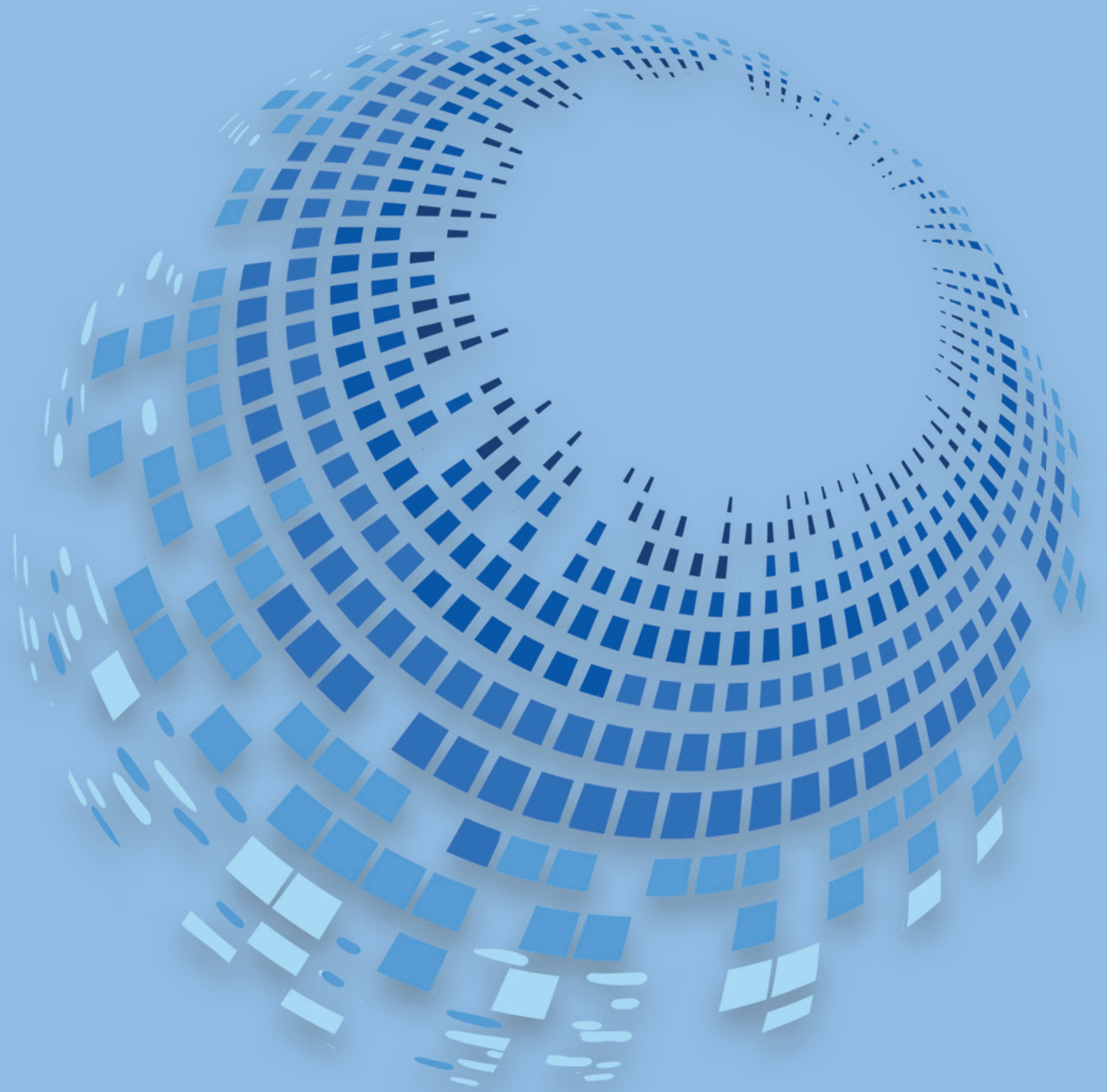
A STUDY ON CHILDREN'S RIGHT TO PRIVACY IN THE DIGITAL SPHERE IN THE AFRICAN REGION



Centre for Human Rights
UNIVERSITY OF PRETORIA

RAOUL WALLENBERG INSTITUTE
OF HUMAN RIGHTS AND HUMANITARIAN LAW

Sweden
Sverige

A study on children's right to privacy in the digital sphere in the African region

Pretoria University Law Press
PULP
2022

A study on children's right to privacy in the digital sphere in the African region

Published by:
Pretoria University Law Press (PULP)
The Pretoria University Law Press (PULP) is a publisher at the Faculty of Law, University of Pretoria, South Africa. PULP endeavours to publish and make available innovative, high-quality scholarly texts on law in Africa. PULP also publishes a series of collections of legal documents related to public law in Africa, as well as text books from African countries other than South Africa.

For more information on PULP, see www.pulp.up.ac.za

Printed and bound by:
Pinetown Printers, South Africa

To order, contact:
PULP
Faculty of Law
University of Pretoria
South Africa
0002
pulp@up.ac.za
www.pulp.up.ac.za

ISBN: 978-1-991213-15-0

Table of Contents

Acronyms

AAG	Advertising Association of Ghana
ACERWC	African Committee of Experts on the Rights and Welfare of the Child
ACRWC	African Charter on the Rights and Welfare of the Child
ANAIP	National Authority for Access to Public Information
ANRT	National Regulatory Agency Telecommunications
ANSI	National Computer Security Agency
ANSSI	National Agency for the Security of Information Systems
ANTIC	National Information and Communication Technology Agency
APCON	Advertising Practitioners Council of Nigeria
APDP	Personal Data Protection Authority
ARCEP	Autorité de régulation des communications éléctroniques
ARTP	Telecommunications and Post Regulatory Authority
ASAZIM	Advertising Standards Authority
ATI	Tunisian Internet Agency
ATIA	Access to Information Act
ATT	Technical Telecommunication Agency
AU	African Union
CAPMAS	Central Agency for Public Mobilisation and Statistics
CAR	Communications Authority of Kenya
CDP	Commission for the Protection of Personal Data
CDU	Child Development Unit
CERT	Computer Emergency Response Team
CERT.MU	Cybersecurity Emergency Response Team Mauritius
CERT.UG	Cybersecurity Emergency Response Team Uganda
CIL	Commission de l'Informatique et des Libertés
CNDP	Commission nationale de contrôle de la protection des données à caractère personnel
CNTE	National Centre for Technologies in Education
COP	Child Online Protection
CPA	Child Protection Act
CRC	Convention on the Rights of the Child
CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse Materials
DHA	Department of Home Affairs
DMS	Device Management System
DNA	Deoxyribonucleic Acid
DPA	Data Protection Act
DPC	Data Protection Commission
DPPA	Data Protection and Privacy Act
DRC	Democratic Republic of Congo
ECPAT	End Child Prostitution in Asian Tourism
ECtHR	European Court of Human Rights
ETCA	Electronic Transactions and Cybersecurity Act
EU	European Union
FCCPA	Federal Competition and Consumer Protection Act
FPB	Film and Publication Board
GDPR	General Data Protection Regulation
GPS	Global Positioning System

HAICA	Independent High Authority for Audiovisual Communication
ICA	Interception of Communications Act
ICCPR	International Covenant on Civil and Political Rights
ICTA	Information and Communication Technologies Authority
INCM	Communications Regulatory Authority
ISIS	Islamic State of Iraq and Syria
ISPs	Internet and Internet Service Providers
ITU	International Telecommunications Union
IWF	Internet Watch Foundation
KE-CIRT CC	National Kenya Computer Incident Response Team – Coordination Centre
LGBTQI	Lesbian, Gay, Bisexual, Transgender, Queer, & Intersex
MACRA	Malawi Communication Regulatory Authority
MAUCORS	Mauritian Cybercrime Online Reporting System
MCIT	Ministry of Communications and Information Technology
MISA	Media Institute of Southern Africa
MMA	Media Monitoring Africa
NCB	National Computer Board
NCC	Nigerian Communications Commission
NGO	Non-Governmental Organisation
NIIMS	National Integrated Identity Management Scheme
NITA	National Information Technology Agency
NITA-U	National Information Technology Authority Uganda
NITDA	National Information Technology Agency
NTRA	National Telecommunication Regulatory Authority
ODPC	Office of the Data Protection Commissioner
OTT	Over the Top Tax
POPIA	Protection of Personal Information Act
PORTRAZ	Postal and Telecommunications Act
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
PSE	Plan Sénégal Emergent
PVE	National Action Plan for Preventing Violent Extremism
R2K	Right2Know Campaign
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act
SADC	Southern African Development Community
SALRC	South African Law Reform Commission
SNC2022	National Cyber Security Strategy 2022
SONA	Standards Organisation of Nigeria Act 2015
TCRA	Tanzania Communications Regulatory Authority
UCC	Uganda Communications Commission
UCTT'	Control Unit of the Telecommunications Traffic
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNICEF	United Nations Children's Fund
UPR	Universal Peer Review
VPN	Virtual Private Network

Preface

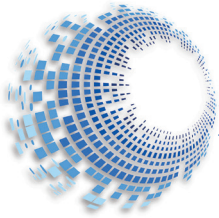
This study provides, broadly, an overview of the protection of children's right to privacy in Africa, with a specific focus in children's privacy rights during their interaction with technology in the digital era. The overarching goal of the study is to promote enhanced protection for children's right to privacy in the digital sphere in Africa. This goal is achieved through three main interventions: research for evidence and knowledge building on the standards and practice on children privacy online; evidence-based advocacy for children's privacy in the digital sphere, and capacity building to enhance the development and implementation of relevant protections to enhance online privacy for children. The first pillar of the project entails knowledge building on the regional and domestic standards governing children's privacy when navigating the internet. One of the main components of this aspect is a regional study which seeks to foster evidenced-based understanding of key issues relating to children's privacy online in the African context.

Succinctly, the study provides, in detail, the nature and scope of children's right to privacy in the digital sphere in Africa, an assessment of the effectiveness of legal frameworks for the protection of children's privacy in Africa, it identifies gaps in the protection and implementation of children's privacy online, it highlights good practices in Africa and beyond relating to the protection of children's rights in the digital sphere and makes practical recommendations to policymakers, technology companies and other key stakeholders on the measures to adopt to protect children's privacy during their interaction with technology and the internet in a manner that limits their exposure to harmful content or activity.

The method of the study is predominantly analytical and based on a human rights-based approach to children's privacy rights in a digital sphere in Africa. The study focuses on relevant national practice, regional and international child rights instruments, primary documents such as laws and policies, documents produced by treaty bodies, national legislation, and case law. It includes a systematic analysis of selected countries, from all sub-regions) in Africa to augment the findings, and to ensure a representative picture of the status of protection of children's privacy rights in the digital sphere. The study is a valuable contribution to studies on the protection of children's right to privacy in Africa. Its importance lies in its close assessment of national and regional instruments, interpretation and implementation of children's right to privacy.

A special thanks to previous and current staff of the Centre, in particular, the Manager of the Children's Rights Unit, Dr Elvis Fokala, who steered the project, Dr Nkatha Murungi who initiated the project, Ms Hlengiwe Dube for technical support, the lead consultant – Prof Julia Sloth-Nielsen, and researchers in the children's rights unit – Mai Aman, Nqobani Nyathi and Reece Gemma Pierce-Jones. The financial contribution of the Raoul Wallenberg Institute (Kenya office) is also acknowledged with thanks.

Frans Viljoen
Director, Centre for Human Rights
Faculty of Law, University of Pretoria



Executive summary

This report provides a summary of initiatives on the African continent to regulate the digital environment. It is centred on children's rights to privacy, and legal and regulatory measures that advance this human- rights goal. Based on individual country studies drawn from countries in all five regions of the continent, it profiles efforts (or lack of efforts) to adopt laws and a regulatory framework to engage in this sphere. The study concludes with recommendations and suggestions for enhanced attention to be paid to this emerging area of concern.

Introduction

Nowadays, every human right has a digital dimension which invites specific questions regarding the reconsideration of the Convention on the Rights of the Child (CRC) and African Children's Charter's articles relating to the digital environment due to children's 'digital rights'. Examples of these rights are the rights to be forgotten, to consent to terms and conditions, privacy policies of online services or apps, or to digital literacy. Whether the digital environment is seen as a potential threat to, or, enabler of children's rights, it can no longer be ignored as a factor in children's well-being and development.[1] It is necessary to read child privacy not only as a right, but also as a component of the best interests of the child. This is possible because the concept of 'the best interests of the child' was constructed to be dynamic.[2] Owing to a sharp increase in internet usage by most younger children together with the complexity of a technology-mediated environment, the right to privacy has come to the forefront of children's rights discourse. Privacy protection in such a complex environment has become a prerequisite for guaranteeing online child safety, and is a precursor for the exercise of fundamental civil and political rights such as freedom of expression and access to information. Thus, children's privacy protection has begun to constitute a separate, though interrelated, pillar within many online child safety initiatives.[3]

Methodology

The overall goal of the project is to promote enhanced protection for children's right to privacy in the digital sphere in Africa. This goal is intended to be achieved through three main interventions: research for evidence and knowledge building on the standards and practice on children's privacy online; evidence-based advocacy for children's privacy in the digital sphere; and capacity building to enhance the development and implementation of relevant protections to enhance online privacy for children. The first pillar of the project entails knowledge building on the regional and domestic standards governing children's privacy when navigating the internet. One of the main components of this aspect is a regional study which seeks to foster evidenced-based understanding of key issues relating to children's privacy online in the African context. This report is intended to fulfil that purpose.

Accordingly, the Centre for Human Rights at the University of Pretoria sought to institute a regional study to analyse the legal protection and practical enjoyment of children's right to privacy in the digital sphere in the African context. By utilising concrete examples and authoritative information from African countries, the study is expected to generate the empirical basis for the capacity building and advocacy elements of the project. The study explores the international and regional standards on children's privacy online, and identifies the standards and key issues in the protection of children's right to privacy in the digital sphere in Africa.

This report was compiled in the first instance from desktop literature, UN documents, and African Union materials. However, crucially, it was supplemented by country reviews that were produced on the basis of a questionnaire (Appendix 1). All in all, 19 country reviews were completed:

1 U Kilkelly & T Liefaard *International human rights of children* (2019) 489.

2 N Kravchuk 'Privacy as a new component of "the best interests of the child" in the new digital environment' (2021) 29 *The International Journal of Children's Rights* 99.

3 Kravchuk (n 2) 105.

Four for North Africa,[4] six for West Africa,[5] two for central Africa,[6] five for Eastern Africa[7] and four for Southern Africa.[8] The reports were compiled on the basis of a questionnaire to ensure a degree of uniformity; this questionnaire is attached as an Appendix. The country reports illuminate the extent of legal privacy protection for children in their respective jurisdictions. They are extensively used in part 3 of this report onwards.

Part 1: The concept of privacy – A complex concept

Privacy is not a simple idea nor is it easily embodied in a clear, agreed-upon set of guidelines. It is a concept that has evolved over time. Originally focussed on protection of correspondence and communications from interception it now has a much wider remit. Even experts on the subject debate what privacy is, but most agree that it is very context specific.[9] What information is safe or appropriate to share with a friend is very different from what someone would share with a teacher or an internet service. Livingstone et al divide privacy contexts into three categories: interpersonal, institutional and commercial.[10] But even within these categories, privacy is still very specific to many individual contexts. What someone should or should not want to share with parents is different from what one might want to share with peers, two different interpersonal contexts. The same goes for doctors versus teachers, two institutional contexts. Privacy needs also vary considerably from person to person according to their personality or experience. Privacy norms are in flux and are being innovated especially in the digital realm. They may vary considerably across cultures.[11]

What is often linked to privacy is the concept of harm. These are the major harm contexts that lie behind most privacy discussions: 1) Strangers trying to sexually solicit or groom youth for sexual activity. 2) Receiving inappropriate sexual images. 3) Being bullied, threatened or harassed. 4) Having one's computer hacked, valuable software or money stolen. 5) Being manipulated by technology companies or commercial enterprises. 6) Being spied upon by law enforcement, school authorities or government agencies and thus made vulnerable to sanctions or discrimination.[12] 7) Having one's reputation damaged in the eyes of family and friends. The privacy implications are also very dependent on the dynamics of the harm – from cookies, or image capture, or someone obtaining your password. This makes it very difficult to generalise about appropriate privacy. Privacy concerns may also depend on the source of the threat – friends, strangers, business operators and so forth.

> The key privacy challenge (and paradox) currently posed by the internet is the simultaneous interconnectedness of voluntary sharing of personal information online, important for children's agency,

4 Egypt, Morocco, Algeria and Tunisia.
5 Benin, Cote D'Ivoire, Senegal, Nigeria, Ghana and Burkina Faso.
6 Democratic Republic of Congo and Cameroon.
7 Tanzania, Kenya, Uganda, Mauritius, and Ethiopia.
8 Mozambique, South Africa, Malawi and Zimbabwe.
9 C Raab & B Goold 'Protecting information privacy' (2011) https://www.equalityhumanrights.com/sites/default/files/research-report-69-protecting-information-privacy.pdf (accessed 10 February 2022).
10 S Livingstone, M Stoilova & R Nandagiri 'Children's data and privacy online: Growing up in a digital age. An evidence review' (2019) *London: London School of Economics and Political Science* 3.
11 Livingstone, Stoilova & Nandagiri (n 2) 10.
12 LR Shade & R Singh "Honestly, we're not spying on kids": School surveillance of young people's social media' (October 2016) *Social Media + Society.*

> and the attendant threats to their privacy, also important for their safety. While children value their privacy and engage in protective strategies, they also greatly appreciate the ability to engage online.[13]

A recent United Nations Children's Fund (UNICEF) report on children's privacy online and freedom of expression distinguishes several dimensions of privacy affected by digital technologies – physical, communication, informational and decisional privacy.[14] Physical privacy is violated in situations where the use of tracking, monitoring or live broadcasting technologies can reveal a child's image, activities or location. Threats to communication privacy relate to access to posts, chats and messages by unintended recipients. Violation of information privacy can occur with the collection, storage and processing of children's personal data, especially if this occurs without their understanding or consent. Finally, disruptions of decisional privacy are associated with the restriction of access to useful information which can limit children's independent decision-making or development capacities.

