CHILDHOOD VULNERABILITIES

in South Africa

Some Ethical Perspectives

J. Grobbelaar & C. Jones (Eds)

CHAPTER 10

PROTECTING CHILDREN IN THE DIGITAL SOCIETY

Louis Fourie

INTRODUCTION AND BACKGROUND

All over the world glowing computer, tablet or mobile phone screens are illuminating the faces of children who are often so immersed in what the technology offers that they are unaware of the world around them (Third et al. 2017:9). Information and Communication Technology (ICT) has become pervasive in almost all spheres of daily life. And with the general adoption of ICT, children increasingly have access at home and school to computers or personal smart phones (Rizza & Pereira 2013:9).

At about 4.54 billion active users worldwide (58.2% of the population), each spending an average 6.5 hours online each day, the internet plays a major role worldwide in changing the methods and speed of communication (Minić & Spalević 2014:417; Lin 2019; Clement 2020). Since about one third of internet users in the world are children, it is understandable that the internet has a significant effect on their lives (Livingstone, Carr & Byrne 2015:6; Byrne & Burton 2017:39-40). According to a recent UNICEF report (eds. Keeley & Little 2017:1), the youth of ages 15-24 are currently the most connected age group, with a 71% presence online compared to 48% of the total population of the world.

Social media has become ubiquitous and the preferred instruments of interpersonal communication, as well as educational, political and business exchange. In Africa, the second most populous continent, where about half the population is below the age of 15, children and young people are the most prolific users of trendy new technology and social media (Ephraim 2013:275-277; Mascheroni & Ólafsson 2018:15).

The predominant use of mobile technologies by children to access the internet (Byrne & Burton 2017:44) has resulted in a new 'bedroom culture' where online access becomes personal and private with little or no supervision by the parents (Wojniak & Majorek 2016:132; eds. Keeley & Little 2017:1). Children all over the world are also starting to use the internet at an increasingly younger age and are often able

to use a mobile phone or tablet before they learn to talk, leaving many online policies lacking since they predominantly focus on children above 12 years (OECD 2016:100-103; Byrne & Burton 2017:44).

Due to the importance of social networking such as Facebook, WhatsApp, Snapchat and Instagram to cultivate and sustain interpersonal relationships, 86.3% of children in South Africa have a social networking account. The most popular are WhatsApp (94.2%) and Facebook (68.5%). However, only one in three children has set their social networking profiles to private. The remaining two-thirds of children are exposed to high risk (Phyfer, Burton & Leoschut 2016:31, 35; Graafland 2018:16; cf. DQ Institute 2018).

Children use the internet more than any other medium to communicate and socialise. Technology, such as chat applications, e-mail, instant messaging, online virtual worlds, multiplayer online games, and social networking made it possible for children to communicate and socialise far beyond the safety of their homes. Digital technology has become a normal part of life and is merely a nonorganic extension of their bodies, while social media is perceived as a 'real' world and not a virtual world (Minić & Spalević 2014:426). However, it is the ubiquity, the easy accessibility and anonymity of this technology that create new risks of abuse irrespective of the geographic location of children (Mishna, McLukie & Saini 2009:107; Rizza & Pereira 2013:9, 39; Wojniak & Majorek 2016:132). New technology often coincides with new ways of misuse or abuse of that technology (Hachiya 2017:177).

The DQ Impact Report (DQ Institute 2018) indicated that 56% of 8-12 year old children are exposed to cyber-risks, such as cyberbullying, video game addiction, online grooming and online sexual behaviour, while 64% of South African children engage in cyber risks. In South Africa, 34.5% of children have been exposed to hate speech and 51.2% to inappropriate sexual images (Phyfer et al. 2016:39, 50, 66). The high percentages can possibly be attributed to insufficient social structures to deal with cyber risks, such as a lower public awareness about cyber-risks; ineffective online protection policies; a lack of preparation of children, and a low involvement of parents (DQ Institute 2018).

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

The DQ Institute (2018) study further found that the combination of a mobile phone and social media increases the risk of the child to 70% due to longer screen time (32 hours or more per week) and less supervision (50% of 8-12 year olds access the internet via mobile phone) (cf. Rideout 2015:16, 40). It is estimated that by the end of 2020, about 390 million 8-12 year old children will be at risk. This problem is exacerbated by the exponential growth of constant connectivity (720 million of 8-12 year olds online by the end of 2020) and a general lack of protection. A total of 90% of the 720 million child users worldwide are from emerging ICT countries where the cyber risk for children is significantly higher.

Just like urbanisation and globalisation during previous eras, digital technology has changed the world immensely. The digitalisation of our world is an inescapable force that impacts almost every sphere of our lives – shaping our economies, societies and cultures. And as increasingly more children gain access to the online world, it is also changing childhood forever. Children are, from their birth, imbued with a constant stream of digital technology shaping their life experiences, perceptions, ideas and worldviews and are at the epicentre of ICT changes (Valentine & Holloway 2001:71-72; eds. Keeley & Little 2017:1, 8-9).

DEFINING THE PROBLEM

Unfortunately, as is the case with all new technology, digital technology does not come without significant risks to the safety, privacy and well-being of children (Grant 2010:4-5; Minić & Spalević 2014:417). Digital technology can easily amplify existing offline threats and misuse, as well as expand opportunities for taking advantage of children's often poorly managed privacy, thus increasing the vulnerability of susceptible children. The result is that children often encounter cyberbullying, harassment, unwanted sexual solicitation, and improper advertising and marketing driven by algorithms (Byrne & Burton

2017:40). These challenges will only intensify in future as the digital revolution progresses and the lives of children are touched by artificial intelligence, robotics, machine learning, deep learning, the Internet of Things (IoT) with its ubiquitous sensors and monitoring, and an increasing number of digital devices and online platforms (eds. Keeley & Little 2017:1, 8-9).

Children's rapid adoption of the internet and other online technologies, together with an increase in time spent online, and the constantly changing media landscape (e.g. more apps and tailored sites, more individualised media use, and more mobile internet), expose children to digital risks and harmful content, as well as threaten their privacy and safety (Livingstone et al. 2014:272, 275, 279-280; see Paniagua and Istance 2018:62-65).

Digital technology is not only intensifying some well-known childhood risks, such as bullying, but also encouraging new forms of the exploitation of children, such as 'made-to-order' child pornography and live streaming of explicit sexual abuse of children. Due to the internet, it is now easier than ever for predators to contact unsuspecting children through anonymous and poorly protected social media profiles and even game forums. Innovative new technologies, such as crypto currencies are unfortunately powering the Dark Web with its harmful child content and streaming of child sexual abuse, while making it increasingly difficult for law enforcement to stay abreast (eds. Keeley & Little 2017:2).

Strangely enough, 92% of all child sexual abuse websites identified by the Internet Watch Foundation are hosted in only five countries, namely the Netherlands, United States, Canada, France and the Russian Federation (eds. Keeley & Little 2017:2). Until now, efforts to address this problem has had relatively little impact.

This chapter will touch on the abovementioned ethical issues that affect children who are immersed in technology while growing up in the digital era. Various digital risks that children are exposed to will be covered, the ethical challenges involved, as well as the role of the different stakeholders in assisting children to build resilience. Although there are several views about the intrinsic dangers of the

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

digital world in comparison to offline dangers, the aim of the chapter is to point out the digital risks without being alarmist or selective as is sometimes the case with the popular media.

A TYPOLOGY OF ICT-RELATED RISKS

Various classifications of ICT-related risks exist, but the taxonomy developed by EU Kids Online is particularly valuable in the understanding of the concerns. EU Kids Online groups the concerns into three categories, namely content, contact and conduct risks as displayed in Table 1. Content risks are those where the child is the receiver of mass-produced content, while contact risks refers to the risks where the child is an active participant in an adult-initiated activity. Conduct risks entails peer-to-peer risks where the child is a perpetrator, actor or creator of risky content or contact (Livingstone & Haddon 2009:7-8).

The category of conduct risks goes against the popular myth of the harmless or innocent 'victim-child' that limits the child to the role of a passive recipient of content or abuse and thus ignores the active role or online conduct of children against other children (Barbovski & Dreier 2013:60).

Table 1: Classification of ICT-related risks

	Content Child as receiver (Mostly mass productions)	Contact Child as participant (Adult-initiated activity)	Conduct Child as actor (Child as perpetrator or creator of risky content or contact)
Aggression and violence	<ul style="list-style-type: none"> • Websites encouraging unhealthy or dangerous behaviours, such as self-harm, self-abuse, self-mutilation, suicide, bulimia, anorexia, bomb-making, or drugs preparation • Hate speech and hateful content • Exposure to extremist, violent, or gruesome images and content • Exaggerated information 	<ul style="list-style-type: none"> • Harassment, stalking • Radicalisation • Persuasion to take part in harmful or perilous behaviours • Hate speech 	<ul style="list-style-type: none"> • Cyberbullying, stalking and harassment • Digital violence • Digital humiliation of others • Hostile and violent peer activity • Hateful materials about other children

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

Sexual abuse	<ul style="list-style-type: none"> • Unwanted or harmful exposure to inappropriate, sexual or pornographic images or content • Unethical behaviour • Hyper-sexualisation • Vulgarism 	<ul style="list-style-type: none"> • Participation in unsafe communication, e.g. an adult seeking inappropriate contact • Seduction and luring into meeting strangers in the real world • Sexual harassment • Sexual solicitation • Sexual grooming • Cyber stalking • Child exploitation • Sexual extortion 	<ul style="list-style-type: none"> • Production, posting, distribution and consumption of child abuse or sexual material • Child sexual abuse • Child-produced indecent images • Sexting
Values	<ul style="list-style-type: none"> • Racist or discriminatory material • Biased information or advice (e.g. drugs; promiscuity) • Exposure to inaccurate or misleading information • Ascribing infallibility to a machine • Internet addiction 	<ul style="list-style-type: none"> • Ideological persuasion • Wrongful persuasion (e.g. self-harm) 	<ul style="list-style-type: none"> • Potentially harmful user-generated content • Provoking racism • Encouraging suicide, anorexia • Narcissism

Commercial exploitation	<ul style="list-style-type: none"> • Embedded advertising and marketing • Spam • Sponsorship 	<ul style="list-style-type: none"> • Tracking and harvesting of personal information • AI & algorithms pressuring children, e.g. nudging • Violation and misuse of personal data • Hacking • Fraud and theft 	<ul style="list-style-type: none"> • Online gambling • Illegal downloading and copyright infringement • Hacking • Live streaming of child sexual abuse • Trafficking for the purpose of sexual exploitation • Sexual exploitation of children in travel and tourism
--------------------------------	---	---	---

Sources: Livingstone and Haddon (2009:7-8), Keeley and Little (eds. 2017:68, 72-73) and Matyjas (2008:207-208).

