processed and the nature of children's information that is being processed.

To provide further clarity and guidance on the processing of children's personal information, the Information Regulator, the oversight body with the mandate to oversee the implementation of POPIA, developed a guidance note specifically addressing the processing of children's personal information.[147] It primarily provides guidance to responsible parties who require authorisation to process children's personal information as stipulated in the Act. The guidance note elaborates on appropriate safeguards and public interest. The determination of public interest varies across jurisdictions and requires case-specific assessment given that it is broad and nuanced. It signifies that an undertaking typically yields widespread benefits to the public at large and is essential for fostering justice and equality.[148] In the guidance note the conception of appropriate safeguards is embedded in section 19(1) of POPIA that places a responsibility on the parties processing personal information to ensure its confidentiality and integrity through utilisation of organisational or technical measures to avoid unauthorised access, damage or loss.[149] It is also necessary to establish a comprehensive framework for conducting risk assessment, managing risks and updating existing safeguards, assessing the implementation of the adopted safeguards, taking into account generally-accepted measures and sector-specific safeguards.

6.2.2 The case of Rwanda's digital ambassadors programme

In Rwanda, concerted interventions are being undertaken to address the need for digital literacy. A notable initiative is the Digital Ambassadors Programme, a government-funded initiative strategically designed to provide digital literacy to communities.[150] It is a component of the Smart

[147] South Africa Information Regulator 'Guidance note on processing of personal information of children' (2021), https://inforegulator.org.za/wp-content/uploads/2020/07/GuidanceNote-Processing-PersonalInformation-Children-20210628-1.pdf (accessed 14 June 2022).

[148] As above. Public interest examples in terms of sec 37 of the POPIA include: (a) the interests of national security; (b) the prevention, detection and prosecution of offences; (c) important economic and financial interests of a public body; (d) fostering compliance with legal provisions established in the interests referred to under paragraphs (b) and (c); (e) historical, statistical or research activity; or (f) the special importance of the interest in freedom of expression.

[149] South Africa Information Regulator (n 148).

[150] Government of Rwanda Digital Ambassadors Programme, https://www.minict.gov.rw/projects/digital-ambassadors-programme (accessed 16 June 2022).

Rwanda Master Plan.[151] Significantly, training sessions are conducted in local languages, with due consideration given to contextual nuances unique to Rwanda. The overarching goal of this initiative is to empower communities to fully harness the potential of digital technologies. This educational intervention serves as a means to ensure that a broad spectrum of community members, encompassing parents and caregivers, are sufficiently proficient in digital technologies. The acquisition of such skills is instrumental in enhancing their proficiency in parenting in the dynamic landscape of the digital age.

The foregoing discussion underscores the inherent risks associated with the digital environment, rendering it unsafe for children to navigate autonomously with absolute privacy. While countries like South Africa and Rwanda have adopted progressive measures in regulating the processing of children's information and promoting digital literacy, these initiatives fall short in addressing the complexities arising from children's online presence and digital technology usage. Comprehensive and nuanced approaches are required in addressing an array of concerns across diverse sectors. The proactive measures undertaken in South Africa and Rwanda are not common practice in Africa. The regulatory framework for the processing of children's personal information is still developing.

7 Lessons for Africa

In the European and US context, technology advancements and integration predate that of Africa and and the regulatory frameworks, particularly concerning child online protection, are more mature. This segment of the chapter highlights child protection and privacy measures that African states could consider in fostering healthy digital lifestyles for children. The insights are predominantly derived from advanced European frameworks that extensively address privacy and child protection in the digital sphere. Given the expansive nature of these initiatives, a comprehensive assessment is beyond the scope of this chapter; therefore, only a select few will be explicated for illustrative and lesson-drawing purposes. Selected examples cover general regulations for the protection of children online, data protection in educational settings, guidance for parents, mechanisms