Digital practices, such as automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance are becoming routine. Such practices may lead to arbitrary or unlawful interference with children's right to privacy; they may have adverse consequences on children, which can continue to affect them at later stages of their lives.[15]

While the commercial use of children's data is at the forefront of current privacy debates, the empirical evidence related to children's experiences, awareness and competence regarding privacy online lags behind. The available evidence suggests that commercial privacy is the area where children are least able to comprehend and manage on their own.

Privacy is vital for child development – key privacy-related media literacy skills are closely associated with a range of child developmental areas – autonomy, identity, intimacy, responsibility, trust, pro-social behaviour, resilience, critical thinking and sexual exploration. Interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful.[16] Any such interference should therefore be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimisation, be proportionate and designed to observe the best interests of the child and must not conflict with the provisions, aims or objectives of the CRC.[17] These principles apply equally in the context of the African Charter on the Rights and Welfare of the Child.

A major gap in children's understanding of privacy is that they associate it mainly with interpersonal sharing of data and rarely consider the commercial or institutional use of their data.[18] Hence, their privacy strategies are mainly limited to management of their online identity – for example, withholding or providing fake information, or creating multiple identities, removing content, tags or withdrawing from the internet, managing privacy settings or friendship circles.[19]

Many children use online avatars or pseudonyms that protect their identity, and such practices can be important in protecting children's privacy. State parties should require an approach integrating safety-by-design and privacy-by-design to anonymity, while ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, such as cyber aggression, hate speech or sexual exploitation and abuse. Protecting a child's privacy in the digital environment may be vital in circumstances where parents or caregivers themselves pose a threat to the child's safety or where they are in conflict over the child's care.[20]

Juxtaposed against the well-known threat of harm in the online environment, as articulated above, are also children's agency and autonomy. This brings

13 Livingstone, Stoilova & Nandagiri (n 2) 3.
14 C Nyst, A Gorostiaga & P Geary 'Children's online privacy and freedom of expression' (2018) 8.
15 UN Committee on the Rights of the Child, General Comment 25 on children's rights in relation to the digital environment (2021) UN Doc CRC/C/CG/25 dated 2 March 2021, 11 para 68.
16 Livingstone, Stoilova & Nandagiri (n 2) 17.
17 Committee on the Rights of the Child (n 6) 12 para 69.
18 S Livingstone, M Stoilova & R Nandagiri 'Children's data and privacy online: Reviewing the existing evidence' (2018).
19 Livingstone, Stoilova & Nandagiri (n 10) 20.
20 Committee on the Rights of the Child (n 7) 13 para 77.

into question the issue of consent, and specifically the question as to what children can consent to and when, consistent with their evolving autonomy. And, while the dynamics of the online context can threaten and potentially violate privacy, children also experience that it gives them a sense of their identity, promotes their need for self-expression and can be a tool for peer to peer development. It can enhance their choice and control over personal information and thus, their privacy online. At the same time, for the African context, questions arise about online content that promotes radicalisation of children, as well as about the promotion of discrimination and hate speech, including ethnic and racial discrimination, as well as Lesbian, Gay, Bisexual, Transgender, Queer, & Intersex (LGBTQI) discrimination.

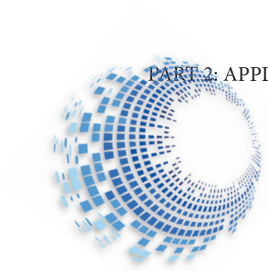
In Europe, 2018 saw the implementation of wide-ranging new legislation in the form of the General Data Protection Regulation (GDPR).[21] The GDPR builds on a series of assumptions regarding the maturity of children (to give their consent) and the role of parents (in requiring their consent for the use of data from under-age children), most notably in relation to article 8.5 of the GDPR. The overall tone for the treatment of a child's personal data in the GDPR, is children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, safeguards and their rights in relation to the processing of personal data. It also presumes knowledge of how children can understand the Terms and Conditions of the services they use (in requiring that these be comprehensible to services users), and the risks that face children (in the requirement for risk impact assessments).[22] It is applicable on the African continent to the extent that any organisation on the continent processes the data of European Union Citizens. It also provides a useful benchmark for African states in their own legal development and has in fact already served as the basis for such legislation. In fact, some countries have based their legislation on this, such as Nigeria. The Nigerian Data Protection Regulation of 2019, based on the European GDPR, has been enforced quite vigorously. An example of this is that in the case of non-compliance, the GDPR provides for possible monetary or administrative penalties that will be issued by supervisory authorities.[23] The GDPR is clearly influencing other recent law reform initiatives, such as in Kenya, as detailed elsewhere in this report. The ECtHR has thus far not considered any data-processing cases where violations of a child's privacy is at issue.[24]

21 Intersoft Consulting 'GDPR' 25 May 2018 General Data Protection Regulation (GDPR) – Official Legal Text gdpr-info.eu (accessed 10 June 2021).

22 J Aldgate & W Rose 'Assessing and managing risk in *getting it right for every child*' https://lx.iriss.org.uk/sites/default/files/resources/0069411.pdf (accessed 10 February 2022).

23 One Trust Data Guidance™ 'GDPR v Nigeria Data Protection Regulation' (2019) *Comparing Privacy Laws* 5.

24 N Kravchuk 'Privacy as a new component of "the best interests of the child" in the new digital environment' (2021) 29 *The International Journal of Children's Rights* 99, at 106. She does refer though to *Avilkina and others v Russia*, where confidential medical information about the applicants, including a minor, was disclosed by a medical facility following a request by the prosecutor's office, and where the Court reiterated that the protection of personal data, including medical information, is of fundamental importance to a person's enjoyment of their right to respect for his/her private and family life, guaranteed by article 8 of the ECHR. There have also been cases confirming the child's right to freedom from unlawful attacks on his or her reputation, a dimension of privacy.



Part 2: Applicable international law, regional law, and General Comments

Article 16 of the CRC protects the child against 'arbitrary or unlawful interference with his or her privacy, family, home or correspondence [and] to unlawful attacks on his or her honour and reputation'. Thus, as Tobin points out, in part, the formulation of article 16 is essentially a restatement of the article 17 of the International Covenant on Civil and Political Rights (ICCPR), which itself is based on article 12 of the Universal Declaration of Human Rights (UDHR).[25] It has been noted that

> privacy related rights have extended beyond their original concern - threats to private space particularly the home- to encompass personal security, self-fulfilment, and identity, including the organisation of family life and relationships, sexual mores and some business activities. Such is the flexibility of the right to privacy that is it often referred to as the 'filler' right for its capacity to be invoked when no other right appears relevant or appropriate.[26]

An unreasonable or unlawful interference with any component of a person's privacy amounts to a violation of said privacy. The right to privacy derives from the UDHR and article 17 of the ICCPR. Privacy refers to freedom from 'unwanted or undue intrusion or disturbance in one's private life or affairs; freedom to be let alone'. This includes freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorised disclosure of one's personal data or information, whether by a government, corporation, or individual. Privacy also prohibits the revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, and the disclosure of information confidentially given or received by the individual.[27] Additionally, the right to privacy protects against seizure of private possessions or the violation of private communications. The right to privacy is closely related to and entails a person's identity and personal autonomy, founded on the value of dignity.[28]

Kilkelly and Liefaard note that

> the right to privacy is also an important participatory right, particularly in the case of older children, insofar as it is part and parcel of individual autonomy, a necessary precondition of participation. The participatory function of the right to privacy is not something that is often alluded to in legal and policy documents. In the digital environment, especially, privacy is often reduced to data protection. But while data protection is certainly closely related to one's privacy, privacy itself is a much broader and more complex concept.[29]

According to Assim, on the face of it, article 16 of the CRC appears to focus mainly on the child's privacy as an individual and within the context of the family, home, or family environment as the 'natural environment for the growth and well-being of' children (CRC Preamble, para 5). However, she concedes that the right applies in a variety of settings other than the home.[30]

The African Charter on the Rights and Welfare of the Child (ACRWC) introduces an additional feature to children's right to privacy, which is not present in the CRC provision on privacy.[31] It

25 J Tobin & SM Field 'Article 16: The right to protection of privacy, home, family, correspondence, honour and reputation' in J Tobin & P Alston (2019*) A Commentary on the Convention on the Rights of the Child* (2019) 551.

26 Tobin and Field (n 1) 552.

27 Dictionary.com https://www.dictionary.com/browse/privacy#:~:text=the%20state%20of%20being%20free,See%20also%20invasion%20of%20privacy (accessed 10 February 2022).

28 UM Assim 'Civil rights and freedoms of the child' in T Liefaard & U Kilkelly *The international human rights of children* (2018) 389-417.

29 U Kilkelly & T Liefaard *The international human rights of children* (2018) 94-96.

30 For example, including the prohibition of advertising for fostering or adoption and the maintenance of privacy during court proceedings whether as victims, witnesses, and children accused of crimes.

31 Tobin & Field (n 1) 554. Though Tobin & Field suggest that article 5 of the CRC, on parents providing guidance

guarantees children the right to privacy 'provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of the children' (article 10). It has been argued that subjecting the child's privacy right to parental supervision negates or limits the exercise of the right for children, as it would be difficult to establish the reasonableness or otherwise of such supervision.[32] However, it is equally arguable that this 'limitation' does not deprive the right of all meaning given that the extent of parental supervision would ultimately decrease along with the child's evolving capacities (article 5 of the CRC).[33] However, the African Committee of Experts on the Rights and Welfare of the Child is clear about the fact that violations of the rights of the child, including privacy, cannot be justified by 'supervision over the conduct of the child'. The closest equivalent to article 5 of the CRC in the African Children's Charter is article 20:

> Parents or other persons responsible for the child shall have the primary responsibility of the upbringing and development of the child and shall have the duty:
> (a) to ensure that the best interests of the child are their basic concern at all times;
> (b) to secure within their financial abilities, conditions of living necessary to the child's development; and
> (c) to ensure that domestic discipline is administered with humanity and in a manner consistent with the inherent dignity of the child.

Article 20 thus reinforces the provision of article 10 which provides for the parents right (and obligation) to exercise reasonable supervision over their children's conduct.

Assim argues that in the context of access to information, and the use of social media in an age of increasing digital media and technological advancements, parents play a role in monitoring their children to ensure their safety and protection.[34] This role falls within the confines of parental rights and responsibilities to fulfil the child's best interests, which seems to justify the parental supervision qualification. Kilkelly and Liefaard argue that

> in certain circumstances, it may conceptually be difficult to reconcile the child's right to privacy with the legitimate parental, societal, and governmental interest in protecting children from harm, particularly when it comes to children's participation in the digital environment.[35] The legitimate objective of shielding children from the potential risks associated with certain online activities must be balanced against ensuring that the child's right to privacy as well as other rights such as the rights to freedom of expression and association are not disregarded.[36]

They also allude to the fact that the feasibility of privacy protections based on parental or even child consent is looking increasingly doubtful as data collection and analysis become increasingly automated and reliant on algorithmic calculations with unknown biases and largely unaccountable processes.[37]

A discussion of the scope and ambit of the child's right to privacy in the digital environment would not be complete without referring to the fact that many parents intrude on their children's rights to privacy, for instance, by sharing pictures or clips of them, from ultrasound pictures and birth announcements to photographs of day-to-day events in parents' and children's lives. This practice, also referred to as 'sharenting', has been argued to be a practice of self-representation by and of parents and their parenting. However, they are making aspects of their children's lives public, (most) often without the consent of the child, while according to article 16 of the CRC, they should not 'arbitrarily' or 'unlawfully' interfere with their child's (right to) privacy. While many parents are aware of the safety-related risks caused by 'sharenting' and try to mitigate them, threats to a child's reputation are mostly ignored. It leads to a conflict of rights, namely, the child's privacy versus the parent's right to freedom of expression. Kravchuk describes this issue as follows: 'Of all contemporary threats to the privacy of the

to children in the exercise of their rights, does accommodate this.

32 T Boezaart *Introduction to child law* (2009); M Gose *The African Charter on the Rights and Welfare of the Child* (2002).

33 Assim (n 4) 410. This was also established in *MEC for Education, KwaZulu Natal v Pillay* 2008 (1) SA 474 (CC) para 56.

34 Assim (n 4) 411-417.

35 Kilkelly & Liefaard (n 5) 487-513.

36 Kilkelly & Liefaard (n 5) 497.

37 As above.

child, the one created by parents' activities online seems to be the most difficult to address'.[38]

1 CRC General Comment 25[39]

The CRC Committee issued its most recent General Comment on Children's Rights in the Digital Environment in April 2021. It follows a Day of General Discussion held on this theme in 2014, and an extensive discussion process, with many submissions received after both the concept note and the first draft of the General Comment were published and calls for comment were invited. Children were also consulted. The General Comment contains copious references to children's rights to privacy, and offers guidance to states parties in this regard.

The General Comment situates the discussion in the context of the four general principles of the UN Convention on the Rights of the Child: non-discrimination (paragraphs 9-11); best interests of the child (paragraphs 12-13); right to life, survival and development (paragraphs 14-15); and respect for the views of the child (paragraphs 16-18). A further section is devoted to children's evolving capacities (paragraphs 19-21). Access to justice, remedies and reparations are covered in paragraphs 43 to 49. According to paragraph 46, appropriate reparation includes restitution, compensation and satisfaction and may require apology, correction, removal of unlawful content, access to psychological recovery services or other measures.

Turning to the intersection with the right to freedom of expression, the General Comment advises that any restrictions on children's right to freedom of expression in the digital environment, such as filters, including safety measures, should be lawful, necessary and proportionate. The rationale for such restrictions should be transparent and communicated to children in age-appropriate language.[40]

Apart from legislative review, the General Comment mandates that children's online protection should be integrated within national child protection policies. States parties should implement measures that protect children from risks, including cyber aggression and digital technology-facilitated and online child sexual exploitation and abuse.[41] As regards awareness raising, states parties are exhorted to facilitate educational programmes for children, parents and caregivers, the general public and policymakers to enhance their knowledge of children's rights in relation to the opportunities and risks associated with digital products and services. Such programmes should include information on how children can benefit from digital products and services and develop their digital literacy and skills, and how to protect children's privacy and prevent victimisation.[42]

States parties should take measures, including through the development, monitoring, implementation and evaluation of legislation, regulations and policies, to ensure compliance by businesses with their obligations to prevent their networks or online services from being used in ways that cause or contribute to violations or abuses of children's rights, including their rights to privacy and protection, and to provide children, parents and caregivers with prompt and effective remedies.[43] The General Comment advises that in addition to developing legislation and policies, state parties should require all frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. That includes businesses that target children, have children as end users or otherwise affect children.[44]

As regards coordination, to encompass the cross-cutting consequences of the digital environment for children's rights, states parties should identify a government body that is mandated to coordinate

38 N Kravchuk 'Privacy as a new component of "the best interests of the child" in the new digital environment' (2021) 29 The International Journal of Children's Rights 99, at 110.

39 UN Committee on the Rights of the Child, General Comment 25 on children's rights in relation to the digital environment' (2021) UN Doc CRC/C/CG/25 dated 2 March 2021.

40 Committee on the Rights of the Child (n 15) 10 para 59.

41 Committee on the Rights of the Child (n 15) 5 para 25.

42 Committee on the Rights of the Child (n 15) 6 para 32.

43 Committee on the Rights of the Child (n 15) 7 para 36.

44 Committee on the Rights of the Child (n 15) 7 para 39.

policies, guidelines and programmes relating to children's rights among central government departments and the various levels of government to realise children's rights in relation to the digital environment at the cross-sectoral, national, regional and local levels.[45]

States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuro marketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children.[46]

The General Comment advises that states parties should take legislative, administrative and other measures to ensure that children's privacy is respected and protected by all organisations and in all environments that process their data. Legislation should include strong safeguards, transparency, independent oversight and access to remedy. States parties should require the integration of privacy-by-design into digital products and services that affect children. They should regularly review privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy. Where encryption is considered an appropriate means, states parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material. Such measures must be strictly limited according to the principles of legality, necessity and proportionality.[47]

Specifically, in regard to privacy, the Committee notes that certain combinations of personal data, including biometric data, can uniquely identify a child. Digital practices, such as automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance are becoming routine. They are of the view that such practices may lead to arbitrary or unlawful interference with children's right to privacy.[48]

According to the General Comment, interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful. Any such interference should therefore be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimisation, be proportionate and designed to observe the best interests of the child and must not conflict with the provisions, aims or objectives of the Convention.[49]

2 Further relevant excerpts from the General Comment

71. Where consent is sought to process a child's data, States parties should ensure that consent is informed and freely given by the child or, depending on the child's age and evolving capacity, by the parent or caregiver, and obtained prior to processing those data. Where a child's own consent is considered insufficient and parental consent is required to process a child's personal data, States parties should require that organizations processing such data verify that consent is informed, meaningful and given by the child's parent or caregiver.