The EU Kids Online II survey of 2009 to 2010 provided a unique and valuable insight into a range of activities undertaken by children online, the various risks that accompany them, as well as the parental strategies to reduce these risks. Although the survey focused on Europe, it collected valuable qualitative data from nearly 10 000 children and clearly illustrated the correlation between online opportunities and risks (Livingstone et al. 2011:142).

The study found that the biggest concern for children is around content risks, such as pornography and violent images (58%), followed by contact and conduct risks (42%). Younger children are more concerned with content-related risks, with a growing concern regarding pornographic content during their teen years. As they grow older, the concern around conduct and contact-related risks increases. It is significant that some of the risks that are very prominent in the media and on the public agenda, such as sharing personal information online, or talking to and meeting strangers, were rarely mentioned. The highest risk was attributed to video-sharing sites (e.g. YouTube)

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

(32%), followed by websites (29%), social networking sites (13%) and games (10%) (Livingstone et al. 2014:1-7; Wojniak & Majorek 2016:132-133).

What makes the situation more complex is that it is much more difficult for children to judge behaviour as right or wrong in the virtual world (Vesnaja & Niveditha 2012:2) due to a “sense of disorientation and isolation leading to the disregard of reality” and a blending of reality and virtual reality (Minić & Spalević 2014:418-419).

ICT-RELATED RISKS

Although the digital world did not create the unethical behaviour of sexual abuse and exploitation of children, it does facilitate existing forms and also creates totally new forms.

CONTENT RISKS

EXPOSURE TO INAPPROPRIATE CONTENT

Perhaps the most widely known danger is the easy access of children to a superfluity of anti-social content, such as pornography, destructive religious sectarianism, fascism, child abuse, and many more (Matyjas 2008:203). Of the content-related offences, exposure to abusive child pornography tends to be dominant (Mishna et al. 2009:113; Minić & Spalević 2014:421). The exposure takes place through immoral websites, vulgar expressions in chat rooms, profane language and sacrilege (Aslani et al. 2013:215), as well the production and dissemination of graphic sexual content via mobile devices (Mishna et al. 2009:108). The widespread use of mobile technology and easy access to broadband internet has increased the vulnerability of children, especially those without the necessary protection. Research indicated

that as high as 53% of exposure victims were under ten years old (eds. Keeley & Little 2017:77-79).

A further contributor to inappropriate content is hateful websites that propagate violent behaviour amongst children through violent murder videos and other acts of violence (Aslani et al. 2013:215).

Children's unrestrained and easy access to pornography and inappropriate content on the internet is partly due to parents' inability to exercise control or to implement an 'appropriate-use' policy. Interestingly, it seems that parents' concerns are less about protecting the innocence of the child but rather about the knowledge about alternative sexual traditions and models of sexuality that could invade the perceived sanctity of the home (Valentine & Holloway 2001:72).

VIOLENT GAMES

Unfortunately, some games that are meant for child entertainment are full of brutality and violence and have a negative influence on the development and behaviour of children. Certain games are known to cultivate aggression, a feeling of unlimited power over others, narcissism, a disregard for rules, extreme competitiveness and submission of others, impetuosity, and emotional apathy. Games often allow children protection against the real world and allow them to fulfil their dreams and desires. This escape from the real to an illusionary world – often to fill a void or escape rejection – is the very reason why games become psychologically addictive (Matyjas 2008:202, 205-206). It is for this reason that parents should be aware of the dangers presented by games, as well as the underlying problems (:206-207).

Children easily believe in the infallibility of the computer with the result that “the nihilism of modern technology destroys sensibility, solidarity, and critical thinking” as summarised by Minić and Spalević (2014:427). The revival of known magic and religious rituals by the techno-culture, and especially games, often takes the soul of the child as victim and shakes the very foundation of humanity (:427).

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

DIGITAL ADDICTION

Although technology provides access to an overabundance of digital content, entertainment and social connectivity, premature and unrestrained use of digital technology can lead to digital and screen addiction (eds. Keeley & Little 2017:9). Children often use the internet as a substitute reality to escape daily routine, obligations and real life problems. Children who spend an exorbitant amount of time in the virtual world experience deterioration in traditional social interactions. They neglect their studies and even basic physiological needs, such as sleeping and eating (Matyjas 2008:203-204).

CONTACT RISKS

SEXUAL ABUSE AND EXPLOITATION

The internet is increasingly being used by children to meet people and make friends since children find it easier to be themselves in a virtual world. This is further promoted by social networks that aim to promote homophily by bringing like-minded people together, based on their user profiles (Graafland 2018:17).

Although social media provides a platform for children to meet and befriend people, it does entail several risks because children are less careful whom they socialise with on the internet and would often share personal information, engage in undesirable exchanges or meet strangers in person (Graafland 2018:17-18). This behaviour increases the probability of sexual harassment, grooming, and sexual abuse by adults (Lupton & Williamson 2017:782). The proliferation of mobile devices and broadband access has made children more accessible than ever before.

Technological advances exacerbate the above problem by allowing perpetrators to remain anonymous, operate under fake identities, mask their digital tracks, simultaneously pursue multiple

victims, and track them across websites and platforms, (eds. Keeley & Little 2017:77-79). Cryptocurrencies used as anonymous payment systems and end-to-end encrypted platforms used for the sharing of abusive media, make the tracking by law enforcement exceptionally difficult and thus contributed to an increase in the live streaming and distribution of child exploitation material. This situation is further complicated through the distribution of child sexual abuse material through Peer-to-Peer (P2P) network file sharing, the Deep Web and the Dark Web. The Dark Web conceals content and uses anonymity granting web browsers and is known for numerous illegal markets and online child abuse circles (eds. Keeley & Little 2017:79-80).

Contact risks can take several forms:

- *Internet paedophilia*: Internet paedophilia is one of the most prominent forms of computer crime in many countries. Paedophiles increasingly use technology to search the internet for potential child victims and are often part of organised crime. Many paedophiles have made the internet their playground and, under the guise of anonymity, constantly subject children to inappropriate sexual messages that have an effect on their psychological development. The typical modus operandi is to falsely present themselves as a peer to gain the trust of the child, which is then used to start a sexual discussion, exchange explicit sexual photos or meet in person (Minić & Spalević 2014:419, 421-425).
- *Cyber stalking*: Cyber stalking involves the use of the internet to pursue, harass, or contact children in an unsolicited fashion ranging from irritating e-mails to death threats. Often the aim is to identify, 'groom', and entice individuals to perform sexual acts on or offline. Cyber stalkers are skilful at siphoning personal information about a child through communications with a child's online friendship group. Some of the children are so distraught by fear that

the stalker would harm them that they engage in self-harming behaviour (Mishna et al. 2009:108-109, 111-112).

- *Grooming*: The internet with its wealth of social networking sites, e-mail, instant messaging and chat rooms creates endless opportunities for online predators to groom their victims by gaining the child's attention or trust and befriending them before moving the communication to video- and photo-sharing platforms, which can lead to content-driven or financially driven extortion or personal offline meetings (UNICEF 2012:15; eds. Keeley & Little 2017:77-79). Since much of the grooming or the befriending of children online for sexual abuse is happening across borders it poses exceptional challenges to law enforcement agencies (Livingstone et al. 2015:12).
- *Cyber solicitation*: The solicitation of teenagers to engage in online sexual acts, 'cybering' (explicit sexual dialogue) or 'flashing' (displaying nudity via webcams) is endemic and usually comes from an older unknown or known person, some of whom are in positions of power and trust. They usually get the child to give in through constant pressure, by offering rewards, and even threats. Quite often the nudity is reposted all over social networking sites without consent, leading to remorse, regret, shame and self-harm amongst victims, who fear that it may resurface anytime since it has an infinite existence. The volume of online child abuse images has grown to such an extent that law enforcement units are not able to cope (Livingstone et al. 2015:12). The online cyber-sexual encounters sometimes progress to actual meetings with all the fear and dangers involved (Mishna et al. 2009:112-113; cf. Third et al. 2017:16).
- *Online dating*: For many children, the internet is an integral component of their romantic and sexual discovery.

Numerous children as young as 13 years old are involved in passionate online romantic and sexual relationships (Mishna et al. 2009:109). These encounters range from cybering and flashing to long-term relationships that often progress to meetings in the real world (:109-110).

COMMERCIAL HARVESTING AND MISUSE OF DATA

Technologists had an idealistic dream of a connected world where everyone could communicate and share their knowledge. Unfortunately, the digital footprints of people (and children) on the web are being thoroughly mined into a trillions-of-rand-a-year industry. The face, voice, body functions and private lives of individuals are being tracked and closely monitored by marketing companies. With the propagation of the Internet of Things (IoT), most devices are now connected to the internet and sensors are increasingly embedded in objects. Large technology companies are collecting every post, click, like, website visited, and purchase in real-time through 'Push Pages' (sharing of user's profile identifiers between companies) and 'fingerprinting' (an incredibly accurate method of identifying people). If the newer 'canvas' method of fingerprinting is used, entailing embedded coding in the HTML5 code of a website, users could be identified precisely without the use of cookies. And unlike cookies, nothing that is saved on the computer can be deleted (Fourie 2020).

Face- and voice-recognition algorithms are employed to track and create a lifelong digital record of all movements, conversations and actions in public. This gathered data is so extensive that it is possible to determine a child's medical history and religiosity (Regan & Jesse 2019:171).

Over time, organisations can form a very accurate picture of a child's emotional pulse – what they like, what gets their attention, what they fear, what their boundaries are, and what it would take to cross those boundaries. The data collection techniques have

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

grown so sophisticated that marketers, advertisers, and politicians are becoming increasingly proficient to predict the preferences of people and children even before they have considered the choices by themselves. Companies are known to target children as young as four in an attempt to manipulate their consumption patterns. This exploitation of the identity and privacy rights of children may lead to the development of materialistic values and an identity through the purchase of certain consumer goods. Children thus become more susceptible to the persuasion of the current consumer culture, without fully understanding the impact (Lennie 2013:55-57). Human beings, including children, have now become a very valuable commodity.

The gathering of personal data of children through the internet and social media profiles is a growing concern, especially where privacy settings and online security are not well managed. Unfortunately, children often reveal valuable information to marketers, such as personal (e.g. name and e-mail) and profile data (e.g. preferences, hobbies, favourite brands and shops) because of the 'privacy paradox' or perceived benefits to data disclosure. Privacy remains a fuzzy concept for children due to the blurring of the borders between private and public in the online world (Rizza & Pereira 2013:24-25).