[151] Government of Rwanda Smart Rwanda Master Plan (2020), https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/SMART_RWANDA_MASTERPLAN.pdf (accessed 15 June 2022). The Rwandan plan is also inspired by the Smart Africa Manifesto, a 2013 policy document that was adopted by select AU states: Burkina Faso, Gabon, Kenya, Mali, Rwanda, South Sudan, Uganda. It is a statement of commitment 'to provide leadership in accelerating socio-economic development through ICTs'. See https://smartafrica.org/who-we-are/ (accessed 15 June 2022).

for the protection of children's privacy online, guidelines for digital service providers, and media-specific measures. These examples are presented with the intent that they may be adapted to the African context, and contribute meaningfully to strengthening existing frameworks.

7.1 US Children's Online Privacy Protection Act

The US Children's Online Privacy Protection Act (COPPA) is an example of legislation for children in the digital age. It was in response to the growing use of the internet and introduction of data processing that impacted on children's privacy. It establishes responsibilities for online service providers that serve children below the age of 13. These include notifying parents of information practices, ensuring verifiable parental consent for the processing of children's personal information, affording parents the agency to determine the utilisation of their child's personal information, including the ability to curtail further processing. Additionally, the legislation mandates provision for parental access to their child's personal information, advocates for data minimization by requesting only information that is deemed reasonably necessary, and necessitates the implementation of pertinent procedures to uphold the security, integrity, and confidentiality of children's personal information.[152] In this framework, parents have a basis for controlling personal information that is collected from their children in the digital sphere.

7.2 Guidelines on Children's Data Protection in an Education Setting

Adopted in 2020 by the Council of Europe, these Guidelines are designed to offer guidance to key stakeholders in the education sector, such as policy makers, legislators, data controllers, and the education industry in general, to uphold children's rights in processing children's information. It establishes fundamental principles, including the best interests of the child; the evolving capacities of the child; the right to be heard; and the right to non-discrimination.[153] It contains specific recommendations directed at legislators and policy makers, data controllers and for the industry.

[152] US Government US Children's Online Privacy Protection Act, http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

[153] Council of Europe 'Children's data protection in an education setting (Guidelines)' (20 November 2020), https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b (accessed 13 March 2022).

7.3 The UK Children's Commissioner's Guide for Parents

The Guide addresses the manner in which parents ought to engage with their children concerning online sexual harassment, offering essential insights into the ways children navigate the internet and the consequent adverse effects they may encounter. In light of these, it subsequently furnishes parents with counsel on the appropriate methods and timings for addressing these potential pitfalls. It comprehensively explores complex subjects that frequently confront parents, including but not limited to peer pressure, exposure to pornography, the sharing of explicit images (cyberflashing), instances of sexualized bullying, and the manipulation of photographs impacting body image.[154]

7.4 UK Code of Practice to protect children's privacy online

Adopted in 2020 under the auspices of the UK Information Commissioner, the age-appropriate design Code of practice for online services sets out 15 standards for the protection of children's privacy.[155] It is targeted at 'those responsible for designing, developing or providing online services like apps, connected toys, social media platforms, online games, educational websites and streaming services'.[156] The core tenet embodied in the Code is the requirement for service providers to set high standards for default privacy settings on services and other digital products that might be accessed by children, taking due consideration of the best interests of the child.

7.5 OECD Recommendations on the Protection of Children Online

The Recommendations were initially adopted in 2012 and amended in 2021, in response to the risks that children encounter in the digital environment.[157] The 2021 amendments took into account advancements

[154] As above.

[155] UK Information Commissioner 'The age appropriate design: A code of practice for online services' (2020), https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/ (accessed 13 March 2022).

[156] UK Information Commissioner 'ICO publishes Code of Practice to protect children's privacy online' (21 January 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/ (accessed 13 March 2022).