72.States parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations. They should further ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing. They should also provide information to children, parents and caregivers on such matters, in child-friendly language and accessible formats.

73.Children's personal data should be accessible only to the authorities, organizations and individuals designated under the law to process them in compliance with such due process guarantees

45 Committee on the Rights of the Child (n 15) 5 para 27.
46 Committee on the Rights of the Child (n 15) 7 para 42.
47 Committee on the Rights of the Child (n 15) 11 para 70.
48 Committee on the Rights of the Child (n 15) 11 para 68.
49 Committee on the Rights of the Child (n 15) 12 para 69.

as regular audits and accountability measures. Children's data gathered for defined purposes, in any setting, including digitized criminal records, should be protected and exclusive to those purposes and should not be retained unlawfully or unnecessarily or used for other purposes. Where information is provided in one setting and could legitimately benefit the child through its use in another setting, for example, in the context of schooling and tertiary education, the use of such data should be transparent, accountable and subject to the consent of the child, parent or caregiver, as appropriate.

74.Privacy and data protection legislation and measures should not arbitrarily limit children's other rights, such as their right to freedom of expression or protection. States parties should ensure that data protection legislation respects children's privacy and personal data in relation to the digital environment. Through continual technological innovation, the scope of the digital environment is expanding to include ever more services and products, such as clothes and toys. As settings where children spend time become 'connected', through the use of embedded sensors connected to automated systems, States parties should ensure that the products and services that contribute to such environments are subject to robust data protection and other privacy regulations and standards. That includes public settings, such as streets, schools, libraries, sports and entertainment venues and business premises, including shops and cinemas, and the home.

75.Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver; nor should it take place without the right to object to such surveillance, in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose.[50]

3 African Committee of Experts on the Rights and Welfare of the Child (ACERWC) General Comment 7 (article 27 of the Charter)[51]

This recently adopted General Comment deals with the elaboration of the nature of the state obligation to implement the right to protection against all forms of sexual exploitation. Only those sections relevant to the digital era are discussed here, since the General Comment deals extensively with off line sexual exploitation of children too.

With regard to the general principle of participation,[52] it is stated that

> a child acting in the online environment is not different from a child offline, and her/his right to access certain online services without parental consent may well be allowed before the child turns 18; and that even though all young persons under the age of 18 years are entitled to special protection, this must necessarily be balanced against the child's right to information, and his or her right to participation when engaging with the digital world, also in the context of evolving capacity of the child.

At section 5, the General Comment observes that

> there can be a tension between the exercise of parental responsibility and the duty to guide children in their behaviour, and children's right to freedom of expression and to privacy, as well as their evolving capacity and need to engage increasingly with the adult world as they near the end of childhood. Managing these tensions requires sensitive approaches. Parents should be equipped to educate and advise their children about online safety, rather than blocking children from entering the online space altogether, as increasingly the online and offline domains are intertwined and not easily separated. Nevertheless, States parties must play a supportive role to enable parent to fulfil their obligations, including with educational programmes and easy to use guides for parents.

50 Committee on the Rights of the Child (n 15) 12-13.

51 African Committee of Experts on the Rights and Welfare of the Child, General Comment 7 on article 27 of the ACRWC: Sexual exploitation (July 2021).

52 African Committee of Experts on the Rights and Welfare of the Child (n 27) sec 4.6.

The General Comment has a substantial section on 'grooming' including online grooming, and notes that victims can also be lured between online and offline environments. The Committee also advises states parties to ensure that the relevant provisions of their criminal or penal codes cover all forms of child sexual abuse material, whether offline or online.[53] State parties are requested to ensure that the producing, distributing, disseminating, importing, exporting, offering, selling or possessing, for the purposes of sexual exploitation of child sexual abuse materials, as well as ensuring that save for clearly defined professional purposes, mere possession is also made a criminal offence. Even where child sexual abuse materials are not 'possessed' – such as where they are live streamed or viewed on a webcam show in real time – a criminal sanction should be provided for.[54]

A substantial section deals with extraterritoriality and international legal mutual assistance.[55] States parties are urged to adopt legislative measures that should in addition to criminal liability, establish precise conditions and rules for extradition, extra territorial jurisdiction, mutual legal assistance, and the seizure and confiscation of goods. States parties should, according to the General Comment, establish by law the responsibility of the Information and Communication Technologies (ICT) companies to block, remove and report child sexual abuse material hosted on their servers, if needs be, in collaboration with website owners, and of financial institutions to block and refuse financial transactions intended to pay for any such offences. State parties are also requested to provide fast and effective procedures for blocking and removing harmful material involving children, in order to prevent such material from continuing to be accessed and shared. Such procedures should be established in collaboration with law enforcement and reporting hotlines, as well as the private sector, in particular internet service providers and social networks.[56]

4 The AU Convention on Cyber Security and Personal Data Protection

This Convention, adopted in 2014, is premised on the understanding that the protection of personal data and private life constitute a major challenge to the information society, and that such protection requires that a balance be struck between the use of computer technologies and the protection of citizens in their daily or professional life, while guaranteeing the free flow of information.[57] According to the Preamble, a goal of the Convention is to ensure harmonised legislation amongst member states in the area of cybersecurity to establish in each state party a mechanism capable of combatting violations of privacy that may be generated by personal data collection, processing, transmission, storage and use. Another goal identified is the need to establish broad guidelines for the repression of cybercrimes in member states. The Convention also defines the framework for the adaptation of standard proceedings concerning information and telecommunication technologies and spells out the conditions for instituting proceedings specific to cybercrime. The Convention contains an up to date definition of child pornography (amongst others). States are required to criminalise various offences related to child pornography as specified in article 29(3)(a)-(d). Children are otherwise not mentioned in the Convention.

According to article 9, the Convention applies to any automated or non-automated processing of data contained in or meant to be part of a file (with certain clearly defined exceptions), any processing of data undertaken in the territory of the state party, and any processing of data relating to public security, defence, research, criminal prosecution or state security.

53 African Committee of Experts on the Rights and Welfare of the Child (n 27) sec 6.3.1.
54 As above.
55 African Committee of Experts on the Rights and Welfare of the Child (n 27) sec 6.3.6.
56 African Committee of Experts on the Rights and Welfare of the Child (n 27) sec 8.2.
57 African Union Convention 'African Union Convention on Cyber Security and Personal Data Protection' (2014) 1.

Amongst other measures, such as the requirement that national protection authorities be appointed, and the duties they should be imbued with, each state part is required to adopt such legislative and/or regulatory measures as it deems necessary to confer specific responsibility on institutions, either newly established or existing, as well as on designated officials of said institutions, with a view to conferring on them statutory authority and legal capacity to act in all aspects of cyber security application, including but not limited to response to cyber security incidents, and coordination and cooperation in the field of restorative justice, forensic investigations, prosecutions and so forth.[58] States are required to criminalise those acts listed in article 29.

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), has not been ratified by many African states, including Kenya, Malawi, Tanzania, Uganda, Nigeria, Ethiopia, Democratic Republic of Congo, Cameroon, Egypt and Zimbabwe.

Ghana has signed the Malabo Convention and ratified it into national law.[59] Algeria, Mauritius, Mozambique, Senegal and Benin too have ratified this Treaty. Tunisia signed it on 23 April 2019. The parliament still needs to ratify the Convention.

5 UN Special Rapporteur on the Right to Privacy[60]

This Special Rapporteur was appointed in 2015, and is mandated to promote and protect the right to privacy by:

- reviewing government policies and laws on the interception of digital communications and collection of personal data;
- identifying actions that intrude on privacy without compelling justification;
- assisting governments in developing best practices to bring global surveillance under the rule of law;
- articulating private sector responsibilities to respect human rights; and
- helping ensure national procedures and laws are consistent with international human rights obligations.

The Special Rapporteur for privacy is increasingly interested in privacy implications in the following areas: mass surveillance; using and retaining personal data; forensic DNA databases; open data and big data. A call for submission for a report on children rights and privacy closed in September 2020. The report was presented to the Human Rights Council in March 2021. The report deals with artificial intelligence and children's rights.[61]

58 African Union Convention (n 33) art 25.

59 Y Turianskyi 'Africa and Europe: Cyber governance lessons' (2020) 77 *Policy Insights* 10.

60 United Nations Human Rights Special Procedures 'Special Rapporteur on the right to privacy' (2021) https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx#:~:text=Current%20mandate%20holder&text=Joseph%20Cannataci%20of%20Malta%20as,on%20the%20right%20to%20privacy (accessed 2021).

61 Human Rights Council 'Relationship between the realisation of the right to work and the enjoyment of all human rights by persons with disabilities' Report of the United Nations High Commissioner for Human Rights, UN Doc A/HRC/46/47 (21 January 2021) 4.

Part 3: National initiatives in Africa to protect children's right to privacy in the digital sphere drawn from the country studies

1 Constitutional protection

Constitutional protection of the right of everyone to have his or right to privacy protected is a feature of several constitutions, such as those of Nigeria, Malawi, Tanzania, Ethiopia,[62] Kenya, Ghana, Mauritius,[63] Benin, Burkina Faso, Cameroon, Egypt, Mozambique, Morocco, Algeria, South Africa, Zimbabwe and Tunisia. Interestingly, the Mozambican Constitution provides that 'all persons shall be entitled to have access to collected data that relates to them and to have such data rectified', hence introducing at constitutional level the need for personal data protection.[64]

Article 31 of the Congolese Constitution says that:

> All persons have the right to respect for their private life, for the confidentiality of their correspondence, telecommunications and any other form of communication. This right may only be interfered with in the cases provided for by the law.

This protection is explicitly extended to children by article 30 of the 2009 Law on Child Protection, with the proviso that it is 'without prejudice to the rights and responsibilities of his parents or other persons exercising parental authority'.[65]

2 Internet access

Although not at the level of developed countries, almost all country rapporteurs provided evidence of growing internet accessibility in their respective jurisdictions, and the intention to scale up digital access. Malawi, for example, despite being one of the poorest countries in the world, had its newly inaugurated President (Lazarus Chakwera) announce in his inaugural speech that he aims to ensure that at least 80 per cent of Malawians have access to internet services by 2025. In order to facilitate this, he proposed to reform the Malawi Communication Regulatory Authority (MACRA) into a people-centred and professional regulator.[66] This is despite the fact that Malawi has high prices for data, poor network quality, and weak competition has stymied access and connectivity. Mozambique's ICT landscape has seen limited development, with children's online rights receiving marginal attention. Due to the widespread poverty and high cost of access, most internet users access them through public and community access points.[67] Additionally, poor infrastructure is compounded by limited access to electricity there.

62 The Criminal Code in terms of arts 604 to 606 criminalises the violation of privacy safeguards guaranteed under the Constitution. Pursuant to art 606 of the Criminal Code, violation of the privacy of correspondence or consignments including intrusion of one's letter, telegram, telecom, and other electronic correspondence, among others, is punishable, with up to six months of imprisonment or a fine: Criminal Code of the Federal Democratic Republic of Ethiopia 414 of 2004.

63 Although children's rights are not expressly provided for in this Constitution.

64 Constitution of the Republic of Mozambique, art 71(4).

65 The Constitution of the Democratic Republic of the Congo, 2005, art 31.

66 President Chakwera 'State of the Nation' 4 September 2020 https://www.malawi.gov.mw/index.php/proud/news-and-media/speeches (accessed 9 February 2022).

67 A Gillwald, O Mothobi & B Rademan 'The state of ICT in Mozambique' *Research ICT Africa* (January 2019) https://researchictafrica.net/wp/wp-content/uploads/2019/07/2019_After-Access_The-state-of-ICT-in-Mozambique.pdf (accessed 2 February 2022).

Kenya is emerging as ICT leader in the region, being ranked as the second-best sub-Saharan African country in the 2020 Inclusive Internet Index. In recent years, the county has made strides in strengthening its access and connectivity landscape, with over 61 million active mobile subscriptions, 44 million internet subscriptions, and an internet access rate of 87 per cent.[68] Restrictions around online speech, concerns around data protection legislation, and state surveillance of internet activities pose challenges to the advancement of digital rights in Kenya.[69]

Nigeria too has relatively higher internet access than most places in the region, at 73 per cent access. Sixty-four point eight (64.8) per cent of the population are connected to the internet in Morocco. The disparity between urban and rural connectivity persists. Over 92 per cent of Morocco's population utilise mobile phones, 86 per cent of whom use their smartphones to access the internet. The number of internet users in Algeria increased by 2.4 million between 2019 and 2020. Access to internet in Algeria stood at 52 per cent in January 2020.[70] In Tunisia, according to the International Telecommunications Union, internet access stood at 64 per cent at the end of 2018, up from 50 per cent at the end of 2016. Only 36.7 per cent of Tunisians have internet access at home, but 97.7 per cent have cell phone access.[71] Ghana reported internet access is at 46.5 per cent, and Burkina Faso at 21.4 per cent. Adults and children face barriers to internet access, with limited connectivity and high prices. Girls and women face slightly greater barriers because of harmful gender norms and lack of socio-economic standing, amongst others. Children usually access the internet through mobile phones and only 15 per cent of households own a computer.[72] Côte d'Ivoire has witnessed substantial developments in the ICT sector between 2000 and 2020, with the rise of internet users from 40 000 to 12 253 653, a growth of 30,534 per cent for a current access of 45.3 per cent.[73] In Egypt, the percentage of individuals using the internet stood at 57.3 per cent in December 2020.[74] The Central Agency for Public Mobilisation and Statistics (CAPMAS) states that 46.9 per cent of children aged between four-17 use mobile phones, while the percentage is 80.6 per cent for those aged 15-17 years.[75] Although affordable, it is reported that internet connections continue to suffer from poor quality and low speeds there.

Algeria has 26.35 million internet users as at 31 January 2021. The number of internet users in Algeria increased by 2.4 million between 2019 and 2020. Internet access in Algeria stood at 52 per cent in January 2020.

In Mauritius, over 64 per cent of the country has access to the internet, and there are sustained efforts to advance digital literacy and to pave the way for an information-based society.[76] Senegal reports current access of 56.7 per cent and that along with the growing access of information and communication technologies boosted by the 'Plan Sénégal Emergent

68 Communications Authority of Kenya 'Second Quarter Sector Statistics Report for the Financial Year 2020/2021' (December 2020) at 7 and 17 https://ca.go.ke/wp-content/uploads/2021/03/Sector-Statistics-Report-Q2-2020-2021-1.pdf (accessed 27 April 2021). See also E Nabenyo 'Kenya' in Paradigm Initiative (ed) *Digital Rights and Inclusion in Africa Report* (2020) 51.

69 As above.

70 S Kemp 'Digital 2020: Algeria' (17 February 2020) https://datareportal.com/reports/digital-2020-algeria#:~:text=There%20were%2022.71%20million%20internet,at%2052%25%20in%20January%202020 (accessed 2 February 2022).

71 Freedom House 'Tunisia: Freedom on the Net 2020 Country Report, 2020' (2020) https://freedomhouse.org/country/tunisia/freedom-net/2020 (accessed 2 February 2022).

72 DD Sasu 'Regional distribution of households owning computers in Ghana 2018' (5 January 2021) https://www.statista.com/statistics/1139237/households-owning-computers-in-ghana-by-region/ (accessed 23 April 2021).

73 Internet World Stats 'Côte d'Ivoire' June 2010 https://internetworldstats.com/af/ci.htm (accessed 2 February 2022).

74 Ministry of Communications and Information Technology 'Information and Communication Technology Indicators Bulletin' 2020 https://mcit.gov.eg/En/Publication/Publication_Summary/9260 (accessed 2 February 2022).

75 'A young nation: 40% of Egypt's population are under 18' *Ahram Online* 20 November 2017 https://english.ahram.org.eg/NewsContent/1/0/281848/Egypt/0/A-young-nation--of-Egypts-population-are-under-.aspx (accessed 2 February 2022).

76 World Bank 'Individuals using the internet (% of population) – Mauritius' (2020) https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=MU (accessed 2 February 2022).

(PSE)' that set ICT development as one of its main pillars, Senegal has developed the 'Digital Senegal 2025', its National ICT strategy, and the National Cyber Security Strategy 2022 (SNC2022). These various complementary strategies reflect the long-term vision of a secure digital society.[77]

Despite comprehensive data on the number of children using the internet in South Africa, it is clear that children in South Africa are increasingly accessing the online world. Notably, South Africa retains a high ranking in respect of internet rights and freedoms, being ranked as the continents best-performing country in the Inclusive Internet Index for 2020.[78] Over the last few years, South Africa has taken significant strides in moving towards an inclusive digital environment. However, and despite these efforts, South Africa still faces significant hurdles in advancing digital rights, and many of the existing inequalities, barriers to access, and structures of discrimination have been magnified by the global pandemic. Recent statistics indicate that approximately 63 per cent of people in South Africa were part of the digital population as internet users.[79]

Cameroon reports 50 per cent of urban residents having access compared to only 10 per cent of rural inhabitants. Overall internet use stands at 28.9 per cent, with more people using mobile phones than computers for internet access.[80] There is an observable gender divide in Cameroon in relation to access to information. Boys' literacy is higher than girls', and 80 per cent of male adolescents consume mass media compared to 65 per cent of female adolescents.