If this data is combined with internet tracking data, it places their online privacy at considerable risk and even allows companies to manipulate children's online behaviour and decisions through behavioural targeting and marketing (eds. Keeley & Little 2017:91-92). Google was fined \$170 million in September 2019 for illegally collecting personal information from children and using it to target them with advertisements (Fourie 2020).

All this personal information is used to feed people a constant stream of 'personalised' content (cf. Whittlestone et al. 2019:20). This targeted marketing is aimed at changing the behaviour of people. However, in truth, the presented reality is a very filtered reality. The role of the now defunct Cambridge Analytica in the pro-Brexit campaign before the referendum, as well as the 2016 USA election, is infamous. By gathering 5 000 data points on each USA voter through the scraping of their Facebook and other social media accounts, they

were able to connect the dots and very accurately profile each voter and predict their personality. Since personality drives behaviour and behaviour influences people's decisions and how they vote, Cambridge Analytica in support of the Republican Party used this psychological data to embark on a major influencing campaign of voters via social media by inter alia appealing to their fears and hate (*The Guardian* n.d.).

The power of big data, personal profiling and psychographics through the use of artificial intelligence and deep learning will increasingly impact our lives. It is calculated that when a child becomes eighteen, thousands of data points would exist on the web due to the interaction of the child. Disinformation and fake news will increasingly be used, which makes the web dangerous for uninformed children to use. And we currently have little control and little leverage with regard to this dangerous psychological manipulation and exposure of minors to inappropriate commercial advertising where the choices of the child are predetermined.

In the physical world, the extent of advertising and selling of products and services to children are well regulated. Unfortunately, this is not the case in the virtual world, where the extensive mining of personal data, viral marketing, advert games, and in-app purchases place enormous commercial and peer pressure on children and their privacy (Lennie 2013:54; Livingstone et al. 2015:12). Unfortunately, legal frameworks governing this extensive data collection are also still lacking (Regan & Jesse 2019:171).

CONDUCT RISKS

Public dialogue often focuses on the exposure of children to *content* risks (e.g. pornography) and *contact* risks (e.g. online grooming by paedophiles). However, research found that children's own *conduct* is increasingly causing harm to themselves and/or to other children (Livingstone et al. 2014:278, 280). Cyberbullying, youth-produced

sexual imagery, sexting, sextortion, and abuses of the privacy of children are emergent concerns all over the world (Bulger et al. 2017:753).

Unfortunately, the response worldwide to the above risks has mostly been to restrict access to harmful or age-inappropriate content, rather than focusing on the underlying needs as indicated by the youth themselves: finding reliable sources of information, finding support for relationship challenges and dealing with peers (Bulger et al. 2017:753).

It seems that peer-to-peer threats are already entrenched in social media interactions. Conflict between children, often applauded by peers, can easily result in harm, as well as identity and reputational damage (Livingstone et al. 2014:280; Mascheroni & Ólafsson 2018: 25-27).

THE CHILD AS ACTOR

Children participate in a variety of online activities, such as texting, chatting, blogging, vlogging, and the exchange of pictures. Although these activities allow children to exercise their right to expression, it also involves some serious risks (Middaugh, Clark & Ballard 2017:128). Unfortunately, many of these risks go unnoticed since children are considered only as victims (Livingstone et al. 2015:12).

The borders between private and public are very vague to a child of the digital age. Many children, therefore, engage in online sexual exchanges with strangers and would easily send or download online sexual content (DQ Institute 2018). Especially older children would send or post suggestive messages and nude or semi-nude pictures of themselves (Kosenko, Luurs and Binder 2017:142). This behaviour could harm the privacy and endanger children as sexually explicit pictures rapidly spread online and also remain on the internet indefinitely (Livingstone et al. 2015:12). Several cases of revenge pornography by children – the spreading of compromising pictures online of former partners without their consent – have also been documented (OECD 2016:106). These pictures are also often used in

blackmail, which has, in certain instances, led to suicide (eds. Keeley & Little 2017:74)

CHILD-PRODUCED SEXUAL CONTENT

According to research, a significant number of young people engage in the production and distribution of sexual content, for example online streaming for payment (eds. Keeley & Little 2017:77-79; cf. Lennie 2013:3), making them liable for prosecution (cf. Cranmer, Selwyn & Potter 2009:128). In some instances, countries make provision for consensual activities between minors as a normal discovery of sexuality (Bulger et al. 2017:756-757). In South Africa, sexting is chargeable under sections 18, 19 and 20 of the *Criminal Law (Sexual Offences and Related Matters) Amendment Act* (RSA, Act No. 5 of 2015), but consensual sex between children is no longer a crime if the children are between 12 and 16 years old.

As the internet and social networking sites become the normal place to socialise, it is logical that as children grow older and enter puberty, their sexual discourse will also migrate to the online space. Legislation will have to be more sensitive to the complexities of dealing with immature and often innocent children acting with intention and agency. Although current policy and legal frameworks aim to protect children online, substantial development is needed to balance it with the rights of children to participation and engagement. The ‘innocence’ view of children in need of protection does not hold in all cases (Bulger et al. 2017:759).

CYBERBULLYING

Cyberbullying feeds off the neglect of privacy principles by children, such as the sharing of personal information or images with perceived trusted others (Rizza & Pereira 2013:24-25). A strategy to curb cyberbullying will have to start with the respect of privacy and the limiting of disclosure to others.

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

Cyberbullying is when children use digital media to wilfully and repeatedly torment, harass, intimidate, embarrass, humiliate, denigrate, or demean other children through hurtful, cruel or threatening messages; flaming; disclosing of secrets; posting of embarrassing, obscene or slanderous information or pictures; impersonation of the victim; cyber stalking; deliberate exclusion of someone from a group; purposefully unfriending (outing or social exclusion) someone or pretending to befriend someone (Popovac & Leoschut 2012:1; Ephraim 2013:209; Lennie 2013:3; Rizza & Pereira 2013:12; eds. Keeley & Little 2017:74-76).

Research found that South Africa has one of the highest prevalence of cyber aggression and cyberbullying among children. Social media is the most common platform for cyberbullying and the most common perpetrator in South Africa is a classmate. However, the bullying is also done by strangers and known adults. The majority of people feel that current anti-bullying measures are insufficient (Popovac & Leoschut 2012:3; Lennie 2013:49; Newall 2018:3-9).

Two features make cyberbullying significantly different from traditional bullying, namely anonymity and accessibility. Online anonymity minimises the perpetrator's fear of punishment, strengthens the power imbalance between the perpetrator and the victim and, therefore, stimulates more violent and castigatory behaviour (Rizza & Pereira 2013:12; Graafland 2018:24). Virtual spaces allow attacks at any time and place, while mobile phones make the escape from abuse and harassment nearly impossible (Rizza & Pereira 2013:12-13; Minić & Spalević 2014:426; eds. Keeley & Little 2017:74-76). Smart phones added a new dimension since cyberbullying can now go beyond the power of words to include pictures and videos. The lack of visual and auditory feedback regarding the consequences of the actions of the perpetrator reduces the feeling of empathy and leads to a greater tendency to engage in aggressive behaviour in online spaces (Lennie 2013:51-53).

According to research, cyberbullying and violence is often fuelled by violent video games and gossip, which has become quite natural and acceptable in today's life (the naturalistic fallacy) (Lennie 2013:8).

Social media is the ideal tool for gossip. Since it is often accompanied by images and screen captures, it is much harder to defuse due to the perceived truthfulness of images. Social networks are also used by some children for self-promotion, narcissism, and self-gossip (Rizza & Pereira 2013:24, 40; cf. Third et al. 2017:9).

From a legal viewpoint, cyberbullies can find themselves in contravention of the law in some countries. For example, threats of violence, criminal coercion, stalking, and hate crimes are all criminal acts (Ephraim 2013:279; Rizza & Pereira 2013:24).

Cyberbullying can have a negative effect on the psychological and emotional well-being of children, such as higher anxiety, depression, confusion, guilt, shame, lower self-esteem, suicidal thoughts and attempts, self-harm, as well as higher rates of illness, higher absenteeism, lower academic achievement, and withdrawal from peers and family (Mishna et al. 2009:111; Popovac & Leoschut 2012:5; Lennie 2013:50; Rizza & Pereira 2013:15).

Although there is substantial research on cyberbullying as is evident from the above, relatively little is known about cyber-bystanders witnessing the bullying online (cf. Mascheroni & Ólafsson 2018:28-30).

SEXTING

The practise of ‘sexting’ (the transmitting of sexually explicit images through text messages) to other children has gained in popularity in the last few years. Sexting is the creation, sending, receiving, or forwarding of sexually explicit messages, images or photographs between mobile phones and carries tremendous risk. Quite often, these images are widely disseminated, even if not maliciously intended. It is almost impossible to remove the images from people’s phones although it may have been deleted from social media. Some proponents believe sexting is just a normal and healthy mode of sexual expression and the forming of relationships by children. However, evidence exists that highlights the negative consequences although the association between sexting

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

and risky sexual behaviour seems to be weak (Hachiya 2017:181-183; Kosenko et al. 2017:141-143, 153-154).

Many cases have been documented where a child has sent sexually explicit images in confidence to a romantic partner just to later find that it has been circulated throughout the school. Some of these cases led to the suicide of the child. Texting involves complicated ethical issues that have a fundamental influence on the welfare of children (Lennie 2013:3)

Although sexting by children may be consensual, it remains illegal in many countries to re-transmit the image, to use it as revenge porn, or to blackmail a child by threatening to forward the image. Since child pornography laws were composed long before sexting became commonplace, some countries consider the sending of sexual images by a child (even of themselves) as a criminal act under the child-pornography laws, which can result in them being placed on the sexual offenders list – a lifelong sentence (Hachiya 2017:177, 180-182).

It has also been proven that children engaged in sexting are more likely to be involved in sexual activity, often with multiple partners (Hachiya 2017:181).

ETHICAL CHALLENGES

In the past, technology has often been seen from an instrumental perspective as a tool that fulfils a specific purpose, but more recently, there is a growing understanding of the ethical nature of ICT since it impacts the well-being of people (Lennie 2013:33).

Technological improvements are often motivated under the pretext of efficiency. This has unfortunately led to 'a moral vacuum' where current principles are just not efficient enough to deal with the new moral challenges created by digital technology. Digital technology can easily exacerbate prevailing ethical problems, such as the proliferation of highly sexualised content or cyberbullying; or create

new ethical problems exclusive to the digital sphere, such as sexting (Lennie 2013:35, 42).