[157] OECD Recommendation of the Council on Children in the Digital Environment (2021), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389 %20 (accessed 13 March 2022).

in technology and additional risks as a result of the COVID-19 pandemic. The Recommendations recognise the significance of protecting children's data and their privacy for their autonomy and well-being. Consequently, it is essential to empower children so that they 'become confident and competent users of digital technology'.[158] The Recommendations establish principles for a safe and beneficial digital environment for children, encompassing fundamental values; empowerment and resilience; proportionality and respect for human rights; appropriateness and inclusion; and shared responsibility, co-operation, and positive engagement.[159] The Recommendations also include policy-related proposals. These entail the demonstration of leadership and commitment taking into account the best interests of the child in the digital environment;[160] the review, development and amendment of laws that impact on children in the digital environment; the promotion of digital literacy; the adoption of evidence-based policies to support children in the digital space; and the promotion of measures that 'provide for age-appropriate child safety by design'.[161] The concluding segment underscores the imperative of international collaboration, with specific reference to the OECD Guidelines for Digital Service Providers, recognised as pivotal in safeguarding children's online welfare.

7.6 OECD Guidelines for Digital Service Providers

The Guidelines were adopted in 2021 and complement the Recommendations on the Protection of Children Online.[162] They are aimed at providing guidance to service providers

> when they take actions that may directly or indirectly affect children in the digital environment, in determining how best to protect and respect the rights,

[158] As above.

[159] As above.

[160] These include: (a) adopting clear policy objectives at the highest level of government; (b) articulating a whole-of-government approach, through a national strategy where appropriate, that is flexible, technology neutral, and coherent with other strategies for fostering a sustainable and inclusive digital economy; (c) consider establishing or designating oversight bodies, with a view to: (i) coordinating stakeholders' views, efforts, and activities in the development of policies; (ii) meeting policy objectives; (iii) reviewing the effectiveness of policy actions and measures implemented to account for the best interests of children in the digital environment; (iv) coordinating, in accordance with their legal and institutional frameworks, the relevant actions of government bodies with responsibility for responding to the needs of children; (v) ensuring that the actions of government bodies are cohesive and mutually reinforcing, rather than an accumulation of isolated or stand-alone, and potentially inconsistent, initiatives; and (vi) promoting co-operation across borders.

[161] OECD (n 160).

[162] As above.

> safety, and interests of children, recognising that girls, children belonging to racial, ethnic and religious minorities, children with disabilities, and others belonging to disadvantaged groups may require additional support and protection.[163]

The Guidelines acknowledge the nuances in the nature of service providers and identify three broad specific measures that could be adopted by service providers. These are taking a precautionary approach by adopting the child safety by design option; proactively providing sufficient relevant information in a transparent manner; and informing relevant actors, such as children, parents and any other persons with parental responsibility, all the required information about data processing. Finally, the Guidelines urge service providers to establish governance and accountability mechanisms that promote the best interests of the child when accessing their products and services.[164]

7.7 BBC editorial guidelines for safeguarding children's online safety

The editorial guidelines of the British Broadcasting Corporation (BBC) encompass directives regarding the engagement with children and young individuals in online platforms.[165] The BBC provides explicit and comprehensive thematic instructions that pertain to various aspects, including but not limited to issues of privacy;[166] children and young people and content contributors;[167] harm and offence;[168] competitions, votes and interactivity.[169]

[163] As above.

[164] OECD 'Guidelines for digital service providers', https://legalinstruments.oecd.org/public/doc/272/5803627d-b49b-4894-8dbe-35f67fd10007.pdf (accessed 13 March 2022).

[165] British Broadcasting Corporation 'Guidance: Interacting with children and young people online', https://www.bbc.com/editorialguidelines/guidance/children-young-people-online#guidanceinfull (accessed 13 March 2022).

[166] BBC 'Guidance: Privacy), https://www.bbc.com/editorialguidelines/guidelines/privacy/ (accessed 13 March 2022).

[167] BBC 'Guidance: Working with children and young people as contributors', https://www.bbc.com/editorialguidelines/guidance/children-young-people-working/ (accessed 12 March 2022).