In the Democratic Republic of Congo (DRC) internet access is very limited, at 17.7 per cent, and electricity shortages are common.[81] In Benin, current access is 30.5 per cent and has increased hugely in recent times.[82]

In some countries, such as Ethiopia, the overall digital rights landscape has in recent years been marred by extensive internet shutdowns, social media blocks, government surveillance and instances of online harassment.[83] In Zimbabwe, the country report spells out that the economic and political climate has played a significant role in the ICT landscape. There has been a decline in the access and use of ICTs in Zimbabwe with the total active mobile subscriptions declining, and mobile network operating costs growing by over 200 per cent. Access to the internet remains prohibitively expensive for the majority of Zimbabweans, and while there have been no reported internet shutdowns in the last year, restrictions on dissenting content remain rife, and the newly proposed Cybersecurity and Data Protection Bill has raised several concerns relating to privacy and surveillance and limitations on free speech.[84]

77 Sénégal Emergent 'Stratégie Sénégal Numérique 2016-2025' October 2016 https://tinyurl.com/f4t6z63s (accessed 2 February 2022); Commonwealth Telecommunications Organisation 'STRATÉGIE NATIONALE DE CYBERSÉCURITÉ DU SÉNÉGAL (SNC2022)' (November 2017) http://www.numerique.gouv.sn/sites/default/files/SNC2022-vf.pdf (accessed 2 February 2022).

78 Freedom House 'Freedom on the Net 2020 – South Africa' https://freedomhouse.org/country/south-africa/freedom-net/2020 (accessed 10 February 2022).

79 Statista 'Digital population in South Africa as of January 2020' (2020) https://www.statista.com/statistics/685134/south-africa-digital-population/ (accessed 2 February 2022); Statistics South Africa 'General Household Survey' (2018) http://www.statssa.gov.za/publications/P0318/P03182018.pdf (accessed 2 February 2022).

80 S Kemp 'Digital 2020: Cameroon' (17 February 2020) https://datareportal.com/reports/digital-2020-cameroon (accessed 20 April 2021).

81 Internet World Stats 'Internet penetration in Africa' (2020) https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/ (accessed 15 April 2020).

82 International Union of Telecommunications 'Global Cybersecurity Index 2019' (2020) https://tinyurl.com/4u2vrd8r (accessed 9 February 2022).

83 Inclusive Internet Index 'Ethiopia' (2021) https://theinclusiveinternet.eiu.com/explore/countries/ET/ (accessed 2 February 2022).

84 Freedom House 'Freedom on the Net 2020: Zimbabwe' (2020) https://freedomhouse.org/country/zimbabwe/freedom-net/2020 (accessed 2 February 2022).

3 Regulatory authorities

Most countries have one or another form of regulatory authority. Tanzania has a Communications Regulatory Authority (TCRA), which is responsible for regulating the telecommunications and broadcasting sectors in Tanzania.[85] This body is also responsible for issuing licenses to online content service providers and internet service providers. With a view to prevent and manage cybersecurity incidents, the TCRA has developed a Computer Emergency Response Team (CERT).[86] In Mauritius, the Mauritian Constitution protects the right to freedom of expression and access to information, and the Information and Communication Technologies Act 2001 (as amended), establishes the Information, Communications and Technology Authority (ICTA).[87] ICTA is responsible for, among other things, democratising access to information taking into account the quality, diversity and plurality in the choice of services available through the use of information and communication technologies.[88] Also, the Mauritian Cybercrime Online Reporting System (MAUCORS) has been developed as a secure channel for reporting cybercrimes, including offensive or illegal contents such as pornographic materials, child sexual exploitation material, sexually explicit contents, promotion of racism and terrorism, hate speech, violence and graphic content, and spam.[89]

Despite Algeria's publication of the law relating to data protection in 2018, the entry in force of this personal data protection law is subject to the actual installation of the authority in charge of protection of personal data which was at April 2021 not established yet.[90]

In Burkina Faso, internet and ISPs are regulated by the Autorité de régulation des communications éléctroniques (ARCEP), which in English is the Electronic Communications Regulatory Authority, established Law N° 51/98/AN of 4 December 1998, on the general regulation of eCommunications networks and services in Burkina Faso. ARCEP is an independent administrative institution with legal personality and financial autonomy, placed under the administrative supervision of the Prime Minister. Access to information is regulated by the National Authority for Access to Public Information (ANAIP), created by Law N° 051 on access to public information. ANAIP is an independent administrative authority with legal personality and management autonomy, funded by the state.[91]

Data protection is regulated by the Commission de l'Informatique et des Libertés (CIL)/Commission for Computing and Liberties, which is an independent administrative authority, created by the Personal Data Protection Act. CIL has a power to control public and private organisations, and a power to sanction and denounce the prosecution of offenders to its establishing law. CIL also regulates the protection of personal information, in accordance with section 2 of the Personal Data Protection Act. It is operational since December 2007.[92]

Malawi's response is inadequate regarding whether the state blocks, filters or compels service providers to block or filter internet content. It was recorded by Freedom House that 'the current government does not block or filter content aside from child sexual abuse images'.[93]

In Benin, while there is no specific law on cybersecurity, its national cybersecurity measures,

85 To learn more about TCRA, visit zimehifadhiwa 'JAMHURI YA MUUNGANO WA TANZANIA MAMLAKA YA MAWASILIANO TANZANIA TAASISI YENYE VIWANGO VYA ISO 9001: 2015' (2022) https://www.tcra.go.tz/ (accessed 12 June 2021).

86 TZ-Cert 'TZ-Cert profile' https://www.tzcert.go.tz/about-us/tz-cert-profile/ (accessed 9 February 2022).

87 To learn more about ICTA, visit Information and Communication Technologies Authority 'ICTA' (2022) https://www.icta.mu (accessed 12 June 2021).

88 Information and Communication Technologies Act 2001, sec 16(a).

89 Government of Mauritius 'Mauritian cybercrime online reporting system' (2020) http://maucors.govmu.org/English/Reporting/Pages/default.aspx (accessed 7 February 2022).

90 A Sator 'DATA PROTECTION AND CYBERSECURITY LAWS IN ALGERIA' (5 March 2021) https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/algeria (accessed 7 February 2022).

91 Burkina Faso LOI N°051-2015/CNT PORTANT DROIT D'ACCES A L'INFORMATION PUBLIQUE ET AUX DOCUMENTS ADMINISTRATIFS, art 52 https://tinyurl.com/uebdc72c (accessed 7 February 2022).

92 As above.

93 N Taboor 'Malawi puts more focus on protecting children on the Internet' *iAfrikan* 7 November 2017 https://www.

mainly the improvements under the National Agency for the Security of Information Systems (ANSSI), have notably earned it to be ranked 8th African country on the Global Cybersecurity Index.[94] In Uganda, the Ministry of ICT and National Guidance oversees the ICT sector and provides the framework to guide implementation. The Ministry is supported by various regulatory agencies, including the Uganda Communications Commission (UCC) – regulating the telecommunications sector, and the National Information Technology Authority Uganda (NITA-U) – regulating the IT sector. Data regulation is ensured by the Personal Data Protection Authority (APDP), an independent national administrative authority responsible for ensuring that the processing of personal data is carried out in accordance with the provisions of Book V of the Digital Code.[95] This Authority is empowered to conduct investigations or initiate proceedings in the event of non-compliance with the aforementioned provisions. The APDP was created by the Digital Code of 2018 to ensure the 'respect for privacy in general on the territory of the Republic of Benin'. Thus, it also covers both the state and the private sector, and ensures the regulation of personal information.[96]

In Cameroon, the main regulator of the internet, telecommunications and access to information is ANTIC, the National Information and Communication Technology Agency. Its duties include ensuring the ethical use of ICT, consumer protection and privacy, as well as regulating and monitoring activities that relate to the security of information systems and electronic communications networks. There is no specific data protection authority, so this also falls to ANTIC.[97]

In Egypt, telecommunications services and ISPs are regulated by the National Telecommunication Regulatory Authority (NTRA) under the Telecommunication Regulation Law (Law 10 of 2003).[98] The authority is subordinated to the Ministry of Communications and Information Technology (MCIT).[99] The Data Protection Law established the Data Protection Centre and is affiliated to the MCIT.

In 2020 and 2021, several regulations and guidelines were issued in respect to Kenya's Data Protection Act (DPA) including:

- Data Protection Impact Assessment guidelines;
- a Guidance Note on Consent;
- a Complaints Management Manual;
- Data Protection Compliance and Enforcement Regulation;
- Data Protection Registration of Data Controllers and Data Processors Regulations; and
- Data Protection General Regulations.

On the matter of regulatory authorities, the DPA makes provision for the establishment of the Office of the Data Protection Commissioner (ODPC). This Office fulfils numerous functions including:

- establishing and maintaining a register on the processing of data by data controllers and data processors;
- providing oversight and ensuring compliance with the DPA; and
- carrying out investigations of public and private entities to evaluate compliance with the Act.[100]

In Mozambique, there is limited protection of personal information. In relation to breach the Electronic Transactions Law provides that the person or entity responsible for processing electronic data

iafrikan.com/2017/11/07/malawi-child-online-protection-cop/ (accessed 7 February 2022).

94 International Union of Telecommunications 'Global Cybersecurity Index 2019' (2019) https://tinyurl.com/4u2vrd8r (accessed 7 February 2022); Bienvenue sur le site de l'ANSSI Bénin 2021 ANSSI Bénin | Agence Nationale de la Sécurité des Systèmes d'Information https://anssi.bj/ (accessed 12 June 2021).

95 Book V of the 2017 Digital Code of the Republic of Benin.

96 RÉPUBLIQUE DU BÉNIN, Loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, (20 April 2018) https://apdp.bj/wp-content/uploads/2019/04/CODE-DU-NUMERIQUE-DU-BENIN_2018-version-APDP.pdf (accessed 7 February 2022).

97 D Moukouri 'Cameroon - Data protection overview' (March 2021) https://www.dataguidance.com/notes/cameroon-data-protection-overview (accessed 12 April 2021).

98 To learn more about the NTRA, visit National Telecom Regulatory Authority 'NTRA' https://www.tra.gov.eg/en/ (accessed 12 June 2021).

99 Department of Justice, Egypt 'Freedom on the Net 2019' https://www.justice.gov/eoir/page/file/1333771/download (accessed 7 February 2022).

100 Kenya Data Protection Act, 2019, secs 5-17.

must protect personal data against risks, losses, unauthorised access, destruction, use, modification, or disclosure.

From a regularity perspective, in 2020, the Mozambique Control Unit of the Telecommunications Traffic (UCTT) was established by the Communications Regulatory Authority (INCM). The UCTT is dedicated to telecommunications traffic control, management of SIM card registrations, and the protection and security of telecommunications networks against cyberattacks. It is also responsible for ensuring the data protection of telecommunications users.[101] It appears that INCM is the most prominent regulatory body in the context of ICT related matters.

In Morocco, the National Regulatory Agency telecommunications, (ANRT), is a government body created in 1996 under Law N° 24-96, to regulate and liberalise the telecommunications sector.[102] The Commission of the Right of Access to Information was created by Law 31.13 of 12 March 2018 on Access to Information. Its mandate, articulated in article 22 of Law 31.13, is to ensure the proper exercise of the right of access to information. Morocco has a data protection authority, the Commission nationale de contrôle de la protection des données à caractère personnel (CNDP). The Commission is governed by Law 08 of 18 February 2009, relating to the protection of individuals with respect to the processing of personal data and by its Implementation Decree 2-09-165 of 21 May 2009.[103]

In Nigeria, the Nigerian Communications Commission (NCC) regulates Internet Service Providers (ISPs).[104] The National Information Technology Agency (NITDA) regulates access to information and data protection in general. The regulation extends to public institutions as well as the private sector. Data subjects may report breaches of privacy to NITDA. Section 23 of the Cybercrimes Act 2015 prohibits child pornography and grooming but makes no specific mention of children's right to privacy.[105]

The National Data Protection Regulation Implementation Framework of Nigeria classes a 'child' as anyone under 13 and requires that those whose activity targets children

shall ensure its privacy policy is made in a child-friendly form with the aim of making children and their guardians have clear understanding of the data processing activity before grant of consent.[106]

It also encourages organisations that offer services to children to consider whether their information is presented in a clear way that a child would understand.[107]

In Ethiopia, the Proclamation to Provide for the Computer Crime addresses illegal access and an illegal interception which indirectly pertain to privacy. The Information Network Security Agency has a duty to establish online computer crimes investigation system and provide other necessary investigation technologies. Despite this Proclamation seeking to advance certain online protections, it has been criticised for strengthened the government's surveillance powers and enabling real-time monitoring or interception of communications.[108] In 2009, Ethiopia published the draft Data Protection Proclamation, but the draft was never adopted, but it appears that the Ministry of Communication and Information Technology may be preparing a

101 'INCM creates entity responsible for the control of telecommunications traffic' *INCM* 12 June 2020 https://www.arecom.gov.mz/index.php/sala-de-imprensa/noticias/380-incm-cria-entidade-responsavel-pelo-controle-de-trafego-de-telecomunicacoes (accessed 7 February 2022).

102 Agence nationale de réglementation des télécommunications 'ANRT' (2022) https://www.anrt.ma/en/ (accessed 2021).

103 Bulletin Officiel 'Decree 2-09-165 du joumada 11430' (21 May 2009) https://www.cndp.ma/images/lois/Decret-2-09-165-Fr.pdf (accessed 7 February 2022).

104 Nigerian Communications Commission 'NCC' (2022) https://www.ncc.gov.ng/ (accessed 2021)

105 Famsville Solicitors 'Developing a child online privacy protection framework in Nigeria' (29 November 2018) https://www.lexology.com/library/detail.aspx?g=5509490a-b51d-4a66-8f8f-b57de3209acb

106 NITDA 'NIGERIA DATA PROTECTION REGULATION 2019: IMPLEMENTATION FRAMEWORK' (November 2020) https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf (accessed 7 February 2022).

107 NITDA (n 45).

108 Freedom House 'Freedom on the Net: Ethiopia' (2020) https://freedomhouse.org/country/ethiopia/freedom-net/2020 (accessed 7 February 2022).

new draft.[109] This draft does not provide special protection to children or minors.

In Ghana, the Data Protection Act 2012 (DPA) is the key piece of data privacy legislation. It regulates the collection, use and disclosure of personal data and puts in place procedures for processing personal data that originates in Ghana. The data subject must be aware of what data is collected, the purpose for which it is collected, who will receive the data and what would be the consequences of failing to provide the data. The data of children who are 'under parental control' is classed as special personal data under DPA, with much stricter restrictions on processing it.[110] The age of a child under parental control is not specified, but the Ghanaian Constitution sets 18 as the upper age of childhood. DPA covers all personal data and does not make a distinction between online and offline data.

ISPs and other telecoms and media in Ghana are regulated by the National Communications Authority (NCA). Information communications technology is also regulated by the National Information Technology Agency (NITA). Internet Data protection and access to information are regulated by the Data Protection Commission (DPC) which was set up by the DPA.[111]

In the DRC, the Authority for Regulation of Posts and Telecommunications regulates the telecommunications sector. There is no specific body to regulate data protection or access to information.[112]

In Senegal, ISPs are regulated by the Telecommunications and Post Regulatory Authority (ARTP), an independent administrative authority attached to the Presidency of the Republic. The ARTP was created by the Telecommunications Code, and is in charge of regulating the telecommunications and postal sectors. The country report notes that recent developments point to the imminent adoption of an Access to Information Act, otherwise access to information is not regulated despite the constitutional guarantee of the right to information. The Commission for the Protection of Personal Data (CDP) ensures lawful processing of personal data, informs data subjects and data controllers of their rights and obligations, and ensures that ICTs do not infringe public freedoms and privacy.[113] The CDP is an independent administrative authority established by the Personal Data Protection Act.[114]

In Tunisia, the Décision Coll/Reg/2017/17 de l'Instance Nationale des Télécommunications en date du 20 Décembre 2017 is the regulator for all telecommunications and internet-related activities in Tunisia.[115] The 2004 Personal Data Protection Law provides for the establishment of the National Authority for the Protection of Personal Data, which came into being in 2009. According to article 76 of the Protection of Personal Data law the mandate is mainly to provide private entities with authorisation, receive complaints about privacy violations, notify the public prosecutor and make official recommendations on issues related to data protection without any enforcing powers.[116] The High Independent Authority for Audio-visual Communication (HAICA), established by Decree-Law 116 of 2011, has warned and sanctioned television and radio stations for the diffusion of inappropriate content for children and required changes of the material and diffusion hours. HAICA also intervened in cases of non-respect for child privacy on multiple occasions and required stations to stop the diffusion of the concerned programmes and removal of material from their websites and social media pages. HAICA receives complaints and

109 B Taye & R Teshome 'Privacy and personal data protection in Ethiopia' *CIPESA* September 2018https://cipesa.org/?wpfb_dl=379 (accessed 7 February 2022).

110 Data Protection Act 2012 (DPA) sec 37.

111 DPC 'About the commission' https://www.dataprotection.org.gh/ (accessed 9 April 2021).

112 One Trust DataGuidance 'Democratic Republic of Congo – Data protection overview' (August 2021) https://www.dataguidance.com/notes/democratic-republic-congo-data-protection-overview (accessed 8 August 2022).