Although there has been some growth in scholarship with regard to ethical challenges to children, there is limited analysis of how ICT-based issues that are ethical in nature, directly affect children. And when ethical challenges are discussed, the challenges are often very superficial as in the case of Grant (2010:12) and his students. A deeper understanding of the challenges and their inherent connection to the social and human nature of digital communication are of importance to prepare children for future participation in the digital world (Lennie 2013:5, 11).

Eventually the transformative nature of technology reshapes children's self-perceptions, their relationships with other children, their perceptions of time and speed, and their way of thinking (Lennie 2013:13-14, 23-24). The cyberculture and internet, together with all the inherent dangers, can generate fear, hyper-agitation, and desensitisation amongst children (Matyjas 2008:195-196). Research indicates that the digital media pose dangers to the physical, emotional, intellectual, and behavioural development of children, as well as the functioning of the family. Excessive online activities often have a detrimental influence on the psychological development of children, often limiting physical interpersonal relationships (Matyjas 2008:196, 201).

The ethical challenge is that as our adoption of ICT increases, society increasingly submits to the sovereignty of technology, which could have an undue impact on the daily lives of children as cyberspace becomes their playground for social interaction (Lennie 2013:1; Löfberg 2003:142). For these children, information technology provides a disembodied way of living through Virtual Reality, anonymous interaction and the use of pseudonyms in chat rooms (Sando 2003:171). Dreyfus (2001:106-107) warns against this disembodied lifestyle and behaviour experienced by people (and children) in cyberspace that is partly based on a Christian-Platonic foundation:

... when we enter cyberspace and leave behind our animal-shaped, emotional, intuitive, situated, vulnerable, embodied selves, and

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

thereby gain a remarkable new freedom never before available to human beings, we might, at the same time, necessarily lose some of our crucial capacities: our ability to make sense of things so as to distinguish the relevant from the irrelevant, our sense of the seriousness of success and failure that is necessary for learning, and our need to get a maximum grip on the world that gives us our sense of the reality of things. ... Indeed ... I hope to show that, if our body goes, so does relevance, skill, reality, and meaning. (pp. 6-7)

Embodiment is a guard against false fantasies about power, invulnerability and immortality. Embodiment ensures fragility, vulnerability, the possibility of touching, empathy, and dependence on others and the material environment (Sando 2003:184).

It was Kendall (1999:60) that noted that the word 'cyberspace' has a science fiction tone and thus reflects the propensity amongst people to view the online world as an independent reality, totally independent from the real world where human beings are vulnerable. Although she believes that there is no disconnect between the real and online worlds and that people move happily between the worlds since they "perceive their identities and selves as integral and continuous" (Kendall 1999:60), it is not necessarily true of children. The body is an important ethical sensor, which helps us to be aware of the needs and vulnerability of our fellow human beings.

Therefore, any technology which proposes to overcome embodiment and vulnerability, is ethically dangerous because it does away with an important reminder of the essence of being human. What may be acquired in invulnerability and disembodiment may be lost in indifference and aggression against other people. The ethical challenge is that if embodiment is important in the formation of a child's character and online ethical behaviour, then excessive time spent in cyberspace by children seems to be problematic (Sando 2003:185-186).

Although digital technologies have many benefits (eds. Keeley & Little 2017:2), the lack of ethical values has greatly contributed to the abuse of children, amongst others, sexual exploitation, promotion

of immoral ideas and behaviours, misuse of private data, and identity theft (Aslani et al. 2013:214).

Since the start of the millennium, AI and algorithm-based information technology has grown exponentially and has improved the understanding of business operations and the quality of decision making tremendously. Unfortunately, there is also a deleterious side to the use of algorithms, which raises serious ethical concerns (Adams et al. 2018:213; Yang 2019:4-5).

The first challenge comes with the irrational belief that technology is morally neutral and that algorithms are unbiased. Although technology may have no sense of good or evil, algorithms always 'bear the fingerprints of its creator(s)', which certainly influences the models of rational analysis and decision making of the user and, therefore, creates some contentious ethical challenges. Technology often changes our relationships with one another and forms our moral and institutional values (Ephraim 2013:280). It does happen that organisational leaders interfere with developers and influence prejudice and preferences of the system (Yang 2019:4-6). The widely publicised use of big data and algorithms by Cambridge Analytica to influence public opinion, manipulate referenda and elections, is a good example of misuse. Such use is an erosion of social justice and, in essence, threatens democracy, especially when used on children (*The Guardian* n.d.; Yang 2019:6).

A second challenge is the use of nudging theory. Nudging is widely used by online companies such as Takealot's 'You might also like ...' and Netflix's 'Because you have seen ...' and can assist decision makers to make better decisions by limiting the number of choices. Unfortunately, nudging is also used to influence the decision of buyers and often steer them to more expensive services and products, which often leads to the exploitation of unsuspecting children (Yang 2019: 18-20).

Although some progress has been made, a third ethical challenge is that algorithms are not yet very successful in judging human values, which could lead to a sacrifice of fairness and justice due to an inability to distinguish between good and evil. It is thus possible that in the

self-development of algorithms they become destructive (Young 2019: 24-25).

A fourth ethical challenge is the Search Engine Manipulation Effect (SEME) that entails the manipulation of search engine results by search engine providers, as well as the ‘echo chamber’ effect on social media, which can easily limit the critical thinking and freedom of choice of children (Epstein & Robertson 2015:E4512-E4513, E4518-E4520; Krasodonski-Jones 2016:6, 33-35; Bergen 2017).

Industry and government will have to ensure that better values and models based on current ethical guidelines are built into algorithms even if it puts fairness ahead of profit (O’Neil 2016:202; Yang 2019:26). IBM, in 2019, published the *Everyday Ethics for Artificial Intelligence* where they state: “Ethics must be embedded into the design and development process from the very beginning of AI creation” (IBM 2019:8). Due to the rapid evolvement of AI technology in terms of capabilities and impact on especially children, AI systems’ designers and developers must understand the ethical concerns involved in their work (Yang 2019:40). The ethics around AI and algorithms need serious consideration and should guide all AI and algorithm design and development (Adams et al. 2018:216).

Current practices in the use of AI, big data and algorithms have many major ethical and societal implications, with particular reference to children. Although many of the other online challenges have been addressed to some extent, little agreement currently exists on core ethical issues and frameworks underpinning the ethical approach to the development and deployment of these technologies. Often the algorithms are based on such complex internal logic or have developed via deep learning that even developers do not fully understand the logic (Whittlestone et al. 2019:1-2, 20).

Rizza and Pereira (2013:22) refer to social media as dwellings where children act out their lives, construct and negotiate cultural meanings and develop their identities. But it is exactly here that ethical challenges arise. Ethical values, such as autonomy, identity, integrity, responsibility, privacy, freedom, informed consent and justice are

contested by the current development and use of ICT. ICT tools are changing normative ethics and ethical behaviour.

In many national legal systems, every person's right to a personal identity has been entrenched. However, in the digital world, identity has become fluid, dynamic and flexible making it possible for children to be who they wish to be. In the online world, it is possible for a child to have multiple identities. Cyberbullying, for instance, precisely challenges this identity of the child (Rizza & Pereira 2013:23-24). Unfortunately, current regulations are not focusing on addressing violations of a child's identity and reputation and tend to rather focus on privacy.

Since social media do not adhere to the traditional protection against excesses, such as respect for other children, to be careful of strangers and to adhere to certain limits with regard to relationships. Ephraim (2013:280-281) suggests a culture-centred approach that maintains cultural and ethical values and standards, which inter alia include the qualities of compassion, respect for human dignity, and the right to privacy.

COUNTER MEASURES

A SHARED RESPONSIBILITY

The task of ensuring the safety of children online is so complex that a concerted multi-stakeholder collaborative approach between parents, peers, teachers, children, communities, schools, civil society, industry, government, NGOs, international organisations and law enforcement is needed to ensure effective protection of children in the digital domain. Increasing the awareness among children, families, religious communities, the ICT sector, media and government will break the ignorance around child sexual abuse (O'Neill 2013a:258; eds. Keeley & Little 2017:89). In particular, collaboration between the technology

industry and law enforcement is essential to limit online child abuse and exploitation (eds. Keeley & Little 2017:6, 9, 11).

PARENTAL RESPONSIBILITY

In order to protect children from the dangers of the digital world, parents should teach their children to use the internet in a focused manner. But perhaps the most important point is a genuine interest in their children's experiences in the complex digital world and open discussions and guidance around the challenges they experience (Matyjas 2008:204; eds. Keeley & Little 2017:69). Parents need to pay attention to the online activities and make time to be with their children while they are online. They should watch for signs of meanness and act immediately by blocking and reporting the bullying or exploitation of their child (Ephraim 2013:283; eds. Keeley & Little 2017:89).

The exponential development of technology, and, in particular, the lack of a proper distinction between the real and the virtual worlds, has affected the essence of families. Cyber space became a fundamental part of the living space of families and with it came the many challenges of abuse, manipulation and exploitation (ITU & UNICEF 2015:9-10, 13; Minić & Spalević 2014:424-425, 427-428). However, parents often feel overwhelmed due to a lack of awareness, digital knowledge and competence, which makes it difficult for them to take control of their children's digital lives or to effectively protect them online (O'Neill 2013a:257; Livingstone et al. 2015:13; Livingstone et al. 2017:83, 99). Since parents are gateways to child online safety, cyber training to improve their digital understanding and skills is important in the detection and handling of online dangers (eds. Keeley & Little 2017:88-89; Livingstone et al. 2017:100-101).

Since children are often unaware of the importance of privacy settings and its possible consequences, parents must ensure that the default privacy settings are set for the maximum protection of the privacy of their children (EC 2012:10-11). Parents could also consider the use of parental controls and teach their children to keep profiles private by setting it to only allow viewing by friends and family (eds.

Keeley & Little 2017:89). Verifiable parental consent could be used for children under a certain age (EC 2012:10-11). However, parents should not use technical tools to escape their obligation of talking to their children about inappropriate and dangerous online sexual behaviour (Staksrud & Kirksæther 2013:32).

In a study undertaken in South Africa, 43.6% of children stated that they would almost never speak to their parents about what they do on the internet and only 8.6% very often or often talk to their parents about disconcerting online issues. A large number of children can also use a webcam (42.1%), download music or films (71.9%) or visit a social networking site (65.3%) without parental supervision (Phyfer et al. 2016:117-118). Although parenting may be different in different parts of the world, parents will have to become engaged in their children's internet activities.