[168] BBC 'Editorial guidance: Harm and offence', https://www.bbc.com/editorialguidelines/guidelines/harm-and-offence/ (accessed 12 March 2022).

[169] BBC 'Editorial guidance: Competitions, votes and interactivity', https://www.bbc.com/editorialguidelines/guidelines/competitions-votes-interactivity/ (accessed 12 March 2022).

7.8 UNICEF Guidelines for Industry on Child Online Protection

Adopted in 2015, the UNICEF Guidelines are designed to protect child safety online.[170] They target governments, schools and industry. Broadly, the Guidelines

(a) establish a common reference point and guidance to the ICT and online industries and relevant stakeholders;
(b) provide guidance to companies on identifying, preventing and mitigating any adverse impacts of their products and services on children's rights;
(c) provide guidance to companies on identifying ways in which they can promote children's rights and responsible digital citizenship among children;
(d) suggest common principles to form the basis of national or regional commitments across all related industries, while recognising that different types of businesses will use diverse implementation models.[171]

The Guidelines contain a sector-specific checklist addressing various facets of promoting digital technology for civic engagement; digital literacy for parents, teachers and children; and the creation of age-appropriate online content. Additionally, the Guidelines advocate for the establishment of standardised procedures for managing child sexual abuse material and the integration of children's rights into corporate and management policies.[172] The specific sectors covered by these Guidelines are broadcasting services, mobile operators, internet service providers; media service providers, application stores, hardware developers and operating systems developers.

The selected examples from Europe and the US serve as valuable benchmarks for the development of region-specific strategies in Africa aimed at ensuring children's online protection and safeguarding their privacy. The detailed recommendations delineating these strategies are outlined in the subsequent part of this chapter.

8 Conclusion and key recommendations

The examination of child online risks and their privacy implications underscores the imperative for states to implement appropriate measures.

[170] UNICEF 'Guidelines for industry on child online protection' (2015), https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf (accessed 16 June 2022).

[171] As above.

[172] As above.

The ensuing recommendations are directed towards policymakers, the business sector, the media, schools, and other pertinent institutions tasked with managing children's information. A default adherence to high standards of child privacy should be instituted for platforms and digital devices catering to children, accompanied by the provision of mechanisms for redress in cases of privacy breaches. Embracing preventive measures, robust safeguards, and restorative justice in all its forms should constitute the foundational approach to online child protection and privacy.[173] While incorporating privacy-enhancing technologies, such as encryption, it is essential to ensure they do not impede the detection and reporting of child-based exploitation online. Also, upholding the principles of legality, necessity, and proportionality is paramount.[174] These recommendations draw heavily from the insights outlined in UN General Comment 25 as well as research findings from UNICEF.

8.1 States

In the wake of a global transformation ushered in by digitisation, the state remains the duty bearer as the primary protector and assumes the role of providing the overarching guidance on online child protection and privacy through legislative and other measures. The UN General Comment 25 underscores the imperative for states to enact measures ensuring the protection of children in the online sphere. In order to harmonise and advocate for diverse perspectives and requirements of children based on various variables, all policy advancements should align with international human rights and standards, incorporating consultations with children and institutions dedicated to promoting children's rights and welfare.[175] The recommendations for the state that will be discussed focus on legislative and policy measures for child protection and privacy and data protection; the education sector; parents and caregivers; the media and civil society; and public and private sector institutions. The state's obligations concerning child protection emanate from the CRC, the Africa Children's Charter, soft law instruments that have been developed by the UN Committee on the Rights of the Child and the African Children's Committee; and other relevant international and regional instruments such as model laws, conventions and guidelines.

[173] General Comment 25 para 81.

[174] General Comment 25 para 70. Any decision to decrypt children's data for criminal investigation on online crimes that are perpetrated against children, such as child sexual abuse and exploitation, should be proportionate and in the best interests of the child. See also UNICEF (n 30) 32.

[175] UNICEF (n 30) 35.