113 AVIS COP 'QUARTERLY NOTICE N° 03-2018 OF THE PERSONAL DATA PROTECTION COMMISSION OF SENEGAL (CDP)' (7 November 2018) https://www.cdp.sn/content/avis-trimestriel-n%C2%B0-03-2018-de-la-commission-de-protection-des-donnees-personnelles-du (accessed 10 February 2022).

114 Law N° 2008-12 of 25 January 2008 on the Protection of Personal Data, art 5.

115 National Telecommunication Instance http://www.intt.tn/ (accessed 8 February 2022).

116 National Authority for the Protection of Personal Data http://www.inpdp.nat.tn/ (accessed 8 February 2022).

relies also on its internal monitoring observatory. Its decisions can be challenged in courts.[117]

4 Specific legislation

The legislative landscape is continentally rather fragmented. In some quarters, there has been an increase in legislation that seeks to restrict the enjoyment of internet freedoms, regulations that repress online speech, privacy, and access to information, and the intentional blocking of online and social media platforms during the elections.[118]

In Algeria, Law 18-07[119] establishes general personal data protection requirements such as express consent, data processing notifications, data subject rights, restrictions on direct marketing and data transfers. The processing of personal data concerning a child can only be carried out after obtaining the consent of their legal representative or, where applicable, the authorisation of the competent judge. Law 18-05 of 2018, among other things, sets out further protections for e-consumers, regulates cross-border e-commerce, and details obligations related to advertising through electronic means. Executive Decree 09-410 of 10 December 2009 setting the safety rules applicable to activities relating to sensitive equipment, lists encryption software in the list of sensitive goods. According to article 17 and 20 of this Decree, the exploitation and acquisition of encryption software, by natural or legal persons for the purposes of possession and use, is subject to prior authorisation of the Algerian Regulatory Authority for Post and Telecommunications after favourable opinion from the services of the Ministry of Defence and the Ministry of the Interior.

In Burkina Faso Law 01 0-2004/AN of 20 April 2004 on the protection of personal data aims to protect the rights of individuals with regard to the processing of personal data. The Information Code also elaborates on the right to privacy, from the surveillance perspective. Punishment in terms of this law is imprisonment of two months to one year, a fine of 50 000 to 1 000 000 CFA francs, or both penalties, to whoever wilfully violates privacy of others by listening to, recording, fixing or transmitting by means of any device words or images shared in a private place by a person without their consent.[120]

In Egypt, the Law on the Protection of Personal Data was issued under Resolution 151 of 2020 on 13 July 2020 and published in the Official Gazette on 15 July 2020. This law directly addresses child related data. It considers data relating to children to be sensitive personal data. Chapter six of the law requires controllers and processors, whether a natural or juristic person, to obtain a license from the Personal Data Protection Centre, a regulatory mechanism established by the law. before proceeding to collect, transfer, store, save, process or disclose sensitive personal data. In addition to obtaining an authorisation from the Data Protection Centre, which is the case in any personal data processing, when the data relates to a child, the law requires the legal guardian consent, according to article 12 of the law. It also states that:

> The participation of a child in a game, competition or any other activity shall not be conditional on the submission of the child's Personal Data more than what is necessary for participation.[121]

Additionally, according to Law 175 of 2018 on Anti-Cyber and Information Technology Crimes, any person, whether a natural or legal person, who uses, collects, or processes personal data, shall maintain the privacy of the data stored and not disclose the same without an order of relevant judicial authority. Law 10 of 2003 (Telecommunications Law) protects the privacy of telecommunications and imposes

117 MA Ltifi 'Media freedom in Tunisia stirs wide debate' *Al-Monitor* 13 November 2021 https://www.al-monitor.com/originals/2021/11/media-freedom-tunisia-stirs-wide-debate (accessed 9 February 2022).

118 Paradigm Initiative 'Tanzania' in Paradigm Initiative (ed) *Digital Rights and Inclusion in Africa Report* (2020) 103; E Wanyama 'Tanzania entrenches digital rights repression amidst covid-19 denialism and a looming election' *CIPESA* 19 August 2020 https://cipesa.org/2020/08/tanzania-entrenches-digital-rights-repression-amidst-covid-19-denialism-and-a-looming-election/ (accessed 7 February 2022); Freedom House 'Freedom in the world 2021: Tanzania' (2021) https://freedomhouse.org/country/tanzania/freedom-world/2021 (accessed 7 February 2022).

119 Law 18-07 of 25 Ramadhan 1439 Corresponding to 10 June 2018. Law 18-07 addresses children's right to privacy in art 8.

120 Law 01 0-2004/AN of April 20, 2004, sec 90.

121 The Law on the Protection of Personal Data issued under Resolution 151 of 2020.

penalties in some cases on the unauthorised violation of such privacy.

Egyptian Telecom services providers are required to ensure and maintain the confidentiality of any customer's data. Article 64 of the Telecommunications Law allows service providers, as well as their marketing agents, to collect 'accurate information and data' from 'individuals and various entities within the state'. It also compels providers to give security agencies access to their 'equipment, systems, software, and communication'.[122] Further, article 64 of the Telecommunication Regulation Law outlaws the use by telecommunications companies, their employees, or their customers of any encryption equipment without written consent from the NTRA and security agencies.[123]

In accordance with article 25 of the Anti-Cyber Crimes law of Egypt, individuals who post on websites or social media platforms videos, photos, or texts of others without their consent and in violation of their privacy are punishable by no less than six months in prison and/or a fine of 50 000-100 000 Egyptian Pounds. Posting content that 'violates the family principles and values upheld by Egyptian society' is punishable too.[124] Article 7 grants the investigative authorities the power to block any website whenever they deem that the website's content promotes extremist ideas that violate national security or damages the Egyptian economy.[125] Article 2 of the Telecommunication law requires telecommunications companies and internet service providers to retain and store users' data for 180 days. The law details an extensive list of the requested data to include: data that enables the identification of users, data on the content of their communications and those relating to the flow of use and the devices used. This means that telecom providers could be asked to turn over to authority's data describing all user practices, such as data related to websites visited, and applications installed.

In Kenya, the 2019 Data Protection Act came into force and the government is currently considering adopting other laws. For example, public consultations are being held on the Data Protection (General) Regulations (2021), the Data Protection (Compliance and Enforcement) Regulations (2021) and the Data Protection (Registration of Data Controllers and Data Processors Regulations (2021), as at May 2021. The draft regulations came after the establishment of the Office of the Data Commissioner in November 2020 pursuant to the Data Protection Act 2019.

The 2020 proposed amendments to Kenya's Constitution propose an amendment to article 31 to include, '[e]very person has the right to privacy, which includes the right not to have their personal data infringed'. The memorandum of objects and reasons for the proposed Constitutional amendments notes: The Bill proposes to amend article 31 (Privacy) to incorporate the right for the protection of personal data of citizens. The proposed amendment protects personal data of citizens in view of the advancement and adoption of digital technology by a large percentage of the population and boosts the taming of surveillance capitalism.

While the constitutional amendments have caused controversy and debate in relation to changes to the country's power structures, the explicit inclusion of 'data protection' is a strong signal for Kenya's intentions to safeguard data privacy rights. It is necessary to note, according to the Kenya report, that on 13 May 2021, Kenya's High Court ruled that President Kenyatta does not have the power to amend the Constitution in the manner in which he seeks to do so. It is therefore unlikely that the proposed privacy amendments will be forthcoming.[126]

Freedom House records that:

> Kenyans can freely use encryption tools, but a number of regulations and monitoring systems limit anonymous communication. Several publications and technology blogs often encourage Kenyans to install encryption tools.

122 Telecommunications Law 10 of 2003.

123 As above.

124 Anti-Cyber and Information Technology Crimes Law 175 of 2018.

125 As above.

126 D Miriri 'Kenyan court slams brakes on President's constitutional changes' *Reuters* 13 May 2021 https://www.reuters.com/world/africa/kenyan-court-slams-brakes-presidents-constitutional-changes-2021-05-13/ (accessed 7 February 2022).

For example, through the course of this research, no clear responses emerged regarding end-to-end encryption relating to services affecting children.[127]

Law 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data of 2009 applies to all personal data protection online and offline in Morocco. The legislator also defines the processing of personal data as all operations or sets of operations carried out or not using processes automated and applied to personal data. Moroccan law does not impose any special requirements for the processing of children's personal data.[128] Law 24-96 of 1997 governing the post and telecommunications states in article 26 that operators of public telecommunications networks, providers of telecommunications services, as well as their employees are required to respect the secrecy of correspondence by telecommunications and the conditions for the protection of privacy and personal data of users.[129]

In Malawi, there is no comprehensive data protection law, though a bill has been presented in 2021 for public comment. The bill promises to

> provide a comprehensive legislative framework for the protection and security of personal data, consolidate data protection provisions currently found in various Acts of Parliament, and protect the privacy of individuals without hampering social and economic development in Malawi.

Malawi does have an Electronic Transactions and Cybersecurity Act (ETCA)[130] which replicates some provisions seen in data protection laws. A key objective of ECTA is to 'to address ethical issues in the use of information and communication technology in order to protect the rights of children and the underprivileged'.[131] Similarly, the Communications Act 34 of 2016 criminalises unlawful interception or interference, and disclosure of electronic communications.

In Morocco, Decree 2-13-88137 of 2015, shifts responsibility for authorising and monitoring 'electronic certifications', including encryption, from the civilian National Regulatory Agency Telecommunications (ANRT) to the military's General Directorate for the Security of Information Systems.

Akin to Malawi, Tanzania too lacks a comprehensive data protection and privacy law. However, the Electronic and Postal Communications Regulations (Online Content) which came into effect in 2020, prohibits a range of content including content that:

- Insults, slanders, and defames other persons, or exposes news, photos or comments related to a person's privacy, or publication of private information regardless of whether the information is true; and
- Motivates or promotes phone tapping, espionage, data theft, tracking, recording or intercepting communications or conversation without right.

It is necessary to note that the 2020 regulations have sparked widespread outcry, on the basis that '[t]he regulations entrench the licensing and taxation of bloggers, online discussion forums, radio and television webcasters, and repress online speech, privacy and access to information'.[132] There have been two 'failed attempts' to enact data protection laws in Tanzania: [T]he 2006 Freedom of Information Draft Bill failed to define key terms and was derided by journalists as curtailing freedom of information, and the Draft Data Protection Bill 2014 – which was supposedly based on the European Union (EU) Directive and the Southern African Development Community (SADC) Model Law – omitted consent as a condition for the processing and has been criticised as effectively inoperable despite its similarities to data protection legislation in other countries.[133]

127 Freedom House 'Freedom on the Net 2020: Kenya' https://freedomhouse.org/country/kenya/freedom-net/2020 (accessed 7 February 2022).

128 The Law 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data https://anrt.ma/content/dahir-ndeg-1-09-15-du-22-safar-1430-18-fevrier-2009 (accessed 2021).

129 Bulletin Officie 'Law 24-96 governing the post and telecommunications' 16 October 1975 https://www.anrt.ma/sites/default/files/documentation/1997-1-97-162-24-96-loi-telecom-fr.pdf (accessed 7 February 2022).

130 Electronic Transactions and Cybersecurity Act 33 of 2016.

131 Electronic Transactions and Cybersecurity Act (n 69) sec 3.

132 Wanyama (n 57).

133 ALT Advisory 'Factsheet: Tanzania' (31 March 2021) https://dataprotection.africa/wp-content/uploads/2020/03/Tanzania-Factsheet-updated-20200331.pdf (accessed 7 February 2022).

In Benin, a Digital Code[134] exists along with a National Cybersecurity Strategy and is premised on digital development in coordination with human rights. It repeals all previous contrary provisions.

In Senegal, whilst there is legislation, it is in flux. The Orientation Law on the Information Society also guarantees the fundamental right of individuals to the respect for their privacy, including secrecy of communications and the protection of their rights and freedoms with regard to any processing of personal data (article 6). The Personal Data Protection Act aims to fight against violations of privacy that may be caused by the collection, processing, transmission, storage and use of personal data. It considers all data processing, whether automated or not. Offences against its provisions are referred to the penalties provided for by the Penal Code and the Cybercrime Act. Enacted since 2008, stakeholders have noted its shortcomings and the need for convergence with regional and international data protection developments and standards, including General Data Protection Regulation (GDPR), the Budapest Convention, and the African Union Convention on Cyber Security and Personal Data Protection. Therefore, this law is under review, with a new bill resulting from a national stakeholder's consultation.[135]

In Tunisia, the Organic Act 63 of 27 July 2004 on Personal Data Protection governs aspects of privacy. It details the scope of personal data protection, and establishes a national authority in charge of its enforcement. Article 4 of the law defines personal data, subject to protection, as

> any information, regardless of its origin or form, which directly or indirectly identifies a person or allows a person to become identifiable through various symbols or data except information related to public life or considered as such by the law.

The law does not explicitly indicate if it applies to the online processing of personal data. Public institutions are not required to obtain verbal and written consent from data subjects when collecting and processing data. Data subjects are also barred from accessing or opposing information held about them by the mentioned public authorities.

Article 28 is the main article referred to in case the data subject is a child. It states that

> the processing of personal data concerning a child can only be carried out after obtaining the consent of the guardian and the authorization of the family judge. The family judge can order treatment even without the guardian's consent when the best interests of the child are so required. The family judge can revoke the authorization at any time.

The law addresses child-specific provisions in other articles: articles 30, 43, 44, 47, 52, 57, 62, 68, 73 in relation to advertisements purposes, opposition right, data collection and destruction, communication to tiers, transfer to abroad, health-related and scientific research purposes.[136]

Decree 4473 of 2014 requires internet service providers to adopt the solutions and mechanisms that make it possible to provide a secure browsing service for children on the internet. They have to define a secure browsing service for children on the internet and provide for it in service contracts as a service of choice that depends on the will of the customer.[137]

In Uganda, it has been noted that the Uganda Communications Act, however, seeks to provide a level of privacy protection through provisions that address the unlawful interception and disclosure of communication by a service provider. The Computer Misuse Act provides that it is a misdemeanour to wilfully and repeatedly uses electronic communication to disturb or attempt to disturb a person's right to privacy. The Computer Misuse Act provides certain protections to children, with a particular focus on the child exploitation material. A person who produces, offers or makes available, distributes or transmits, procures or unlawfully possesses child exploitation material on a computer commits an offence. Additionally, a person who makes available pornographic materials to a child

134 Law N° 2017-20 of 20 April 2018, on the Digital Code in the Republic of Benin.

135 S Toussi 'Building a robust data protection regime in Senegal' *CIPESA* 10 March 2020 https://cipesa.org/2020/03/building-a-robust-data-protection-regime-in-senegal/ (accessed 7 February 2022).

136 INPDP 'Loi organique numéro 63 en date du 27 juillet 2004 portant sur la protection des données à caractère personnel' (27 July 2004) http://www.inpdp.nat.tn/ressources/loi_2004.pdf (accessed 7 February 2022) .

137 Journal Officiel de la République Tunisienne 'Decree 4773 of 2014 Fixing the Conditions and Procedures to Grant the Authorisation for the Activity of Supplying Internet Services' (23 January 2015) http://www.intt.tn/upload/txts/fr/d%C3%A9cret2014_4773.pdf (accessed 7 February 2022).

commits an offence. Child exploitation material includes pornographic material that depicts a child engaged in sexually suggestive or explicit conduct a person appearing to be a child engaged in sexually suggestive or explicit conduct; or realistic images representing children engaged in sexually suggestive or explicit conduct. Cyber-harassment, cyber-stalking and offensive communications are also outlawed.[138] The Anti-pornography Act, 2014, also prohibits the production, publication, broadcasting, or importing of child sexual abuse material.[139]

In addition to the above, in 2019, the Data Protection and Privacy Act (DPPA) has become Uganda's primary privacy and data protection legislation. Despite the Act seeking to protect individuals and their personal data by regulating the processing of personal information by state and non-state actors, within and outside Uganda, little has been done to meaningfully implement the Act. It is reported that neither state nor non-state actors have taken measures to change their policies and practices as per the obligations under the Act.[140] Nevertheless, the Act expressly includes provisions relating to the personal information of children. Section 8 provides:

(a) A person shall not collect or process personal data relating to a child unless the collection or processing thereof is:
(b) Carried out with the prior consent of the parent or guardian or any other person having authority to make decisions on behalf of the child;
(c) Necessary to comply with the law; or
(d) For research or statistical purposes.

The DPPA requires data processors, collectors, and controllers to immediately notify the National Information technology authority upon reasonable belief that personal data has been accessed or acquired by an unauthorised person.

Notably, Uganda was one of the first African countries to enact a right to information law, the Access to Information Act (ATIA) 2005 and later the Access to Information Regulations. The ATIA seeks to, among other things, promote the right to access information, promote an efficient, effective, transparent and accountable government and enable the public to effectively access and participate in decisions that affect them as citizens of the country. These do not, however, provide for a regulatory body that oversees access to information.