Just as parents establish temporal and geographic restrictions with regard to physical spaces in order to protect their children from harm, they should set clear time and space limits with regard to the internet and should be informed what their children are doing or whom they are visiting (Valentine & Holloway 2001:76-77). Parental responsibility changes according to the age and development level of the child. Just as parents will not let a young and inexperienced child cycle unaccompanied on a busy road or without a helmet, similarly equivalent precautions should be taken before a young child is allowed onto the highway of the internet (O'Neill 2013a:259).

THE VALUE OF PEER SUPPORT AND COMMUNITIES

According to research, children should be encouraged to show empathy and support each other when abused. If possible, they should become 'upstanders' against abuse and cyberbullying (eds. Keely & Little 2017:108). Experience has proved that one of the best ways to address the dynamic phenomenon of cyberbullying and other exploitation of children, is to increase awareness through the use of children and to give compelling support to the process. This should be followed up by

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

the creation of safe spaces where children could discuss the challenges they experience online (Rizza & Pereira 2013:8).

The appointment of cyber mentors or virtual peer support has proved valuable. The online mentoring by peers is anonymous and protected by a software filter, while being monitored by senior cyber mentors (Mishna et al. 2009:107).

THE ROLE OF THE SCHOOL

Digital and media literacy should be taught in all schools from the very early years to keep children informed and safe online and should go beyond technical skills (EC 2012:8). It should include how children could protect themselves from online dangers, such as cyberbullying and sexual abuse by not sharing photos or filling out personal details on online forms. They should understand the risk of creating and sharing content and that every post online (text, photo or video) is no longer private and possibly cannot be erased. Especially self-generated content, such as sexually explicit material exposes them to the risk of cyberbullying or extortion and may be distributed all over the internet. Children should understand how important it is to protect their personal information (eds. Keeley & Little 2017:128-129).

Research indicates that although children are aware of online risks and dangers, they mostly describe their risks in terms of operational user problems or media-hyped fears. Schools should, therefore, systematically educate children regarding online dangers, risks and e-safety to ensure that they become responsible digital citizens (Cranmer et al. 2009:127; Mishna et al. 2009:107; DQ Institute 2018). They should be enabled to take responsibility for their online behaviour; to practice safety; to protect their data and devices; to establish healthy social relationships with others; and to use digital technology and media in a disciplined way (eds. Keeley & Little 2017:3; DQ Institute 2018).

Teachers, trained in the use of appropriate monitoring and filtering software, could be assigned as internet safety coordinators (Cranmer

et al. 2009:129). Since cyberbullying often emerges within the school environment, schools can play a substantial role in addressing the phenomenon through social and emotional learning (Rizza & Pereira 2013:20; Wojniak & Majorek 2016:133).

LEVERAGE THE POWER OF THE PRIVATE SECTOR

Since the private sector plays a key role in the digital revolution, businesses have become integrated into the lives of children and should, due to their power and influence, play a much greater role in protecting children by removing unsuitable content (eds. Keeley & Little 2017:129). Especially internet service providers (ISPs) and content providers play a significant role in respect to corporate responsibility practices to ensure the safety of children through the promotion of ethical standards on data and privacy (Ephraim 2013:283; Ságvári & Máder 2013:155-156; eds. Keeley & Little 2017:3, 11). Companies should integrate child rights into all corporate policies and management processes (ITU & UNICEF 2015:12).

The presence of large numbers of underage children on services (and websites) originally intended for adult audiences creates a huge embarrassment for many digital companies. Although companies, such as Facebook, would not readily admit to the problem, they apparently delete about 20 000 accounts of children under 13 years per day that provided false information about their age (O'Neill 2013a:255). Social media networks, therefore, should assist in child safety by providing 'report abuse' buttons, enforcing strict age limits for new user accounts, using filtering technologies, creating child safety zones on the internet and thorough age and identity verification (Graafland 2018:39).

Based on the legal principle of the 'duty of care', companies must do much more to take reasonable care so as not to harm the children who use their online services even if not legitimately registered (O'Neill 2013a:255). It is just not enough for companies, such as Facebook, to state that they cannot guarantee that the platform is safe and that people use it at their own risk. Even if there is no legal obligation on online companies, such as Facebook, to accept responsibility for underage

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

child users, there is unquestionably an ethical obligation under common law to exercise a due standard of care and ensure the safety of their service given the high prevalence of underage users. Verification of age should not only rely on technical methods, but also involve the parents and undertake awareness campaigns (O'Neill 2013a:256). Technology companies could also, in collaboration with government, create a system of content classification and corresponding age rating for all services, and integrate it with parental controls (EC 2012:12). Unfortunately, many parents allow their underage children to create social networking accounts. It thus seems futile to state that parents should have the final say if their child could open a social networking account (O'Neill 2013a:254).

Service providers could make their platforms more suitable for underage children by limiting the visibility of profiles through a default private setting (O'Neill 2013a:255). Companies should adjust technology according to current ethics (Rizza & Pereira 2013:8). A good example of how technology can be customised to assist with intentionality is the decision of a German state to prohibit the Facebook 'Like' button because it allows illegal profiling and violates privacy laws (Mack 2011).

As a major driving force of the Fourth Industrial Revolution, the ICT industry is ethically bounded by the obligation to place the protection of children at the very heart of all technological innovation and to develop industry standards to ensure the safety of children accordingly (ITU & UNICEF 2015:12; eds. Keeley & Little 2017:69). Industry should create a safe online environment for children by implementing age appropriate privacy settings (Wojniak & Majorek 2016:134-35; eds. Keeley & Little 2017:89). Technology companies should also share their knowledge, expertise and digital tools with law enforcement agencies to improve the protection of children online. Parents could be assisted with tools, such as filtering, blocking and age verification (eds. Keeley & Little 2017:126-127, 130).

ETHICAL DESIGN AND PRIVACY

It is well known that technologies are often purposely designed to exploit human or child weaknesses, psychological biases or vulnerabilities, such as the need for social acceptance or the fear of rejection. Technology companies will have to reconsider their designs to ensure that they are ethical and not only focused on the exploitation of children for financial gain. They should embrace the principle of safety-by-design that incorporates security, safety and privacy features into their products (O'Neill 2013a:259; Rizza & Pereira 2013:28-29; eds. Keely & Little 2017:108, 129-130). Ethics must thus “be embedded in the design and development process” (IBM 2019:8).

Privacy is of the utmost importance where children are involved. Proper protection of the privacy of children necessitates an alignment between technology and regulation. For instance, social media will have to consider simple functionalities, such as the giving of consent to others to publish information, as well as undo and redundancy functions (Rizza & Pereira 2013:26).

The large technology and advertising companies will have to balance their use of personal data to improve the quality and efficiency of services versus respecting the privacy and autonomy of individuals; automation for convenience versus self-actualisation and dignity; as well as ensure that the algorithms are not biased and treat all children fairly and equally (Whittlestone et al. 2019:2).

One of the major concerns with regard to AI, big data and algorithms is that it is fairly easy to change the original purpose for which it was created, essentially modifying their ethical valence. Although supposed to be domain-neutral, the information acquisition and processing, and decision-making techniques of AI, as well as big data and algorithm technologies, can become progressively pervasive in the lives of children. There is indeed a need for regulation in this regard to protect vulnerable children (Whittlestone et al. 2019:8, 11).

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

TECHNOLOGY TOOLS

Several technology tools could be used to monitor children's activities and to filter prohibited connections and websites (Valentine & Holloway 2001:77-78; cf. Grant 2010:9). New forensic tools using AI can also assist in curbing the sexual abuse of children. Systems are available that can monitor peer-to-peer (P2P) network activity and will furnish the identity of sharers of child sexual abuse material, as well as their geolocation. Profiling and semantic recognition can be used to detect abusive content, behaviour and cyberbullying (Rizza & Pereira 2013:21-22).

Since Microsoft donated its PhotoDNA technology to the International Centre for Missing and Exploited Children and it was integrated with INTERPOL's International Child Sexual Exploitation (ICSE) database, it is possible to search for the unique signature or digital fingerprint of any online image (eds. Keeley & Little 2017: 88-89).

In Europe, the tool iCOP has been developed to detect new or previously unknown child sexual abuse material that is shared on P2P networks. iCOP performs live forensic analysis through the use of AI and machine learning to compare hundreds of thousands of files to detect recent or on-going child abuse (eds. Keeley & Little 2017: 88-89).

THE ROLE OF GOVERNMENT

To enable children to effectively deal with online risks of sexual abuse, it is important that the state should establish adequate mechanisms for the reporting of abusive content and contacts (EC 2012:9). As part of their Safer Internet Action, the European Union and Canada established national hotlines to allow children to anonymously report content that is believed to be illegal (Mishna et al. 2009:107). Although hotlines play an important role as a reporting mechanism, it can never be the sole solution. Alternatively, many countries filtered, and blocked sites containing sexual abuse material of children and

use software detection tools and upload filters at the level of internet service providers (O'Neill 2013b:39, 41-45, 48, 51-52; Wojniak & Majorek 2016:134).

The state should also scale up awareness amongst all children, parents, and teachers to make them cyber-aware and ensure that peer education amongst children is promoted (eds. Keeley & Little 2017:89). In Europe, awareness centres, promoting safe and responsible internet and cell phone use, are used with great success (Rizza & Pereira 2013:11; eds. Keely & Little 2017:108).

Government law enforcement could also build profiles of potential perpetrators, their signature moves, and aggressive terminology and patterns of dominance in online conversations to make it more difficult for them to hide behind multiple digital personas.

Although some policy makers worldwide are addressing the online risks that are endangering children, countries in Africa and South Africa are unfortunately often lacking behind with the formulation of policy frameworks and national strategies regarding the online safety of children. South Africa needs a common ICT strategy and a standardised and integrated approach to uphold children's rights and preserve child safety online.

LEGAL PROTECTION

In June 2016, internet access was recognised as one of the basic human rights (Human Rights Council 2016:4, 53-55). However, due to the exponential growth in ICT and high rate of internet adoption, the policy, governance and legislative frameworks, determining online access and use, could not keep up and are mostly territorial (Bulger et al. 2017:751).

Children's right to protection when they go online is an internationally entrenched principle in laws that protect children from online exploitation and maltreatment (Bulger et al. 2017:751). These laws mostly build on the decisions of the United Nations (UN) Convention on the Rights of the Child (UN 1989) in the digital age

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

and include inter alia their rights to freedom of expression of views, thoughts, beliefs and opinion (UN 1989 articles 12-14); freedom of association and participation (Article 15); the right to privacy and protection against unlawful attacks on their honour and reputation (Article 16) and the right to protection “from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse” (Article 19) (UN 1989). It is the responsibility of government to develop legal and policy frameworks to protect the child as legitimate rights-holder with full human rights (Livingstone et al. 2015:9; Bulger et al. 2017: 751-752).