8.1.1 Child safety and privacy and data protection frameworks

Ensuring the efficacy of children's rights legislation and policies requires regular scrutiny to ascertain their compatibility with the evolving digital landscape and alignment with the best interests of the child. This entails the enactment of laws and policies designed to shield children in the online sphere, safeguarding the confidentiality and integrity of their personal information.[176] Amendments to existing legislation conceived without foresight into the digital age are necessary, alongside the introduction of new laws tailored to address contemporary challenges. Concurrently, the establishment of relevant institutions is vital to oversee and enforce these regulations. Noteworthy is the UK's establishment of a children's commissioner dedicated to addressing online protection concerns. Conversely, the challenge in Africa lies in the implementation of existing frameworks. To rectify this, a more robust sectorial or thematic approach is recommended, facilitating the formulation of additional regulations or guidance relevant to the protection of children's rights in the digital realm.

8.1.2 Recommendations for digital literacy

States should ensure that, in the implementation of measures aimed at realising the right to education, education policies explicitly incorporate media and digital literacy, seamlessly integrating them into both school and teacher training curricula.[177] Recognising digital literacy as a fundamental life skill is paramount, serving as a critical mechanism for effectively navigating the complexities of the digital world, including its inherent risks.[178] The inclusion of digital proficiency skills within teacher training

[176] General Comment 25 para 70. The fundamental point is that children's personal information should not be arbitrarily accessible except by designated entities, for specified duration and purposes in line with the law. See General Comment 25 para 73.

[177] UNESCO Policy Brief: Digital Literacy in Education 7, https://iite.unesco.org/files/policy_briefs/pdf/en/digital_literacy.pdf (accessed 16 June 2022). See also Berson & Berson (n 6) 142. Berson and Berson conceptualise digital literacy as 'a compilation of legal precedent, voluntary policies, and ethical conduct. It represents the ability to access digital forms of information, critically evaluate its quality and utility, analyse information for connections to and expansions of knowledge, and use digital tools to produce original works. It emphasises the capacity to fully participate as a responsible member of a technologically engaged society and refers to the skills that people need to understand and constructively navigate the digital media that surrounds them. It addresses safety and security while fostering broader preparation for digitised and networked environments.'

[178] Berson & Berson (n 6) 142-143. See also Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci (n 117) para 118. In his report Cannatai also affirmed that '[d]igital literacy education can prevent harmful online behaviour at its source', so 'children and adolescents need operational skills and cognitive and social abilities to use technologies in thoughtful, ethical and safe ways'. This should be in addition to the

programs empowers educators to adeptly guide learners on crucial aspects of the digital environment, such as safety and privacy. Within African communities facing challenges associated with the digital space and technological innovations, parents and caregivers often find themselves insufficiently prepared to navigate the complexities of parenting in the digital age. Notably absent are targeted programs addressing the unique needs of parents and caregivers. Consequently, states should proactively adopt policy measures that foster opportunities for parental digital literacy, equipping parents with the necessary tools to safeguard their children, particularly the younger ones, in the digital environment.[179] These tools include managing online relationships, ensuring the secure sharing of personal information, reporting abuse, implementing effective filtering, age verification, and password protection – all pivotal components contributing to online safety.[180] An example of community digital literacy is the previously-discussed Rwandan Digital Ambassadors Programme.

However, controversies surround the efficacy of digital literacy as a comprehensive strategy for mitigating digital risks. Despite efforts to impart knowledge to children, educators, and parents about the intricacies of the digital landscape and its implications for safety and privacy, the inherent challenge is multifaceted. In tandem with fostering digital literacy, a recalibration of the conditions governing data processing is necessary, with a primary emphasis on the responsibilities of service providers.[181] Scrutiny of prevailing data processing conditions reveals a lack of clarity, thereby complicating the ability of children and parents to navigate the system effectively. The underlying reality is that, on occasion, these conditions are not optimised to facilitate the seamless management of one's data.[182]

8.1.3 Recommendations for schools and other educational institutions

The digitisation of the education sector significantly impacts the processing of children's data. Educational institutions process information such as class videos, academic performance, attendance, age, address, sex

privacy engineering of digital technologies that technology companies should adopt. See para 123.