In Cote D'Ivoire, a set of legislative measures has been put in place to ensure proper infrastructure management, service supply, good governance and respect for consumer rights. These legislations include, but are not limited to: the Orientation of Information Society Act of 2017, the Personal Data Protection Act of 2013, the eTransactions Act of 2017, the Cybercrime Act of 2017, and the Order on Telecommunications and ICT of 2012. However, there is no law that directly addresses children's right to privacy, for the Personal Data Protection Act largely provides for the right of the data subject to obtain the erasure of his personal data and the cessation of its dissemination, in particular those made available when he was a child. In addition, the Minority Act addresses child's protection without a specific focus on child's privacy.[141]

By contrast, in the DRC there is no legislation on data protection. There is currently no policy on the protection of children from online harm (although a bill on online protection has been proposed by the Youth Parliament) and there are no safeguards on filtering and monitoring.[142]

In Cameroon, the Cybersecurity and Cybercrime Law of 2010 places a duty of confidentiality upon telecommunications operators. Article 41 of this Act provides for the privacy of electronic communications and personal data may only be processed on lawful grounds. However, Cameroon as yet, has no dedicated data protection or privacy law.[143]

138 The Computer Misuse Act 2011, secs 23, 24, 25, 26.
139 Anti-pornography Act, 2014, sec 14.
140 Unwanted Witness 'One year on, what has Uganda's Data Protection Law changed?' *Privacy International* 3 March 2020 https://privacyinternational.org/news-analysis/3385/one-year-what-has-ugandas-data-protection-law-changed (accessed 7 February 2022).
141 Côte d'Ivoire; Law 2013-450 of 19 June 2013, on the Protection of Personal Data, art 33.
142 The Youth Parliament of the Democratic Republic of Congo http://jeunescongo.e-monsite.com/ (accessed 22 April 2021).
143 Defy Hate Now 'The state of digital rights in Cameroon' (21 January 2020) https://defyhatenow.org/the-state-of-digital-rights-in-cameroon-2/ (accessed 12 April 2021); A Borainea & LD Ngaundje 'The fight against cybercrime

In Nigeria, two bills to combat hate speech have been proposed: The National Commission for the Prohibition of Hate Speech Bill, 2019, and the Protection from Internet Falsehood and Manipulation and other Related Offences Bill, 2019. It is reported that Amnesty International has expressed concerns that they would

> give authorities arbitrary powers to shut down the internet and limit access to social media and make criticizing the government punishable with penalties of up to three years in prison.[144]

The Bill does not make explicit the liability of internet and social media platforms or prescribe suitable punishments for corporate entities. The Bill largely deals with ethnic hate speech rather than all forms of discrimination. Anti LGBT hate speech is not covered. Homosexual acts are illegal throughout Nigeria and punishable by death in 12 states.[145]

Mauritius is described as a data protection trail blazer in Africa.[146] It was among the first movers in the data privacy space in Africa. In 2004, Mauritius enacted the Data Protection Act and became the first African country to establish the Office of the Data Protection Commissioner and make it operational. In January 2018, the Data Protection Act came into effect, repealing the former act, so as to align with the European Union General Data Protection Regulation 2016/679 (GDPR). The updates to the law include the implementation of data protection impact assessments, notification of personal data breaches, stricter security requirements attached to data processing, and clearer standards around the details of lawful processing. The updated law includes provisions pertaining to data protection impact assessments, notification of personal data breaches, stricter security requirements attached to data processing, and clearer standards around the details of lawful processing.

The Data Protection Office, headed by the Data Protection Commissioner, is responsible for, among other things:

- ensuring compliance with the Act and its regulations;
- issuing or approving Codes of Practice or Guidelines;
- maintaining a register of controllers and processors;
- exercising control on all data processing operations; and
- investigating complaints.

Section 30 of the Data Protection Act provides:

1. No person shall process the personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian.
2. Where the personal data of a child below the age of 16 years are involved, a controller shall make every reasonable effort to verify that consent has been given or authorised, considering available technology

In Mauritius, recently proposed amendments to the existing Information and Communication Technologies Act by the Information and Communication Technologies Authority (ICTA) have sparked a widespread outcry, and concerns regarding significant threats to freedom of expression, privacy and security.[147] The proposed amendments have raised alarm bells amongst local and international free expression advocates, as they would enable government officials who have established instances of 'abuse and misuse' to block social media accounts and track down users using their IP addresses. Their main concern, however, is that ICTA seeks to install a local/proxy server that impersonates social media networks to fool devices and web browsers into sending secure information to the local server instead of social media networks, effectively creating an archive of the social media information of all users in Mauritius before resending it to the social media networks' servers. This plan fails to mention

in Cameroon' (2019) 35 *International Journal of Computer* 90.

144 'Nigeria: Bills on hate speech and social media are dangerous attacks on freedom of expression' *Amnesty International* 4 December 2019 https://www.amnesty.org/en/latest/news/2019/12/nigeria-bills-on-hate-speech-and-social-media-are-dangerous-attacks-on-freedom-of-expression/ (accessed 7 February 2022).

145 This is a common theme in other country reports, such as Uganda andTanzania.

146 ALT Advisory 'Factsheet Mauritius' *Data Protection Africa* 31 March 2020 https://dataprotection.africa/wp-content/uploads/2020/03/Mauritius-Factsheet-updated-20200331.pdf (accessed 7 February 2022).

147 Information & Communication Technologies Authority 'Consultation paper on proposed amendments to the ICT Act for regulating the use and addressing the abuse and misuse of Social Media in Mauritius' (14 April 2021) https://www.icta.mu/docs/2021/Social_Media_Public_Consultation.pdf (accessed 7 February 2022).

how long the information will be archived, or how user data will be protected from data breaches.[148] The report quotes one commentator to the effect that

> The proposed amendments are radically disproportionate to their stated aims of countering offensive speech on social media and would create space for state surveillance of the lawful conduct of private citizens while undermining digital security through attacking encryption.

The ICTA in response to concerns has noted that the amendment is not meant to enable spying on Mauritians and notes that only public social networks will be targeted. Private messengers like Whatsapp, Viber and Telegram are not affected at all, and private communications between individuals are also protected by the Constitution.

In anticipation of the 38th Session of the Universal Peer Review (UPR) Process at the United Nations Human Rights Council that took place in April 2021, a collaboration of organisations filed a submission on digital rights in Mozambique. The submission provides a useful overview of the privacy landscape in Mozambique and explains that there have been efforts by civil society and the government to engage in opportunities for creating a safer online environment in Mozambique. For instance, Media Institute of Southern Africa (MISA) Mozambique and the Ministry of Science and Technology met and reflected on how to further uphold privacy and personal data projection beyond the existence of a cybersecurity legal framework.

In 2019 the Mozambican Penal Code was revised, and now includes provisions related to the invasion of privacy, prohibiting the interception, recording, transmission or disclosure of online communications, including email, messages, audio-visual and social media content without consent.[149] The revision has not been welcomed by all, with some digital rights experts noting that the new amendments could threaten freedom of expression. The primary concern appears to lie with the new penalty against whoever

> 'captures, photographs, films, manipulates, records or disseminates images of persons or intimate objects or spaces", as well as on whoever "secretly observes or listens to persons who are in a private place',

and also, those who disclose 'facts concerning the private life or serious illness of another person'.[150]

In 2020, the President signed South Africa's data protection law – Protection of Personal Information Act (POPIA) – signalling an important moment for data protection in the country, not only to ensure much needed regulatory compliance, but also to ensure that the right to privacy is meaningfully realised in the information age. POPIA fully came into effect on 1 July 2021. POPIA was signed into law on 19 November 2013 and has come into force incrementally. Section 114 of POPIA, which came into force on 1 July 2020, requires compliance with POPIA within one year from the date of its commencement. POPIA provides eight conditions for the lawful processing of personal information. In summary, these are as follows:

- Condition 1: Accountability (section 8): That the responsible party must ensure that the conditions for the lawful processing of personal information are complied with at the time of determining the purpose and means of the processing and during the processing itself.
- Condition 2: Processing limitation (sections 9-12): That personal information must be processed lawfully and in a reasonable manner, and only if it is adequate, relevant and not excessive given the purpose for which it is processed.

148 J York & D Greene 'Proposed new internet law in Mauritius raises serious human rights concerns' *Electronic Frontier Foundation* 30 April 2021 https://www.eff.org/deeplinks/2021/04/proposed-new-internet-law-mauritius-raises-serious-human-rights-concerns (accessed 7 February 2022).

149 Law N º 24/2019.

150 'MISA-Mozambique and government discuss legislative priorities in cybersecurity and data protection' *MISA Mozambique* 28 September 2020 https://www.misa.org.mz/index.php/destaques/noticias/97-misa-mocambique-e-governo-discutem-prioridades-legislativas-em-ciberseguranca-e-proteccao-de-dados (accessed 7 February 2022); D Tsandzana 'New privacy law in Mozambique threatens freedom of expression, activists say' *Global Voices* 16 January 2020 https://globalvoices.org/2020/01/16/new-privacy-law-in-mozambique-threatens-freedom-of-expression-activists-say/ (7 February 2022).

- Condition 3: Purpose specification (sections 13-14): That personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party, and should not be retained for longer than is necessary to achieve that purpose.
- Condition 4: Further processing limitation (section 15): That further processing of personal information should be compatible with the purpose for which it was collected.
- Condition 5: Information quality (section 16): That the responsible party is required to take steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.
- Condition 6: Openness (sections 17 and 18): That the responsible party is required to take reasonably practicable steps to ensure that the data subject is aware of, amongst other things, what personal information is being collected, the source of the information, the purpose for which it is being collected, and the name and address of the responsible party.
- Condition 7: Security safeguards (sections 19-22): That the responsible party is required to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures, having regard to generally accepted information security practices and procedures.
- Condition 8: Data subject participation (sections 23-25): That a data subject has a right to request a responsible party to confirm whether personal information is held about the data subject, and be provided with the record or a description of the information held. A data subject may further request a responsible party to correct or delete personal information about the data subject that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

POPIA further sets out substantive requirements for, amongst other things, direct marketing; the use of directories; automated decision-making about data subjects; and the circumstances under which personal information may be transferred outside of South Africa. Chapter 5 of POPIA establishes the Office of the Information Regulator (Information Regulator), comprised of a Chairperson and additional members. Its functions include providing education on protection and processing of personal information; monitoring and enforcing POPIA compliance; consulting and mediating; investigating and resolving complaints; issuing enforcement notices and facilitating cross-border cooperation.[151]

The Cyber Crime Bill remains before the South African President for assent.[152] Additionally, a proposed Bill on hate speech is before Parliament – the Prevention and Combating of Hate Crimes and Hate Speech Bill – and recent amendments have been proposed to the Promotion of Equality and Prevention of Unfair Discrimination Act.

In Zimbabwe, a Cyber Security and Data Protection Bill is pending. It was gazetted on 15 May 2020. The Bill is intended to consolidate cyber-related offences and provide for data protection and seeks to 'create a technology-driven business environment and encourage technological development and the lawful use of technology'. The Bill will establish a Data Protection Authority

151 Protection of Personal Information Act (POPIA) 4 of 2013; A Singh 'Why POPIA is about rights – not just compliance' *Alt-Advisory* 23 June 2020 https://altadvisory.africa/2020/06/23/why-popia-is-about-rights-not-just-compliance/ (accessed 25 November 2020); The Presidency 'Commencement of certain sections of the Protection of Personal Information Act, 2013' (2020) http://www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013 (accessed 7 February 2022); African Union Convention on Cyber Security and Personal Data Protection 'List of countries which signed, ratified/acceded' (18 June 2020) https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (accessed 7 February 2022); In accordance with Proclamation R25 of 2014 the following sections came into force with effect from 11 April 2014: sec 1; Part A of chapter 5; secs 112 and 113. In accordance with Proclamation R21 of 2020, the following sections came into force with effect from 1 July 2020: secs 2-38; secs 55-109; secs 111 and 114(1), (2) and (3); and the following sections came into force with effect from 30 June 2021: secs 110 and 114(4); secs 69-72; 'Factsheet: : South Africa' *AltAdvisory* 3 August 2020 https://dataprotection.africa/wp-content/uploads/2020/08/South-Africa-Factsheet-updated-20200803.pdf (accessed 7 February 2022).

152 T Sibidla 'Data protection and privacy regulation: A roundup of developments in Africa in 2021' https://www.werksmans.com/legal-updates-and-opinions/data-protection-and-privacy-regulation-a-roundup-of-developments-in-africa-in-2021/ (accessed 7 February 2022).

as the same institution mandated under the Postal and Telecommunications Act (PORTRAZ).[153] The Bill provides for, among other things:

- The establishment of the Cyber Security Centre and the Data Protection Authority within POTRAZ and their relevant functions.
- The minimum standards and general rules on the processing of data.
- The permissibility and non-permissibility of the transfer of personal information outside Zimbabwe.
- The introduction of cybercrimes and their respective penalties, including hacking, the unlawful acquisition or use of data, the transmission of data messages inciting violence or damage to property, cyber-bullying and harassment, the transmission of false data message intending to cause harm, the transmission of intimate images without consent, identity-related offences and offences against children.
- The investigation and collection of evidence of cybercrime and unauthorized data collection and breaches.
- The obligations and immunity of electronic communications network or access service providers, hosting providers, caching providers and internet service providers.

The Bill has sparked a significant outcry, with prominent domestic and international organisations raising concerns over the Bill and its potential shortfalls in terms of its constitutionality and in terms of Zimbabwe's regional and international commitments. The Bill has been widely critiqued as being a tool for the Zimbabwean government to stifle freedom of expression, access to information, promote interference of private communications and data, and use search and seizure powers to access the information of activists in order to quell protests.

From a regulatory perspective, the Bill envisages the establishment of the Cyber Security Centre and the Data Protection Authority within the POTRAZ and their relevant functions. POTRAZ is the regulatory authority of Zimbabwe's postal and telecommunications sector.[154]

Also, in Zimbabwe, the Interception of Communications Act (ICA) regulates the interception of communications, including telephonic communications, postal telecommunications as well as certain online communications. This Act does not explicitly reference privacy rights, and civil society organisations such as MISA Zimbabwe have called into question its constitutionality, raising concerns around the lack of transparency and oversight mechanisms. Constitutionality concerns have also been raised by the Zimbabwe Human Rights NGO Forum, the Digital Society of Zimbabwe, the International Human Rights Clinic at Harvard Law School, and Privacy International.[155]

5 Child laws

Some child laws protect the child's right to privacy. An example is Nigeria's Child Rights Act, 2003, which grants this protection to children, but with the proviso that this does not 'affect the rights of parents and, where applicable, legal guardians, to exercise reasonable supervision and control over the conduct of their children and wards'.[156] However, only 24 states have localised this Act. In Tanzania, the Law of the Child is Tanzania's primary legislation dealing with children's rights[157] and seeks to give effect to international and regional conventions on the rights of the child. It provides that 'the best interest of a child shall be the primary consideration in all actions concerning a child whether undertaken by public or private social welfare institutions, courts or administrative bodies'.[158] This legislation further recognises that children have a right to an opinion and provides that no person shall deprive a child capable of forming views the right to express an opinion, to be listened to and to participate in decisions that affect their well-being. The Law of the Child does not explicitly provide for children's privacy rights. Section 5 of the 2011 Zanzibar

153 Chapter 12:50 of Act 2 of 2000.

154 As above.

155 Zimbabwe Human Rights NGO Forum, the Digital Society of Zimbabwe, the International Human Rights Clinic at Harvard Law School, and Privacy International 'Stakeholder Report Universal Periodic Review 26th Session – Zimbabwe: The rights to privacy in Zimbabwe' (March 2016) https://hrp.law.harvard.edu/wp-content/uploads/2016/04/zimbabwe_upr2016.pdf (accessed 8 February 2022).

156 Echoing the African Children's Charter provision.

157 2011 Zanzibar Children's Act; the 2009 Law of the Child Act of the Mainland.

158 Law of the Child, 2009 Part II, subs (a), para 4.2

Children's Act, obliges the state to ensure that the 'views expressed by the child may be given due consideration'. Section 11 of the 2009 Law of the Child Act of the Mainland, provides that a child has the

> right of opinion and no person shall deprive a child capable of forming views the right to express an opinion, to be listened to and to participate in decisions which affect his well-being.

In Egypt, Law 12 of 1996, amended by Law 126 of 2008 (the Child Law) mentions the child's right to privacy but only in specific cases, such as publication of the identity of any child in conflict with the law. Article 89 of the law prohibits the publishing, showing, or circulation of any printed material or audio or visual productions on children that 'addresses basic instincts or beautifies behaviour contrary to the society values, or leads them to delinquency'.[159] The Child Law addresses child pornography explicitly in article 116(a). It prohibits the production, preparation, viewing, printing, promotion, possession, and broadcast of pornographic material using children, or related to the sexual exploitation of children.[160] This, according to the Egypt report, stretches to radicalisation of children, and article 86 bis of the Penal Code provides aggravated penalties for intentionally promoting by any means the purposes of terrorist organisations or for obtaining or producing directly or indirectly articles, publications or recordings of any kind intended to promote or encourage such purposes.[161] Furthermore, article 12 of the Data Protection law states that:

> The participation of a child in a game, competition or any other activity shall not be conditional on the submission of the child's Personal Data more than what is necessary for participation therein.[162]

It also prohibits the use of a computer or internet or information networks to induct mentioned actions or induce children to engage in prostitution or pornographic activities or defame them, or sell them.

The Children Act (as amended in 2016) of Uganda provides explicit protection for children's right to privacy. It also fills some critical gaps related to offences against children.[163] Although it does not expressly reference online harms, the general prohibition on all forms of violence including sexual abuse and exploitation, child trafficking, and emotional abuse could be interpreted to apply to the online environment as well.[164]

Benin's Child's Code 2015-08 directly provides for the child's right to privacy. It is a framework document, which integrates the Convention on the Rights of the Child along with all national laws and regulations as well as key international instruments adopted by Benin on the status, rights and protection of the child. It thus endorses that

> No child shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, or unlawful attacks on his honour and reputation. The child has the right to lawful protection against such interference or attacks.[165]

The Digital Code specially addresses the right to privacy, including the children's right to privacy in the digital sphere. It is a national framework document, which devotes its entire Fifth Book (articles 379-490) to the protection of individual's privacy. Article 379 specifies that its provisions

> are intended to set up a legal framework for the protection privacy and professional life following the collection, processing, transmission, storage and use of personal data.