Often, countries included special provisions within existing laws and regulations to fulfil the above-mentioned obligation and to protect children from online exploitation and abuse. Most countries, therefore, criminalised the creation, dissemination and consumption of Child Sexual Abuse Material (CSAM or child pornography) and the online solicitation and grooming of children. Access to certain harmful content is also restricted, such as gambling and ‘adult’ pornography (Bulger et al. 2017:751-752).

Graafland (2020:39) is of the opinion that “the majority of risks that exist both online and offline, existing laws and regulation apply and no additional laws are needed.” However, it is not enough to merely adapt current laws to make what is illegal offline also illegal online. What is needed is to think anew from the traditional elements of the crime, such as activity, intention, unlawfulness, knowledge of unlawfulness and prejudice, to create new offences based on the inherent features of cyber characteristics. From the very essence of cyber-activities, it is important to anticipate criminal activity and, therefore, to create offences based on the early phases of criminal activity. Especially with regard to the protection of children, it is important that a new offence is created by penalising the introduction to a crime as opposed to a completed crime where the consequences are irreversible. By approaching crime on this basis, criminality is created on the basis of the anticipation of a crime as opposed to a traditionally completed offence, which is judged by the consequences

of such crimes. The intention of this pre-emptive approach is to strengthen the deterrent and preventative feature of crime as opposed to the penal feature (Fourie, Heath & Fourie 2011).

Some countries do make an effort to think innovatively, such as France, that made the filming and online distribution of violent acts ('happy slapping') a crime. Japan made it illegal to arrange dates with minors who have been met on dating websites. Australia, Ireland, Norway, France, the UK, New Zealand and Japan promulgated legislation with regard to cyber-grooming (Graafland 2018:39). But although children comprise a third of internet users in the world, most national policies focus on the adult user, while broader national policies focusing on the child do not adequately address the challenges accompanying digital technologies. It is important that children be included in all ICT regulation, policies and acts (ITU & UNICEF 2015:6-7; eds. Keeley & Little 2017:130).

Government needs to enact laws criminalising all forms of sexual abuse and exploitation of children, with particular reference to online abuse (eds. Keeley & Little 2017:88-89). Unfortunately, the transnational nature of internet services and providers limits the power of governments to fully address the challenges experienced by children online (Livingstone et al. 2015:13). Due to the exponential development of technologies, especially in the fourth industrial era, technological developments often outpace ethical frameworks and legal definitions. It would, therefore, be more appropriate for countries to adopt tech-neutral policies and definitions (Graafland 2018:39).

In South Africa, legislation focuses only on the general protection of children, together with some civil and criminal legislation basically relevant to ICTs. Unfortunately, the environment for children's rights and protection in the digital era is seriously wanting in South Africa. Legislation with regard to the online safety of children is at best limited, fragmented and sometimes even contradictory (Bulger et al. 2017:754). The South African Law Reform Commission (2015:24-47) expressed serious concerns regarding the creation, distribution and exposure of children to child abuse material, as well as sexting by children and the online grooming of children by adults. The commission, therefore,

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

initiated a discussion on law reform in this regard and pointed out several important gaps regarding the protection of children in current South African Law, such as the inadequacy of some definitions, the lack of criminalising of certain online activities, the fragmentation of the protection of children, and the inadequate protection of children with regard to online abuse (:55-137).

The *Children's Act* (RSA, Act No. 38 of 2005) has been revised after public consultation in *The Children's Amendment Bill* of 2019 (RSA 2019b) and did attempt to align the *Children's Act* with the *Criminal Law (Sexual Offences and Related Matters), Amendment Act*, 2008, for example with regard to a child's right to privacy (RSA, Act No 5 of 2015:15). However, with regard to the protection of children against exploitation and abuse, the amended bill is at best insufficient and does not really address or cross-reference cyber dangers.

The protection of children from online sexual abuse received worldwide attention and led to several initiatives, such as the United Nations Convention on the Rights of the Child (UN CRC) and the resultant Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography; the Council of Europe's Convention on Cybercrime; and the Global Alliance Against Child Sexual Abuse encompassing 52 countries. Together, these initiatives have made the distribution of inappropriate child abuse materials illegal. Although South Africa aligned itself with these international principles (Bulger et al. 2017:755), much of the practical implementation must still be seen.

In the USA, child pornography is defined as any visual depiction of sexually explicit conduct involving a person less than 18 years of age. "Misleading domain names" and "misleading words or images on the internet" that may cause children to unintentionally view explicit child abuse material online are prohibited (US Department of Justice 2015). The European Union also includes 'virtual child pornography' and 'grooming' in their 2011 directive to member states (Bulger et al. 2017:755-756).

In South Africa, legislation addressing child pornography was promulgated in 1996 as the *Film and Publications Board Act* (RSA, Act

No. 65 of 1996) and amended in 2019 in the *Film and Publications Board Amendment Act* (RSA, Act No. 11 of 2019) to align the definition of child pornography with the Criminal Law Act. The definition of the “distribution” of online material was expanded to include content streaming and that of “harmful” to include “emotional, psychological and moral distress.” The term “hate speech” referring to “any speech, gesture, conduct, writing, display or publication, made using the internet ..., which propagates, advocates or communicates words against any person or identifiable group ... to incite harm and promote or propagate hatred...” has been included. Amendments to the *Film and Publications Board Act* in 2019 provided much more extensive definitions of sexual abuse images of children, as well as the inclusion of revenge pornography (RSA, Act No. 11 of 2019). Unfortunately, current definitions in South African legislation do not include the downloading of an image on any digital device (Bulger et al. 2017:756).

South Africa has further criminalised the exposure of children to pornography and acts of sexual grooming of children under the *Criminal Law (Sexual Offences and Related Matters) Amendment Act* (RSA, Act No. 5 of 2015), which included online sexual offences. The Justice Alliance of South Africa (JASA) has been working without much success on an Internet and Cell Phone Pornography Bill that endeavours to totally ban pornography from the country by ensuring that it is filtered out at Tier One service providers (South African Law Reform Commission 2015:138-139, 148).

However, the online behaviour of children and in particular youth-produced and shared sexual content, bring several new challenges in the protection of children and overlaps with the legal definition of adults involved in offensive practices (Bulger et al. 2017:756). Legislative frameworks are often too narrow in their approach to properly address the complexities of children’s online experiences and usually depart from children as vulnerable victims, thus disregarding their agency and participation (Livingstone et al. 2015:5). Sexting or the distribution of nude images among children is, for example, considered a criminal offence in some countries and can lead to prosecution, punishment

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

and listing as sex-offenders of adolescents (UNICEF 2012:54, 79–80; Byrne, Albright & Kardefelt-Winther 2016:6).

In Europe, the child online safety emphasis has shifted from a focus on protection and restriction to a greater focus on awareness and the empowerment of children and parents (Mascheroni et al. 2013:218). Instead of trying to provide a safer internet for children, the aim is shifting to a better internet service for children (EC 2012:2-17). Other regions, and in particular Africa, still need to make this change in focus from a safer to a better internet. The complexity of the challenge calls for a holistic approach to child rights based on evidence (reliable data) and not on the traditional approach of combating child sexual abuse often based on sensational incidents and media reports (UNICEF 2012:11; Livingstone 2013:103-106; Livingstone et al. 2015:16-17). The Centre for Justice and Crime Prevention in South Africa has done excellent evidence-based work regarding the barriers, opportunities and risks experienced by South African children (Phyfer et al. 2016:1-129).

Children are not only a vulnerable group, but also active participants, agents and creators of online content. Policy makers will have to tend to rigorous investigation and much more detailed and credible data about the use of digital technology by children, as well as their real-life circumstances and social norms (Byrne & Burton 2017:41-43).

Unfortunately, South Africa lacks an overarching policy on ICT and children. Policies are currently scattered over a number of sectors, for example education, cybersecurity, child welfare and protection, and are often handled by different departments and ministries, while the impact is rarely measured (Byrne & Burton 2017:47-48). Existing South African legislation is at best ineffective to combat online child abuse. South Africa is in need of a new law that specifically deals with the “creation, possession and distribution of child abuse material” (South African Law Reform Commission 2015:146-147).

CYBERBULLYING

Cyberbullying is often incorrectly framed as a privacy issue, but should rather be seen as an identity-related ethical issue. If it is seen as a privacy issue, policy strategies focus on data protection. While the right to privacy entails the suppression of private aspects of children from public knowledge, the right to identity entails the dissemination of information of children to the public sphere without authorisation and in ways that cannot be reconciled with their identity or public image. Government would thus do better by focusing their policies on the identity rights of children (Rizza & Pereira 2013:26, 31).

In order to combat cyberbullying, a multi-dimensional strategy and holistic approach should be followed since cyberbullying is never just online. Parents, the school, peer groups, social services and the media could play an important preventative role to change the values, beliefs and behaviour around cyberbullying (Rizza & Pereira 2013:15-16, 18, 21).

HARVESTING OF DATA

The widespread gathering of personal data by the large technological and advertising companies *inter alia* through tracking, facial and voice recognition raises many concerns and will have to be addressed. Privacy is a human right and not a commercial concession. However, views on privacy rights differ between the USA, UK, Continental Europe, Asia, Africa, Latin America, as well as between political structures.

Threats to privacy are constantly arising – especially from the commercial and security sectors, and social networks (Stückelberger 2014:22) leading to the following concerns that need to be addressed:

- Any collection of information about an individual or child should only take place with the knowledge and consent of the individual or parent. It is an open question if the Fair Information Practice Principles (FIPPs) found in

current privacy policies are effective at all (Regan & Jesse 2019:175).

- Children have the right to remain anonymous and unidentified. This right is often protected in law by a clause on 'personally identifiable information' or information directly related to a specific individual. However, with multiple data points per person, big data, artificial intelligence algorithms and data analytics, it is almost impossible to remain anonymous (Regan & Jesse 2019:177-179). Legislation will need to be adapted accordingly. Although the *Protection of Personal Information Act* (RSA, Act No. 4 of 2013) of South Africa, promulgated in 2013, does provide significant protection with regard to the collecting, storing, processing and sharing of personal information, little has yet been done regarding its implementation since government has failed to appoint a regulator.
- Analytics powered by big data increasingly challenge individual autonomy. Algorithms, for instance, lead and nudge children to buy specific items and use specific routes or restaurants. The danger is that children are subjected to a continuous loop without freedom to make their own decisions. The danger with nudges is that they manipulate children (Regan & Jesse 2019:179-180).
- Big data uses algorithms and AI to make predictions about individuals. But research has shown that algorithms can be biased and can thus discriminate on the basis of race, gender, age or other personal traits (Regan & Jesse 2019:180-181, 188-189). Companies will have to ensure that their algorithms are free of bias and treats all people fairly and equally.