[179] General Comment 25 para 21.

[180] UNICEF (n 30) 34.

[181] S Livingstone '"It's none of their business!" Children's understanding of privacy in the platform society' (15 August 2020), https://blogs.lse.ac.uk/parenting4digitalfuture/2020/07/15/privacy-in-the-platform-society/ (accessed 9 March 2022).

[182] As above.

and ethnicity. Additionally, some schools install surveillance cameras in classrooms or school premises. Given the mandatory nature of education, some of the regulations associated with it are seldom contested by learners or parents, potentially leading to a lack of scrutiny. In the absence of robust safeguards, regulations, and security measures, there exists a risk of data collection that falls outside the boundaries defined by data protection principles. These principles include, but are not limited to, obtaining meaningful consent, practising data minimization, ensuring accountability, minimising the purpose of data usage, maintaining transparency, and ensuring data accuracy.[183] The onset of the COVID-19 pandemic and the subsequent shift towards virtual education underscored a prevalent disregard for child data privacy laws, notwithstanding the extensive digital footprints generated by virtual learning, thereby heightening privacy concerns.[184] While the processing of a child's information in the education sector serves legitimate purposes, it is imperative that such processing adheres strictly to established data protection principles.[185]

The education sector manages substantial volumes of children's information, thereby creating potential avenues for abuse in the absence of strict regulatory adherence. A notable concern involves the unlawful and unauthorised utilisation of students' accounts, facilitating access to inappropriate content and enabling engagement in illicit activities, thereby posing a significant risk of long-term reputational harm to the child.[186] Such situations emanate from weak password management systems, particularly when custodianship of passwords is vested in administrators. Addressing these irregularities and vulnerabilities is crucial to safeguarding the integrity and security of students' information in the education sector.[187]

8.1.4 Recommendations for private institutions

According to Third and others, 'it is timely and important to assert states' obligations to ensure that businesses bear their responsibilities regarding children's rights.'[188] In this regard, states should adopt policies that govern the processing and management of data by both public and private entities,

[183] Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci (n 117) para 107.

[184] As above.

[185] General Comment 25 para 73.

[186] Popa (n 97).

[187] As above.

[188] Third and others (n 2) 387.

with a primary focus on safeguarding children's data.[189] The legal and policy framework should expressly mandate that any institution engaged in the processing of children's data formulates and implements robust child protection policies, specifically tailored to address online threats and prevent various forms of abuse such as the exploitation of children's information for commercial benefits. This encompasses mitigating the exploitation of children's information for commercial gains, exemplified by the monetization of such data for targeted marketing and advertising purposes. This could through the establishment and enforcement of child-specific ethical standards, integrating paramount considerations of privacy and security measures into the broader framework.[190]

The UN Guiding Principles on Business and Human Rights provides a framework from which states should regulate the conduct of businesses in the spectrum of human rights.[191] Central to this framework is the foundational principle that 'states must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises'.[192] Businesses, on the other hand, bear the responsibility to uphold and 'respect human rights throughout their operations'.[193] Complementary to these principles, UNICEF also developed guidelines for industry on child online protection.[194] Service providers, particularly social media platforms, bear the responsibility of ensuring that their terms and conditions, privacy policies, and data protection policies are presented in a manner that is easily comprehensible and accessible to both children and parents. In fulfilling their duty-bearing role, states must establish an enabling environment conducive to the realisation of these objectives. This necessitates the implementation of relevant legislative and policy frameworks by the state to regulate the conduct of businesses in alignment with the outlined principles.

The legislative framework should comprehensively address the multifaceted responsibilities of business enterprises including implementation; enforcement mechanisms; and mechanisms for redress.

[189] Third and others (n 2) 387.

[190] UNICEF (n 30) 34.

[191] United Nations 'Guiding principles on business and human rights', https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed 9 March 2022).