It also directly addresses children's privacy protection, especially with regard to the digital environment. Several of its provisions focus on children's right to privacy, especially those relating to consent, lawful processing, service supply or direct marketing. Dealing with transparency in the processing of personal data, article 418 requires the data controller to communicate in a clear and simple, meaningful, transparent, understandable

159 Law 12 of 1996 amended by Law 126 of 2008, art 89.
160 Law 12 of 1996, art 116 *bis* (a).
161 Penal Code Article 86 *bis*.
162 Data Protection Law, art 12.
163 The Children (Amendment) Act 2016.
164 As above.
165 UN General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series,

and accessible manner vis-à-vis the child as a data subject in the processing of their personal data.

In Burkina Faso, children's right to privacy is directly addressed by the Law on the Protection of Children in Conflict with the Law or in Danger (Law 015-2014.) Under section 5,

> the child has the right to protection of the law against arbitrary or unlawful interference with his privacy, family, home or correspondence and against all unlawful attacks on his honour and reputation,

without prejudice to the rules relating to the exercise of parental authority. Further, the privacy and confidentiality of the child including the confidentiality of their personal information during court proceedings are guaranteed.[166] Section 4 recognises the child's right to participation in decisions affecting him, as well as his right to express himself. It is emphasised that a child is given the opportunity to express its opinions and to be heard in all legal and administrative proceedings relating to its situation. The Data Protection Act of Burkina Faso does not provide for child-sensitive provisions and safeguards, but the Law Protecting the Child in Conflict with the Law or in Danger provides for some child protection mechanisms, as well as the Law of 8 July 2009 Protecting the Rights of Children and Adolescents in the Media. For instance, it requires cyberspaces (in section 5) to

> prohibit the access of children under 16 to dangerous websites for the awakening of their conscience, under penalty of boycott of their business and prosecution before the International Criminal Court.[167]

In Mozambique, the Law on the Promotion and Protection of the Rights of the Child 7 of 2008, aims to promote and protect the rights of the child, as defined in the Constitution, and in terms of international and regional human rights law. Article 23 of the Law provides for the privacy rights of the child, providing that no child may be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor to unlawful offences against their honour and reputation.[168] End Child Prostitution in Asian Tourism (ECPAT) International and Rede da Criança in their Supplementary report on 'Sexual Exploitation of Children in Mozambique' to the third and fourth periodic reports of Mozambique on the implementation of the Convention on the Rights of the Child and the Optional Protocol on the sale of children, child prostitution and child pornography made some notable findings and recommendations. The organisations explained that despite low internet access in Mozambique, the incremental rise in internet users has resulted in increased risks associated with online grooming, online child sexual exploitation and the distribution of child sexual abuse material in Mozambique. The organisations recorded that there are no legal provisions that 'require internet service providers to report suspected child sexual abuse materials (CSAM) to the relevant law enforcement agencies, and there is no legislation on online grooming'.[169]

In Cameroon, there is no law that specifically addresses the privacy of children, and in fact their privacy is explicitly curtailed by article 300 of the Cameroonian Criminal Code, which gives parents and guardians the right to open or stop the correspondence of children under the age of 18.[170]

In Senegal, too, there is no law that directly addresses children's right to privacy. The Personal Data Protection Act does not include express child-sensitive provisions and safeguards. The Cybercrime Act deals with specific matters as child pornography,

vol 1577, p 3, art 16; Integrated by the Child's Code in Benin, at 514.

166 Burkina Faso; Law 015-2014/AN of 13 May 2014 on the protection of children in conflict with the law or in danger secs 5, 36, 53, 59, 69 and 74.

167 Children Parliament; Law N° 0001-2009 / PDE of 8 July 2009 protecting the rights of children and adolescents in the media in Burkina Faso, sec 5 https://tinyurl.com/24365rkz (accessed 8 February 2022).

168 The Law on the Promotion and Protection of the Rights of the Child 7 of 2008, art 23. Kindly note that this is not an official translation.

169 ECPAT International and Rede da Criança 'Supplementary report on "Sexual Exploitation of Children in Mozambique" to the third and fourth periodic reports of Mozambique on the implementation of the Convention on the Rights of the Child and the Optional Protocol on the sale of children, child prostitution and child pornography' (1 November 2018) https://www.ecpat.org/wp-content/uploads/2018/07/Convention-on-the-Rights-of-the-Child-report-on-Sexual-Exploitation-of-Children-to-the-Committee-on-the-Rights-of-the-Child-Mozambique-English-2018.pdf (accessed 8 February 2022).

170 Cameroonian Criminal Code, art 300.

discrimination and xenophobia.[171] A Children's Code which can regulate the rights of children comprehensively has been ten years in the making and is not yet complete.

Ethiopia is one of the few countries that does not have a legal framework specifically addressing children's rights at all.[172] This contributes to the gaps and deficiencies in the policy framework and implementation of programmes in Ethiopia. The Committee on the Rights of the Child has noted that they 'regret the absence of a systematic legislative review in order to bring domestic laws into compliance with the Convention', they are further 'concerned that a comprehensive Children's Code has not yet been adopted'.[173] However, the Computer Crime Proclamation does prohibit the production, transmission, sale, distribution, or possession without authorisation, any picture, poster, video, or image through a computer system that depicts a minor engaged in sexually explicit conduct, or a person appearing to be a minor engaged in sexually explicit conduct.[174] And in 2020, the Hate Speech and Disinformation Prevention and Suppression Proclamation was enacted. This Proclamation seeks to address the deliberate dissemination of hate speech and disinformation which pose threats to social harmony, political stability, national unity, human dignity, diversity and equality. It covers, inter alia, social media. The proclamation has been widely critiqued as its definition of hate speech 'is quite nebulous and overbroad and may be regarded as illegal under international human rights law'.[175]

In Ghana, the only reference to privacy in the Children's Act 1998 is to children's privacy being respected in the context of family tribunals, and the only reference to children in the Electronic Transactions Act 2008 refers to child pornography, which is outlawed. According to the country report, UNICEF has expressed concerns about gaps in the legal framework, a lack of guidelines and standards and the ineffective implementation of the frameworks and standards that do exist, which means that in effect, children's privacy and exposure online is unregulated. There is no explicit policy on online protection of children, no legislation on mandatory reporting by ISPs, and it is unclear how individuals or organisations are supposed to report breaches of children's rights.[176]

In 2001, Kenya enacted the Children Act. The Act is comprehensive and explicitly includes the right to privacy in section 19 as follows: 'Every child shall have the right to privacy subject to parental guidance'. This mirrors article 10 (Protection of Privacy) in the African Charter on the Rights and Welfare of the Child.

Children's rights are receiving increased attention in Mauritius with the introduction of a new Child Protection Bill that seeks to provide a comprehensive and modern legislative framework to give better effect to the United Nations Convention on the Rights of the Child and the African Charter on the Rights and Welfare of the Child.[177] The current Child Protection Act (CPA) is expected to be repealed. The 2020 Bill, in article 27 provides that 'no person shall do an act which

171 President of the Republic, A Wade, & Prime Minister C Soumar 'Law on cybercrime' (25 January 2008) https://ictpolicyafrica.org (accessed 8 February 2022).

172 Morocco reports no evidence of the existence of a dedicated children's law either.

173 Concluding observations on the combined fourth and fifth periodic reports of Ethiopia (3 June 2015) UN Doc CRC/C/ETH/CO/4-5 (2015) https://www.refworld.org/publisher,CRC,CONCOBSERVATIONS,ETH,566fc30b4,0.html (accessed 8 February 2022).

174 The inclusion of 'without authorisation' is contrary to international law which expressly prohibits child sexual exploitation and abuse or child sexual abuse material: See Convention on the Rights of the Child (n 104), the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (2000), and Committee on the Rights of the Child, General comment 25 (2021) on children's rights in relation to the digital environment, (2021) UN Doc CRC/C/GC/25, dated 2 March 2021 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en (accessed 8 February 2022).

175 Y Ayalew 'Assessing the limitations to freedom of expression on the internet in Ethiopia against the African Charter on Human and Peoples' Rights' (2020) 20 *African Human Rights Law Journal* 315 at 325.

176 Ministry of Gender, Children and Social Protection 'Children's online safety concerns in Ghana: A position paper on legislative and policy gaps' (July 2018) https://www.unicef.org/ghana/media/1806/file/Child%20Online%20Safety%20%20Legislation%20and%20Policy%20Gaps.pdf (accessed 23 April 2021).

177 Child Protection Bill of 2020.

affects the privacy of a child'. It further provides privacy protections against media publication to children who are witnesses, victims, or in conflict with the law, explicitly noting that media includes any print, broadcast, or online media. The Bill further recognises child participation and provides:

> Every child who is of such age, maturity and stage of development as to be able to participate in any matter concerning the child shall, so far as is practicable, have the right to participate in the matter and any views expressed by the child shall be given due consideration.

The Computer Misuse and Cybercrimes Act amends the current Child Protection Act to expand the definition of a photograph to include 'data stored on a computer disc or by other electronic means which is capable of conversion into a photograph'.[178] The Computer Misuse and Cybercrimes Act further expands the provision criminalising indecent photographs of children. In terms of the ICT Act, the ICTA is required to take steps to regulate or curtail the harmful and illegal content on the internet and other information and communication services. The ICTA also has a procedure of content-filtering related to child sexual abuse websites. The ICTA Consumer Guide explains that ICTA has a centralised Online Content Filtering solution to filter access to child sexual abuse sites. The deployment of the filtering system aims to reduce the availability and circulation of child abuse images in Mauritius. In March 2021, the Child Sexual Abuse (CSA) Filtering System, identified 35 246 attempts (hits) to access CSA websites by Mauritian internet users, and 928 Mauritian IPs addresses to which access to CSA websites were blocked. In April 2021, the hits amounted to 32 551 with 1 274 websites blocked.[179]

Again, in Mauritius, the National Computer Board (NCB), functioning under the Ministry of Information and Communication Technologies and part of the Cybersecurity Emergency Response Team (CERT MU) developed a Child Safety Online Action Plan. The main objective of this plan is to develop a plan of action that protects children on the internet. A multi-faceted approach was taken with different policies.[180] Concerns have been expressed about implementation, however.[181] During 2020, a variety of content was published across social media platforms, which appeared to be an attempt to stoke ethnic, racial and religious tensions in Mauritius. According to reports, there were 'growing concerns of interference in Facebook groups, accounts and pages, in addition to a large scale and organized creation of fake profiles seeking to comment with increasingly divisive language'.[182]

In South Africa, POPIA recognises that children are deserving of particular protection when it comes to the processing of their personal data. In terms of sections 34-45, the personal information of a child may not be processed, unless carried out with a competent person's prior consent. It is necessary for a right or obligation in law regarding its establishment, exercise or defence to comply with international law obligations.

The Children's Act 38 of 2005 is undergoing amendments to reflect the privacy and data protection rights of children. Specifically, section 6A provides:

> A child's right to privacy and the protection of personal information is subject to the Films and Publications Act, 1996 (Act No. 65 of 1996), the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), the Promotion of Access to Information Act, 2010 (Act No. 2 of 2010), the Criminal Procedure Act, 1977 (Act No. 51 of 1977), or any other law protecting the

178 The Mauritius Computer Misuse and Cybercrime Act, 2003.

179 ICTA 'Child Sexual Abuse (CSA) Online Filtering System' https://www.icta.mu/csa-filtering/ (accessed 8 February 2022).

180 International Telecommunication Union 'First meeting of the Council Working Group on Child Online Protection (CWG-CP)' 17-18 March 2010 https://www.itu.int/council/groups/wg-cop/first-meeting-march-2010/Contribution%20on%20Child%20Safety%20Online%20Activities%20in%20Mauritius%2011%2003%2010.docx (accessed 10 February 2022).

181 ECPAT 'Country overview: A report on the scale, scope and context of the sexual exploitation of children in Mauritius' (June 2019) https://www.ecpat.org/wp-content/uploads/2019/06/Mauritius-ECPAT-Country-Overview-Mauritius-July-2019.pdf (accessed 9 February 2022).

182 N Dehnarain 'Trouble in paradise: Facebook spread of hate speech as Mauritius oil spill crisis continues' *Forbes* 20 September 2020 https://www.forbes.com/sites/nishandegnarain/2020/09/20/trouble-in-paradise-facebook-spread-of-hate-speech-as-mauritius-oil-spill-crisis-continues/?sh=58811af927a5 (accessed 9 February 2022).

privacy and protection of personal information of the child.

The Film and Publication Board (FPB) established in terms of the Films and Publications Act 65 of 1996 makes use of certain mechanisms to deal with issues of child sexual abuse materials. The FPB regulates the content of films, games and certain publications through classification, and seeks to balance the right to freedom of expression with an obligation to protect children from exposure to potentially disturbing, harmful and inappropriate materials. Additionally, the FPB seeks to protect children from sexual exploitation in media content.[183]

In December 2020, the South African Department of Home Affairs (DHA) published the Official Identity Management Policy for public comment. Concerns, particularly relating to children were raised, by the Right2Know Campaign (R2K). In its submissions, R2K suggested that more research is needed for understanding the use of biometrics on children and submitted that the DHA ought to reconsider its position on the collection of biometric data of children and at a minimum conduct a Children's Rights Impact Assessment.[184]

The South Africa report alludes to the fact that in 2019 the South African Law Reform Commission (SALRC) released a Discussion Paper on Sexual Offences (Pornography and Children) and an accompanying Bill. The Discussion Paper reviews the legislative framework that currently applies to children in respect of pornography and child sexual abuse material within the larger framework of all statutory and common law sexual offences. The discussion document references the Sexual Offence Amendment Act and the Film and Publications Act as the current law applicable to the exposure of children to pornography in South Africa. The report suggests that it appears there has not been much movement on this since the call for comment in July 2019.[185]

In Tunisia, Law 95-92 of 9 November 1995 relating to the publication of the child protection code addresses children's right to privacy in a number of articles. Article 6 states that every child has the right to respect for his private life, while considering the rights and responsibilities of their parents or those who are in charge, in accordance with the law. The code also states the obligation to protect this right in the judicial process – articles 88, 97 and 98 – and implies sanctions in cases of non-respect of these provisions – article 120 and 121.[186]

The north of Nigeria has a serious problem with terrorism, notably in the form of Boko Haram which uses the abduction of children as a method of recruitment. The Nigeria report notes that a national action plan for preventing violent extremism (PVE) was developed in 2017 in consultation with civil society organisations, the media, students, and the academic community, and implemented in 2020. The report does not detail if online radicalisation is a phenomenon.

Similarly, the Ethiopia report notes that while violent ethnic extremism and terrorism remain a primary concern in Ethiopia, there is limited available research regarding responses to the online radicalisation of children through digital media.[187] The Proclamation requires social media services to endeavour to suppress and prevent the dissemination of disinformation and hate speech through its platform and act within 24 hours to remove or take out of circulation disinformation or hate speech upon receiving notifications about such communication or post. Social media enterprises are also required to have policies and procedures which reflect these duties. Ethiopia reports[188] concerns

183 Film and Publication Board https://www.fpb.org.za/ (accessed 7 February 2022).

184 Right2Know Campaign 'Submission to the Director-General of the Department of Home Affairs on the Draft Official Identity Management Policy' (2020).

185 South African Law Reform Commission 'Sexual Offences (Pornography and Children) Discussion Paper 149' (April 2019) https://www.ellipsis.co.za/wp-content/uploads/2015/11/dp149-prj107-SexualOffences-PornographyChildren2019.pdf (accessed 9 February 2022); Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007.

186 The Code for the Protection of Children.

187 Y Adeto 'Violent ethnic extremism in Ethiopia: Implications for the stability of the Horn of Africa' (2020) 2 *AJCR*, see also Y Adeto 'Preventing violent extremism in the Horn: The case of ethnic extremism in Ethiopia' (2019) *Policy Paper: European Institute of Peace*.

188 'The government' *Article 19* 19 January 2021 https://www.article19.org/resources/ethiopia-hate-speech-and-disinformation-law-must-not-be-used-to-supress-the-criticism-of-the-government/ (accessed 8 February 2022).

with these provisions noting that the takedown period is 'alarmingly short and present a host of due process concerns', the provision is vague and does not explain who may provide such a 'notice' or the process for providing it, and there is no requirement for notifying a user of a takedown of their content, and no opportunity for judicial oversight or review by a similar independent adjudicatory authority. There are also no appeals mechanisms described.