Data generated through digital tracking and the use of social media is often used for profiling of children and inappropriate marketing and advertising. Several new electronic toys are also connected to the internet and transmit data about the thoughts and feelings of children to toy manufacturers. It is important to establish safeguards, such as data anonymisation, encryption, secure data storage, and the prohibition of the use of data without consent, to protect the privacy of children. The privacy settings of children should by default be set to maximum. Technology and advertising companies should not monetise the information of children and should protect data, such as the child's location and browsing habits (eds. Keeley and Little 2017:127-128).

CONCLUSION

We live in a time, where the confluence of real and virtual worlds creates new contexts and ontologies that we are continuously struggling to fully comprehend. Our ethical values, according to which we act and use technology, are constantly put to the test. The problem is that we have often left this debate to the corporates and their developers who largely have profit as their main goal (Rizza & Pereira 2013:29).

The ethical debate cannot be left to the corporates to decide according to which values children should live (Rizza & Pereira 2013:30). The internet and social media have an impact on the social development of the child and the broader society. A multi-stakeholder approach is, therefore, necessary to protect the child in this volatile and often pervasive and dangerous virtual world of dangers and uncertainties and to ensure that it rather becomes an important source of opportunity and empowerment where children can become the authors of their own future (Third et al. 2017:3). This approach entails an essential role by the parents, as well as the support of industry, school, NGOs and government.

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

Although the internet and social media were originally designed for adults, children are increasingly using it. Digital laws, policies, practices, guidelines and technology products should in future better reflect children's need and ensure their safety (Third et al. 2017:18). Many safety issues around content, contact and conduct on the internet need to be addressed – in particular the issue of the unauthorised use of social media by underage children (Neill 2013a:260).

The growing use of data collection and algorithms by large marketing and advertising firms to influence children in a vulnerable period of their lives is of great concern. Wide legal protection against commercial data collection is afforded to children in many countries, but enforcement is markedly poor. Authorities and industry will have to pay greater attention to software design aspects of the services rendered to children. Minimum safety standards underpinned by ethics and ethical accountability should be enforced to reduce the risks to children (Neill 2013a:260).

If stakeholders do not take the harming of children through technology at least as serious as offline risks, it has the ability to spiral out of control and even mobilise violence on a massive scale. This sadly transpired recently in Myanmar when a social media campaign resulted in horrendous violence against members of the Rohingya ethnic minority, which led to the killing and mutilation of many children and hundreds of thousands of refugees (eds. Keeley & Little 2017:vi).

Zembe-Mkabile, W., Surrender, B., Sanders, D., Jackson, D. & Doherty, T. 2015. The experience of cash transfers in alleviating childhood poverty in South Africa: Mothers' experiences of the child support grant. *Global Public Health*, 10(7):834-851.

CHAPTER 10

Adams, K., Encarnação, P., Rios-Rincón, A.M. & Cook, A.M. 2018. Will artificial intelligence be a blessing or concern in assistive robots for play? *Journal Human Growth Development*, 28(2):213-218. DOI: <http://dx.doi.org/10.7322/jhgd.147242>.

Aslani, G., Senobari, M., Rostaminejad, M.A. & Jafari, E.M. 2013. Identification and management of ethical challenge in e-learning systems. *Procedia – Social and Behavioural Sciences*, 83:214-218. DOI: <http://doi.org/10.1016/j.sbspro.2013.06.042>.

Barbovschi, M. & Dreier, M. 2013. Vulnerable groups of children, 60-63. In: M. Barbovschi, L. Green & S. Vandoninck (eds.). *Innovative approaches for investigating how children understand the risk of new media. Dealing with methodological and ethical challenges*. EU Kids Online & London School of Economics and Political Science, London.

Bergen, M. 2017. Inside Google's struggle to filter lies from breaking news. *Bloomberg Businessweek*, 16 November. Viewed 10 February 2020, from <https://www.bloomberg.com/news/articles/2017-11-16/inside-google-s-struggle-to-filter-lies-from-breaking-news>.

Bulger, M., Burton, P., O'Neill, B. & Staksrud, E. 2017. Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online. *New Media and Society*, 19(5):750-764. <https://doi.org/10.1177/1461444816686325/>.

Byrne, J. & Burton, P. 2017. Children as internet users: how can evidence better inform policy debate? *Journal of Cyber Policy*, 2(1):39-42.

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

- Byrne, J., Albright, K. & Kardefelt-Winther, D. 2016. *Using research findings for policy-making*. Global Kids Online, London. Viewed 20 November 2019, from <http://globalkidsonline.net/wp-content/uploads/2016/05/Guide-11-Policy-making-Byrne-Albright-Kardefelt-Winther.pdf/>.
- Clement, J. 2020. Worldwide digital population as of January 2020. Viewed 16 February 2020, from <https://www.statista.com/statistics/617136/digital-population-worldwide/>.
- Cranmer, S., Selwyn, N. & Potter, J. 2009. "Exploring primary pupils' experiences and understandings of "e-safety". *Educational Information Technology*, 14:127-142. DOI: <http://doi.org/10.1007/s10639-008-9083-7>.
- Dreyfus, H. 2001. *On the internet*. Routledge, London and New York.
- DQ Institute. 2018. Outsmart the cyber-pandemic: 2018 DQ Impact Report. DQ Institute. Viewed 8 January 2020, from https://www.dqinstitute.org/2018DQ_Impact_Report/#Cyber-Pandemic.
- Ephraim, P.E. 2013. African youths and the dangers of social networking: a culture-centered approach to using social media. *Ethics and Information Technology*, 15:275-284.
- Epstein, R. & Robertson, R. 2015. The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. In: *Proceedings of the National Academy of Sciences of the United States of America*, 112(33):E4512-E4521. Viewed 6 January 2020, from <https://www.pnas.org/content/suppl/2015/08/03/1419828112.DCSupplemental>.
- European Commission (EC). 2012. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European strategy for a better internet for children. COM/2012/0196 final. European Commission, Brussels. Viewed 28 December 2019, from <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52012DC0196>.

REFERENCES

-
- Fourie, L.C.H. 2020. End of privacy as an afterthought. *Business Report*, 7 February. Viewed 17 February 2020, from <https://www.iol.co.za/business-report/technology/end-of-privacy-as-an-afterthought-42261230>.
- Fourie, L.C.H., Heath, W. & Fourie, J.L. 2011. Cyber-jurisprudence and social networking. Paper presented at the Defence, Science and Research Conference (DSR 2011), Singapore, 3-5 August.
- Graafland, J.H. 2018. New technologies and 21st century children: Recent trends and outcomes. *OECD Education Working Papers*, 179, EDU/WKP 15. OECD Publishing, Paris. Viewed 20 January 2020, from [https://one.oecd.org/document/EDU/WKP\(2018\)15/en/pdf](https://one.oecd.org/document/EDU/WKP(2018)15/en/pdf).
- Grant, C.T. 2010. Successful engagement of undergraduate Information Technology Management students in a compulsory course in ethical issues in IT in a large class environment. *Information Systems Education Journal*, 8(66):3-16.
- Hachiya, R.F. 2017. Dangers for principals and students when conducting investigations of sexting in schools. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, 90(5-6): 177-183.
- Human Rights Council. 2016. The promotion, protection and enjoyment of human rights on the Internet: draft resolution. In: *United Nations General Assembly Human Rights Council 32nd Session, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: A/HRC/32/L.20*. Viewed 16 January 2020, from http://www.ohchr.org/documents/HRBodies/UPR/A_HRC_32_2_EN.docx.
- IBM. 2019. Everyday ethics for artificial intelligence. IBM Corp. Viewed 10 February 2020, from <https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf>.

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

- ITU & UNICEF. 2015. Guidelines for industry on child online protection. ITU & UNICEF, Geneva. Viewed 11 Feb 2020, from https://www.unicef.org/csr/files/COP_Guidelines_English.pdf.
- Keeley, B. & Little, C. (eds.). 2017. *The state of the world's children 2017: Children in a digital world*. UNICEF, New York. Viewed 3 January 2020, from https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf.
- Kendall, L. 1999. Recontextualizing cyberspace: Methodological considerations for on-line research, 57-75. In: S. Jones (ed.). *Doing internet research*. Sage, Thousand Oaks & London.
- Krasodonski-Jones, A. 2016. Talking to ourselves? Political debate online and the echo chamber effect. Demos. Viewed 15 December 2019, from <https://www.demos.co.uk/wp-content/uploads/2017/02/Echo-Chambers-final-version.pdf>.
- Kosenko, K., Luurs G. & Binder, A. 2017. Sexting and sexual behavior, 2011-2015: A critical review and meta-analysis of a growing literature. *Journal of Computer-Mediated Communication*, 22(3):141-160. DOI: <http://dx.doi.org/10.1111/jcc4.12187>.
- Lennie, S. 2013. Ethical complexities in the virtual world: Teacher perspectives of ICT based issues and conflicts. D.Phil. thesis, University of Toronto, Toronto.
- Lin, Y. 2019. 10 Internet statistics every marketer should know in 2020. Viewed 16 January 2020, from <https://www.oberlo.co.za/blog/internet-statistics>.
- Livingstone, S. 2013. "Knowledge enhancement": The risks and opportunities of evidence-based policy, 93-109. In: B. O'Neill, E. Staksrud & S. McLaughlin (eds.). *Towards a better internet for children? – Policy pillars, players and paradoxes*. Nordicom, Göteborg. Viewed on 18 November 2019, from https://www.nordicom.gu.se/sites/default/files/publikationer-hela-pdf/toward_a_better_internet.pdf

REFERENCES

- Livingstone, S. & Haddon, L. 2009. Introduction, 1-15. In: S. Livingstone & L. Haddon (eds.). *Kids online: opportunities and risks for children*. The Policy Press, Bristol. Viewed on 27 November 2019, from https://www.researchgate.net/publication/265491994_Conclusion_kids_online_opportunities_and_risks_for_children/.
- Livingstone, S., Carr, J. & Byrne, J. 2015. One in three: Internet governance and children's rights. *Paper Series 22*. Centre for International Governance Innovation and The Royal Institute of International Affairs, Waterloo, Ontario & London.
- Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. 2011. Risks and safety on the internet: The perspective of European children: Full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. EU Kids Online Network, London.
- Livingstone, S., Kirwil, L., Ponte, C. & Staksrud, E. 2014. In their own words: what bothers children online? *European Journal of Communication*, 29(3):271-288. DOI: <http://doi.org/10.1177/0267323114521045>.
- Livingstone, S., Ólafsson, K., Helsper, E.J., Lupiáñez-Villanueva, F., Veltri, G.A. & Folkvord, F. 2017. Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. *Journal of Communication*, 67(1):82-105. DOI: <http://doi.org/10.1111/jcom.12277>.
- Löfberg, C. 2003. Ethical and methodical dilemmas in research with/on children and youths on the net. In: M. Thorseth (ed.). *Applied ethics in internet research*. Norwegian University of Science and Technology, Trondheim. Viewed on 28 November 2019, from http://www.hf.ntnu.no/fil/anvendt_etikk/eng/.
- Lupton, D. & Williamson, B. 2017. The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, 19(5): 780-794. DOI: <http://dx.doi.org/10.1177/1461444816686328>.