[192] As above.

[193] As above.

[194] UNICEF 'Guidelines for industry on child online protection' (2015), https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf (accessed 16 June 2022).

The responsibilities entail imposing obligations for businesses to design their platforms in a manner that serves the best interests of the child.[195] The legislation should also mandate businesses to report online exploitation and abuse of children to law enforcement or other designated authorities.[196] A critical component of the regulatory framework should involve the establishment of a robust sanctions regime specifically tailored for offences related to online child exploitation. Clear and accessible mechanisms for redress must be articulated within the legislative framework.

As elucidated earlier, the diverse range of harms experienced by children online necessitates that social media platforms refrain from disseminating child abuse content. These platforms should proactively establish deterrent mechanisms against offenders utilising their platforms for the collection and distribution of information resulting in child abuse and exploitation. Collaborative efforts with law enforcement agencies and other pertinent entities are imperative to effectively combat online criminal activities targeting children.[197]

Another important recommendation pertaining to both private and business entities involves conducting children's rights impact assessments (CRIAs) and child rights impact evaluation (CRIE). CRIA, an evaluative process undertaken prior to the implementation of any action or decision, serves to ascertain the potential impact of proposed measures on children. Conversely, CRIE systematically examines both the intended and unintended consequences of decisions or actions on the rights of children. Undertaking these assessments guarantees a holistic approach that is thorough and inclusive, encompassing the entirety of children's rights.[198] Therefore the imperative of governmental bodies, civil society, and regulatory authorities to hold businesses accountable in this regard cannot be overstated.

8.1.5 Recommendations for the media and civil society

The media is a significant stakeholder in online child protection and their privacy. Its influence extends to fostering or perpetuating the vulnerability

[195] Livingstone (n 186).

[196] UNICEF 'Legislating for the digital age', https://www.unicef.org/media/121261/file/Legislating%20for%20the%20digital%20age%20.pdf (accessed 20 May 2022).

[197] UNICEF (n 30) 34.

[198] E Lievens and others 'The child right to protection against economic exploitation in the digital world' (2019) 4, https://www.ohchr.org/sites/default/files/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/OtherStakeholders/EvaLievensSimonevanderHofetal.pdf (accessed 9 March 2022). This is a submission during the drafting of General Comment 25.

of children in the digital sphere. The media as an evolving sector is also using technology innovations that have an impact on children. Particularly when children are contributors of online content, it becomes imperative to observe due considerations for their privacy and secure parental consent. To uphold ethical standards and ensure diligence, media outlets should engage child experts in scrutinising children's content prior to publication. Upholding high ethical standards and exercising due diligence should be integral to all media engagements involving children.

In its approach to children in the digital age, states should actively collaborate with civil society organisations. Child-led groups and child-rights advocates and other organisations with a focus on digital rights are important allies in the implementation of initiatives related to the promotion and protection of children's rights in the digital environment.[199] Both the media and civil society bear a shared responsibility in strengthening public awareness and fostering digital literacy. Advocates for digital rights should conceptualise interventions aimed at equipping children and communities with essential digital skills. Illustrating the media's role, the Share Aware campaign in the United Kingdom, spearheaded by the National Society for the Prevention of Cruelty to Children, serves as an exemplary initiative. This media campaign is purposefully designed to impart knowledge to children about cyber safety and underscore the significance of safeguarding their personal information.[200]

9 Conclusion

The initial design of the digital landscape did not prioritise children but their presence has escalated in this domain. It is therefore imperative to continuously establish protective mechanisms in this dynamic evolving digital landscape, to minimise their susceptibility, considering that it has become integral to children's lives. This presents opportunities and risks, heightened by the amplified online engagement during the COVID-19 pandemic. While the pandemic response propelled children's access to digital devices and the internet, it is crucial for states, as duty bearers, to regulate the digital environment in a manner that upholds and respects the best interests of every child. The formulation of such interventions requires a multi-stakeholder approach in alignment with international human rights standards. In this regard, it is important to clarify the

[199] UN General Comment 25 para 34.

[200] J Orlando 'Online and out there: How children view privacy differently from adults' *The Conversation* (14 April 2015), https://theconversation.com/online-and-out-there-how-children-view-privacy-differently-from-adults-38535 (accessed 31 March 2022).

stakeholder roles in promoting children's privacy and online safety, for the sustained success of interventions.

The imperative to shift perspective from perceiving children solely within the framework of vulnerability is underscored, advocating for their acknowledgment as rights holders. Active inclusion of children in pertinent regulatory and policy dialogues is necessary, accompanied by comprehensive awareness campaigns aimed at navigating technologies for children, parents, caregivers, and educators. Realising this goal necessitates the establishment of collaborative alliances between the state and stakeholders in the education sector, child rights civil society organisations, academia, the media, the private sector, legal professionals, and communities at large.[201] An overprotective approach unnecessarily limits children's rights to privacy and expression, which should not be limited arbitrarily. Where data protection legislation or other regulatory frameworks are adopted, they should respect child privacy and the protection of their personal information. As children spend more time online and use automated systems, through education, social media interactions or gaming, service providers should adopt the privacy by design approach. They should continuously review their data protection practices and policies and align them with the best interests of the child.[202] A rights-based and multi-stakeholder approach should be adopted in integrating the privacy and protection agendas.[203]

Robust research, including continuous assessment and evaluation is also crucial in understanding the complexities of children's digital experiences. This recommendation requires a nuanced approach particularly in the context of data collection, which should take into account the various dimensions such as socio-economic background, gender, sex, language, location, ethnicity, age, race and disability. The insights gleaned from such research forms the basis for possible action. Finally, while acknowledging the risks, it is imperative to underscore the significance of privacy in fostering children's psychosocial and autonomous development. The efficacy of the proposed recommendations hinges on the adoption and effective implementation of legislative and other measures by states, striking the delicate balance between the right to privacy and online protection. Regular reviews are also important considering the fast paced

[201] Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci (n 117) para 30.

[202] These approaches should also encompass sports and entertainment premises, educational institutions, business premises, homes, streets and shopping centres. See General Comment 25 para 74.

[203] Berson & Berson (n 6) 145. See also Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci (n 117) para 117.

evolution of technology advancements, which also intensifies digital risks for children.

References

Berson, IR & Berson, MJ 'Children and their digital dossiers: Lessons in privacy rights in the digital age' (2006) 21 *International Journal of Social Education* 136

Calvoz, RR and others 'Constitutional implications of punishment for cyber bullying' (2014) *Cardozo Law Review*

Gligorijevic, J 'Children's privacy: The role of parental control and consent' (2019) 19 *Human Rights Law Review* 202

Kopecky, K and others 'The phenomenon of sharenting and its risks in the online environment: Experiences from Czech and Spain' (2020)110 *Children and Youth Services Review* 2

Laubscher, M & van Vollenhoven, WJ 'Cyberbullying: Should schools choose between safety and privacy?' (2015) 18 *Potchefstroom Electronic Law Journal* 2219

Mathiesen, K 'The internet, children, and privacy: The case against parental monitoring' (2013) 15 *Ethics and Information Technology* 263-264

Ouvrein, G & Verswijvel, K 'Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management' (2019) 99 *Children and Youth Services Review* 320

Slonje ,R & Smith, PK 'Cyberbullying: Another main type of bullying?' (2008) 49 *Scandinavian Journal of Psychology* 147-154

Third A and others 'Recognising children's rights in relation to digital technologies: Challenges of voice and evidence, principle and practice' in Wagner B and others (eds) *Research handbook on human rights and technology Global Politics, Law and International Relations* (United Kingdom: Edward Elgar Publishing,2019)

Vallejo, MG and others 'Kids and parents privacy exposure in the internet of things: How to protect personal information?' (2018) 22 *Computación y Sistemas* 1196