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

- Mack, E. 2011. Facebook's "like" button illegal in German state. *Cnet*. Viewed 15 February 2020, from <https://www.cnet.com/news/facebooks-like-button-illegal-in-german-state/>.
- Mascheroni, G. & Ólafsson, K. 2018. *Accesso, usi, rischi e opportunità di internet per i ragazzi italiani. I risultati di EU Kids Online 2017*. EU Kids Online & OssCom. Viewed on 12 December 2019, from <http://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-Italy-report-06-2018.pdf/>.
- Mascheroni, G., Murru, M.F., Aristodemou, E. & Laouris, Y. 2013. Parents: Mediation, self-regulation and co-regulation, 211-225. In: B. O'Neill, E. Staksrud & S. McLaughlin (eds.). *Towards a better internet for children? – Policy pillars, players and paradoxes*. Nordicom, Göteborg. Viewed on 25 November 2019, from https://www.nordicom.gu.se/sites/default/files/publikationer-hela-pdf/toward_a_better_internet.pdf/.
- Matyjas, B. 2008. Cyberculture: Dangers for childhood. *The New Educational Review*, 16(3):195-208.
- Middaugh, E., Clark, L.S. & Ballard, P.J. 2017. Digital media, participatory politics, and Positive Youth Development. *Pediatrics*, 140(2):127-131. DOI: <http://dx.doi.org/10.1542/peds.2016-1758Q>.
- Minić, S.G. & Spalević, Z. 2014. Abuse of computer networks in cyberspace: The role of the family in the modern information age. *Teme: Časopis za društvene nauke*, 38(1):417-431.
- Mishna, F., McLuckie, A. & Saini, M. 2009. Real-world dangers in an online reality: A qualitative study examining online relationships and cyber abuse. *Social Work Research*, 33(2):107-118.
- Newall, M. 2018. Cyberbullying: A global advisor survey, 1-12. Ipsos Public Affairs. Viewed on 5 February 2020, from https://www.ipsos.com/sites/default/files/ct/news/documents/2018-06/cyberbullying_june2018.pdf/.

REFERENCES

-
- OECD. 2016. *Trends shaping education* 2016. OECD Publishing, Paris. Viewed on 6 November 2019, from http://dx.doi.org/10.1787/trends_edu-2016-en.
- O'Neil, C. 2016. *Weapons of math destruction*. Crown, New York.
- O'Neill, B. 2013a. Who cares? Practical ethics and the problem of underage users on social networking sites. *Ethics and Information Technology*, 15: 253-262. DOI <http://doi.org/10.1007/s10676-013-9331-4>.
- O'Neill, B. 2013b. Internet hotlines: A reporting solution for Internet safety?, 39-56. In: B. O'Neill, E. Staksrud & S. McLaughlin (eds.). *Towards a better internet for children? – Policy pillars, players and paradoxes*. Nordicom, Göteborg. Viewed on 14 December 2019, from https://www.nordicom.gu.se/sites/default/files/publikationer-hela-pdf/toward_a_better_internet.pdf/.
- Paniagua, A. & Istance D. 2018. *Teachers as designers of learning environments: The importance of innovative pedagogies*. OECD Publishing, Paris. Viewed on 10 January 2020, from <http://dx.doi.org/10.1787/9789264085374-en>.
- Phyfer, J., Burton, P. & Leoschut, L. 2016. Global Kids Online South Africa: barriers, opportunities and risks. A glimpse into South African children's internet use and online activities. Technical Report. Centre for Justice and Crime Prevention, Cape Town. Viewed on 20 January 2020, from http://eprints.lse.ac.uk/71267/2/GKO_Country-Report_South-Africa_CJCP_upload.pdf/.
- Popovac, M. & Leoschut, L. 2012. Cyber bullying in South Africa: Impact and responses. *Centre for Justice and Crime Prevention Issue Paper*, 13:1-16.
- Regan, P.M. & Jesse, J. 2019. Ethical challenges of edtech, big data and personalized learning: twenty-first century student sorting and tracking. *Ethics and Information Technology*, 21(3):167-179.

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

- Republic of South Africa (RSA). 1996. *Films and Publications Act*, Act No. 65 of 1996. Viewed on 29 January 2020, from <http://pmg-assets.s3-website-eu-west-1.amazonaws.com/161115ACT.pdf/>.
- Republic of South Africa (RSA). 2005. *The Children's Act*, Act No. 38 of 2005. Viewed on 2 February 2020, from <https://www.justice.gov.za/legislation/acts/2005-038%20childrensact.pdf/>.
- Republic of South Africa (RSA). 2013. *Protection of Personal Information Act*, Act No. 4 of 2013. Viewed on 2 February 2020, from <https://www.gov.za/documents/protection-personal-information-act/>.
- Republic of South Africa (RSA). 2015. *Criminal Law (Sexual Offences and Related Matters) Amendment Act*, Act No. 5 of 2015. Viewed on 10 January 2020, from <https://www.justice.gov.za/legislation/acts/2015-005.pdf/>.
- Republic of South Africa (RSA). 2019a. *Films and Publications Amendment Act*, Act No. 11 of 2019. Viewed on 12 February 2020, from https://www.gov.za/sites/default/files/gcis_document/201910/42743gon1292.pdf/.
- Republic of South Africa (RSA). 2019b. *The Children's Amendment Bill*. Viewed on 3 January 2020, from https://www.gov.za/sites/default/files/gcis_document/201810/42005gon1185.pdf/.
- Rideout, V. 2015. *The common sense census: Media use by tweens and teens*. Common Sense Media, San Francisco. Viewed on 6 January 2020, from https://www.common sense media.org/sites/default/files/uploads/research/census_researchreport.pdf/.
- Rizza, C. & Pereira, A. 2013. *Social networks and cyber-bullying among teenagers*. European Union, Luxembourg. Viewed on 8 January 2020, from <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/social-networks-and-cyber-bullying-among-teenagers>.
- Ságvári, B. & Máder, M.P. 2013. Industry: Towards the socially responsible internet: Industry CSR practices across Europe, 93-109. In: B. O'Neill, E. Staksrud & S. McLaughlin (eds.). *Towards a better internet for children?*

REFERENCES

- *Policy pillars, players and paradoxes*. Nordicom, Göteborg. Viewed on 14 December 2019, from https://www.nordicom.gu.se/sites/default/files/publikationer-hela-pdf/toward_a_better_internet.pdf.
- Sando, S. 2003. Vulnerable bodies as ethical sensors. In: M. Thorseth (ed.), *Applied ethics in internet research*. Norwegian University of Science and Technology, Trondheim. Viewed on 18 December 2019, from https://www.academia.edu/2110306/Vulnerable_bodies_as_ethical_sensors.
- South African Law Reform Commission. 2015. Sexual offences: pornography and children. Issue Paper no. 30, Project 107, 5 August. Viewed on 12 February 2020, from https://www.justice.gov.za/salrc/ipapers/ip30_prj107_SexualOffences-PC-2015.pdf.
- Staksrud, E. & Kirksæther, J. 2013. Filtering & content classification, 23-37. In: B. O'Neill, E. Staksrud & S. McLaughlin (eds.). *Towards a better internet for children? – Policy pillars, players and paradoxes*. Nordicom, Göteborg. Viewed on 14 December 2019, from https://www.nordicom.gu.se/sites/default/files/publikationer-hela-pdf/toward_a_better_internet.pdf.
- Stückelberger, C. 2014. Globethics.net principles on ethics in the information society, 19-25. In: A.V. Preisig, H. Rösch & C. Stückelberger (eds.). *Ethical dilemmas in the information society: How codes of ethics help to find ethical solutions*. Globethics.net, Geneva. Viewed on 8 November 2019, from <https://www.ifla.org/files/assets/faife/publications/misc/ethical-dilemmas-in-the-information-society.pdf>.
- The Guardian, n.d. The Cambridge Analytica files. *The Guardian*. Viewed on 13 February 2020, from <https://www.theguardian.com/news/series/cambridge-analytica-files>.
- Third, A., Bellerose, D., De Oliveira, J.D., Lala, G. & Theakstone, G. 2017. Young and online: Children's perspectives on life in the digital age (The state of the world's children 2017 companion report). Western Sydney University, Sydney. Viewed 18 January 2020, from <http://doi.org/10.4225/35/5a1b885f6d4db>.

CHILDHOOD VULNERABILITIES IN SOUTH AFRICA: SOME ETHICAL PERSPECTIVES

- UNICEF Innocenti Research Centre. 2012. Child safety online: Global challenges and strategies. Technical Report. UNICEF, Florence. Viewed 7 January 2020, from https://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf.
- United Nations (UN). 1989. Convention on the Rights of the Child (Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with article 49). United Nations, New York. Viewed on 16 January 2020, from <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>.
- United States (US) Department of Justice. 2015. *18 USC Ch. 110: Sexual exploitation and other abuse of children (From Title 18 – crimes and criminal procedure: Part I – crimes)*. Viewed on 12 January 2020, from <https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter110&edition=prelim>.
- Valentine, G. & Holloway, S. 2001. On-line dangers?: Geographies of parents' fears for children's safety in cyberspace. *Professional Geographer*, 53(1): 71-83.
- Vesnaji, L. & Niveditha, D. 2012. Ethics in cyberspace – a philosophical approach. *International Journal of Advancements in Research & Technology*, 1(3):1-5.
- Whittlestone, J., Nyrop, R., Alexandrova, A., Dihal, K. & Cave, S. 2019. *Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research*. Nuffield Foundation, London.
- Wojniak, J. & Majorek, M. 2016. Children and ICT European initiatives and policies on protecting children online. *Universal Journal of Educational Research*, 4(1):131-136.
- Yang, Y. 2019. Nudge or puppet? Decision-making, ethics, and leadership in the information age. M.A. in Leadership Studies: Capstone Project Papers 55. University of San Diego, San Diego.