Cameroon also reports that both Boko Haram and ISIS are active in the North and are experiencing the Anglophone crises on the North and South West regions of the country. One of the aims of the 2010 law on Cybercrime and Cyberterrorism was to prevent the promotion of terrorism, but the terms of the law mean that it partially criminalises free speech online and has even been used to imprison journalists critical of the government rather than tackling genuine extremism.[189] 'Hate speech' is criminalised by the Hate Speech Law of 2019, with higher penalties applied in the case of hate speech that is tribe-based or spread via media. However, as with the law on cyberterrorism, it is not applied equitably but is often misused as a pro-government instrument.[190] There is no legislation covering end-to-end encryption in the case of children's use of the internet. However, the government of Cameroon has targeted WhatsApp as a method of combatting Anglophone protests.[191]

In Morocco, the antiterrorism law, adopted in 2003, gives the government sweeping powers to filter and delete content that is deemed to 'disrupt public order by intimidation, force, violence, fear, or terror'.[192] The Code of the Press and Publishing (Law 88 of 13) which has been in force since 2016 evokes special provisions related to children. Article 64 of the code prohibits in the print and electronic press any publicity attacking and denigrating of children, or conveying a message likely to prejudice the person of the minor, lead to his misappropriation, affect him or make the propaganda of discrimination against children on the basis of gender. The same article also prohibits any publicity 'inciting to hatred, terrorism' or containing attacks and denigration people based on religion, sex, colour or disability; or conveying a message likely to perpetuate stereotypes of inferiority and sexist discrimination against women.

In Tunisia, the Organic Act 26 of 2015 Relating to the Fight Against Terrorism and the Suppression of Money Laundering provides in article 34 that

> whoever deliberately commits any of the following acts […] providing, by any means whatsoever, weapons, explosives, ammunition or other materials or equipment or means of transport or equipment or ammunition for the benefit of a terrorist organization or agreement or persons in connection with terrorist offenses provided for by this law [is guilty of a terrorist attack].

The use of digital means is considered 'other material or equipment'. The recruitment of terrorists is punishable regardless of the means used such as an invitation email, announcements or instructions on social media pages or through sites devoted to such recruitment. Harsher sanctions apply if a crime used children.[193]

Zimbabwe has an impressive constitutional array of protections for children, and a 2001 Child Law. However, despite mounting and progressive children's rights jurisprudence, there has not yet been any case specifically on children's rights to privacy.

6 Judicial protection of online privacy

In 2017, the High Court of Tanzania was presented with the opportunity to ventilate the applicability and scope of the right to privacy, however, it did not do so. In the matter of Jamii Media Company Ltd v

189 K Ndongmo 'Cameroon digital rights landscape report' in T Roberts (ed) *Digital rights in closing civic space: Lessons from ten African countries* (2021) 236

190 Ndongmo (n 128) 244.

191 'Facebook and WhatsApp restricted in Cameroon on eve of election results' *Netblocks* 21 October 2018 https://netblocks.org/reports/facebook-and-whatsapp-restricted-in-cameroon-on-eve-of-election-results-YkArL1yj (accessed 20 April 2021).

192 Freedom House 'Freedom on the net 2021 Morocco' (2021) https://freedomhouse.org/country/morocco/freedom-net/2021 (accessed 8 February 2022).

193 The Organic Act 26 of 2015 relating to the Fight Against Terrorism and the Suppression of Money Laundering (7 August 2015) https://www.bct.gov.tn/bct/siteprod/documents/Loi_2015_26_fr.pdf (accessed 8 February 2022).

The Attorney General,[194] the petitioner, Jamii Media Company Ltd, operated a website that allowed users to anonymously post their social, economic, or political views. Following specific posts shared on the site, the Tanzanian police, invoking section 32 of the Cybercrimes Act, issued so-called 'disclosure orders' demanding the site's operators to disclose information about users. Jamii then instituted proceedings challenging the constitutionality of sections 32 and 38 of the Act in so far as it infringes the right to privacy and the right to be heard. However, the court did not address privacy issues.

Whilst there has been some jurisprudence relating to the constitutional right to privacy in Uganda, it is not relevant to the issues under discussion. Despite English common law applying in Nigeria, it has no overarching right of privacy. Due to this the principle of information privacy is found in the existence of torts such as breach of confidence.[195]

In Cameroon, the case of the People of Cameroon v Ekume Otte Sakwe tested the effectiveness of the Cybersecurity and Cybercrime Law 2010. Sakwe was charged with the publication of unverified information about three private companies. The case against Sakwe failed for lack of concrete evidence. Other cases brought under the act have also failed for lack of evidence.

In the Egypt report, the well-known 'TikTok' teenager case is discussed. Menna Abdel Aziz, 17, an Egyptian teenager appeared online on the TikTok platform with a swollen and bruised face to expose how she was sexually assaulted. After her video went viral, she was arrested, investigated in the absence of her lawyer and charged with several charges like 'inciting immorality', 'violating Egyptian family values' and 'forgery of an electronic account'. Her attackers were also arrested. In addition to assault charges, they faced charges on violating the sanctity of private life by posting private content online. Abdel Aziz was then placed for pre-trial detention for 114 days in one of the hosting centres specified in the 'Ministry of Social Solidarity' as one of the measures stipulated in article 201 of the Criminal Procedure Law as an alternative to preventive detention. She was then released upon the prosecution's decision that there are no grounds in bringing a case in Case 3328 of 2020 for the charges against her.[196]

In another Egyptian case, a court convicted in case 350 of 2015, four Coptic Christian teenagers for contempt of Islam, after they appeared in a video imitating Islamic prayer and mocking practices of the Islamic State, sentencing them three to five years in prison and referring a fourth to a juvenile detention facility.[197]

In Kenya, courts have considered the right to privacy. The two seminal privacy rights cases in Kenya are Okoiti v Communications Authority of Kenya and Kenyan Human Rights Commission v Communications Authority of Kenya.[198] Both cases stem from a similar set of facts, with different parties, the first being the Director of Kenyans for Justice and Development Trust and the second the Kenya Human Rights Commission, instituting proceedings against the Communications Authority of Kenya. In these two matters mentioned, the High Court of Kenya ruled that a government surveillance system violated the right to privacy and, accordingly, was unconstitutional.[199] The government, through Communications Authority of Kenya (CAR), intended to intercept the data of mobile phone subscribers using a system called Device Management System (DMS) to monitor and identify stolen phones and counterfeit phones, as

194 *Jamii Media Company Ltd v The Attorney General* (2017) TLS LR 447.

195 IS Nwankwo 'Information privacy in Nigeria' in AB Makulilo (ed) *African data privacy laws* (2016) 61-62.

196 'After Menna Abdel Aziz's release and the prosecution's decision that there are no grounds in bringing a case for the charges against her, EIPR calls on the prosecution to take the same approach in similar cases to protect victims of sexual violence' *Egyptian Initiative for Personal Rights* September 2020 https://eipr.org/en/press/2020/09/after-menna-abdel-aziz%E2%80%99s-release-and-prosecutions-decision-there-are-no-grounds (accessed 9 February 2020).

197 'EIPR condemns five-year prison sentence for children on blasphemy charges: 12 defendants convicted in 9 cases since January 2015; 11 cases pending before courts and more cases pending before disciplinary bodies' *Egyptian Initiative for Personal Rights* September 2020 https://eipr.org/en/press/2016/02/eipr-condemns-five-year-prison-sentence-children-blasphemy-charges-12-defendants (accessed 25 February 2016).

198 *Kenya, Okoiti v Communications Authority of Kenya* [2017] eKLR; *Kenya Human Rights Commission v Communications Authority of Kenya* 86 of 2017 (19 April 2018).

199 As above.

well as devices that had not been approved by the regulator. No clarity was issued on the measures which the government would take to protect the subscribers right to privacy.

The judgments provide a useful assessment of what the right entails, which is that every person 'should have control over his or her personal information and should be able to conduct his or her own personal affairs relatively free from unwanted intrusions'. It enables other rights such as freedom of expression and information and association. Further, the right creates a positive obligation on the state to implement the appropriate measures to safeguard the right. The right to privacy is not absolute which is a fact recognised in regards to other constitutional rights as well. Activities which restrict privacy rights are justifiable if they are prescribed by the law, have a legitimate purpose, and the restriction aligns with its purpose. In this case, the Court highlighted that there were less restrictive means to achieve the purpose. The Court did not distinguish between the right to privacy on- and offline despite these matters being squarely related to the contravention of digital privacy rights.[200]

The Kenya report adds that more recently, the Kenyan High Court was tasked with considering the implications of the National Integrated Identity Management Scheme (NIIMS) – a biometric database. NIIMS was introduced as an amendment in the Miscellaneous Amendments Act of 2018. Following a challenge by civil society organisations, the High Court found, among other things that the provision for collection of Deoxyribonucleic Acid (DNA) and Global Positioning System (GPS) coordinates in the impugned amendments, without specific legislation detailing out the appropriate safeguards and procedures in the said collection, and the manner and extent that the right to privacy will be limited in this regard is not justifiable.

The Kenya report also notes that there has been helpful commentary on the judgment, particularly by Privacy International, who provided expert witness testimony in the matter. Privacy International welcomed the judgment, in particularly the acknowledgement of the need for strong legal protections. The matter has been appealed to the Supreme Court, as such, the matter is yet to receive final determination.[201]

In Mauritius, constitutional privacy protections were tested in Madhewoo v the State of Mauritius in 2016.[202] The Supreme Court of Mauritius was tasked with determining whether the National Identity Card (Miscellaneous Provisions) Act of 2013 and Regulations violated, among others, the right to privacy. Mr Madhewoo, the plaintiff, argued that the new smart ID card project envisaged by the legislation infringed his privacy rights. The Supreme Court confirmed that section 9(1) was not an absolute right and interference with that right could be permitted under section 9(2) and concluded that the Regulations were made in the interests of public order under section 9(2)(a). Academics in response to the judgment explain that ultimately this case highlighted that there is 'no constitutionally-protected right to general privacy' in Mauritius, only the rights expressly provided for in the Constitution.[203]

A child's privacy rights came to the fore in a recent case in South Africa, SM v ABB.[204] The father of the child had circulated strings of content from her WhatsApp chatroom (as also that of her mother) in the course of an acrimonious divorce case. Confirmation of an ex parte application for an interim interdict to prevent him further accessing and disseminating both the applicant's (the child's mother) emails and WhatsApp messages, and those of his minor child was sought. The Court found that the behaviour of respondent in accessing the applicant's and the minor child's messages was an infringement of their right to privacy:

200 *Okoiti v Communications Authority of Kenya* (n 137).

201 Privacy International 'Kenyan Court Ruling on Huduma Namba Identity System: The good, the bad and the lessons' (24 February 2020) https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons#:~:text=Lessons%20%7C%20Privacy%20International-,Kenyan%20Court%20Ruling%20on%20Huduma%20Namba%20Identity%20System%3A%20the%20Good,the%20Bad%20and%20the%20Lessons&text=Kenya%20High%20Court%20fails%20to,to%20equality%20and%20non%2Ddiscrimination (accessed 9 February 2022).

202 *Madhewoo v the State of Mauritius* [2016] UKPC 30.

203 Madhewoo (n 141) 204.

204 *SM v ABB* case 20/1732 (11 September 2020, Gauteng Local division).

> the dissemination of the information to the Headmaster and the medical practitioner was done for no other reason than to try and engender a cognitive bias in the minds of those persons against the Applicant and possibly also the minor child.

By disseminating messages between the applicant and the minor child, not only was the applicant's right to privacy violated, but so too was that of the child. The case indicates that parental rights to access their child's digital communications without good reason can be limited.

Also, in South Africa, the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) intends to regulate the interception and monitoring of communications, including the application and issuing of directions authorising the interception of communications. But multiple provisions of RICA have recently been struck down as unconstitutional by South Africa's Constitutional Court.[205] The Constitutional Court found that RICA is unconstitutional in five important respects because it did not provide sufficient safeguards to protect the privacy of citizens. It also confirmed that bulk surveillance is unlawful in South Africa. This case was premised primarily on alleged violations of the right to privacy after it was divulged that a prominent journalist had been placed under surveillance. Interestingly, an NGO, Media Monitoring Africa (MMA) intervened as amicus curiae to advance arguments around the need to ensure specific child-sensitive remedies to ensure that children's best interests are protected and promoted in the context of the surveillance, which RICA does not expressly prohibit. Acknowledging that children in society require special protection, MMA argued that before any surveillance order can be granted, a designated judge responsible for the granting of such orders must be informed that the subject of the surveillance order is a child, or may implicate a child, and must ensure that a series of appropriate safeguards have been complied with before a surveillance order can be granted. The Court did not comment directly on these arguments.[206]

In 2020, a young girl in South Africa received anonymous threats of gang rape and murder over Instagram. In an attempt to obtain information about the perpetrator to protect herself, the young girl and her family became caught up 'in an inter-continental administrative quagmire to compel Facebook Inc to disclose the identity of the holder/s of several Instagram accounts used to make the threats'. Facebook refused to disclose the identity, and the South African office of Facebook refused to accept the service of legal papers, forcing the girl and her family to find lawyers in the United States to serve papers on the California office. The legal representatives have approached the High Court, and it appears that the matter has been set down for 11 August 2021, subject to settlement discussions.[207] update

In Tunisia, a family judge can also order the Technical Telecommunication Agency (ATT) to delete the harmful content in respect of a child distributed online. According to the Decree 4506 of 2013, relating to the creation of the Technical Agency telecommunications and fixing its administrative, financial organization and the modalities of its operation, the ATT's mandate compels it to coordinate with telecommunications network operators and internet service providers in relation to its work so as to provide technical support for judicial investigations.[208] On 26 May 2011, the Tunis Court of First Instance ordered the Tunisian Internet Agency (ATI) to block pornographic websites in response to a complaint from lawyers making the argument that these sites were a threat to minors and the country's Muslim values. The ATI pledged to oppose the blocking order, but its appeal was rejected in August 2011, prompting the agency to take the case to the highest appeal court. On 22 February 2012, the Court of Cassation overturned the Court of Appeal decision. The justification in support of the appeal was that the ATI lacked

205 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC* 2021 (3) SA 246 (CC).

206 As above.

207 T Broughton 'Joburg teen sues Facebook for name of Insta stalker who threatened rape & murder' *Times Live* 27 July 2020 https://www.timeslive.co.za/news/south-africa/2020-07-27-joburg-teen-sues-facebook-for-name-of-insta-stalker-who-threatened-rape-murder/ (accessed 9 February 2022).

208 Decree 4506 of 2013, relating to the creation of the Technical Agency telecommunications and fixing its administrative, financial organisation and the modalities of its operation http://www.intt.tn/upload/txts/fr/d%C3%A9cret2013_4506fr.pdf (accessed 9 February 2022).

the technical capacity to implement the filtering system mandated by the blocking order.[209] Also in Tunisia, a case that drove attention to digital games' impact on children was the Blue Whale challenge. In March 2018, the Court of First Instance in Sousse ordered ATI to block online access to the Blue Whale and Meriam games, which, the court claimed, encourage teenagers to commit suicide. This case was presented in court by an association of parents and with the support of the delegate of children protection in Sousse.[210] This case raised questions about the legal basis of the decision and what to do in the case of decentralised games. In 2019, the Ministry of Interior warned parents of a similar game on other mobile applications.[211]

7 Consent

In relation to media and digital environments, theories of child development have historically guided age-based restrictions on children's media access (in relation to advertising, or sexual and violent content, for instance). However, the evidence base informing decisions on age-based restrictions to use digital services or applications is largely unclear or out of date.[212]

Little is known about children's online consent in Tanzania and Uganda. In Nigeria, the NDPR Implementation Framework classes a 'child' as under 13 for the purposes of internet services. This is line with the US Children's Online Protection Act, which is written into the membership policies of most social media platforms. There are no restrictions on what images or materials parents may share of their children.[213] In Ethiopia, there are no privacy laws or child-friendly policies that consider the varying evolving limitations of what images or material parents may share of their children online. So too, in Burkina Faso, the existing legal framework does not elaborate on child consent related to privacy or online matters.[214] In Cameroon, consent is a prerequisite in several laws relating to the collection and processing of personal data such as the Cybersecurity and Cyberterrorism Law 2010 and Law 2010/021 on electronic commerce, but there is nothing specifically about children in the legislation. Privacy laws do not consider the evolving capabilities of children, making no distinction except between minors and adults, and there are no restrictions on what images or material parents may share about their children.[215] In Egypt, whenever the data concerns a child, the Data Protection law requires the legal guardian's consent (article 12 of the Data Protection Law). The consent needs to be in a written form.[216]

The Data Protection Act of 2019 of Kenya (DPA) has fairly comprehensive provisions relating to children.[217] Section 33 provides that the data controller cannot process personal data relating to children unless consent is given by the child's parent or guardian and the processing is in such a manner that protects and advances the rights and best interests of the child. The DPA further requires a data controller or data processor to incorporate

209 Refworld 'Freedom on the Net 2012 - Tunisia' (25 September 2012) https://www.refworld.org/docid/5062e897c.html (accessed 9 February 2022).

210 DB Youssef 'Is censorship coming back to Tunisia? Court order bans "Blue Whale" online game' *Advox: Global Voices* 14 March 2018 https://advox.globalvoices.org/2018/03/14/is-censorship-coming-back-to-tunisia-court-order-bans-blue-whale-online-game/ (accessed 9 February 2022).

211 As above.

212 U Kilkelly & T Liefaard *International human rights of children* (2019) 490. They continue that the 'EU General Data Protection Regulation (GPDR), which will restrict the processing of children's personal data by providers of online information services without parental permission under the age of 16 (unless Member States decide to reduce this to 13 years old by 2018). As laws and policies restricting children's access to certain types of media content depending on their specific age may have a significant impact on children's exercise of their right to freedom of expression and freedom of association, the imposition of age limits should be justified, evidence-based, and rooted in scientific theory'.

213 UK Safer Internet Centre 'Age restrictions on social media services' (25 April 2018) https://www.saferinternet.org.uk/blog/age-restrictions-social-media-services (accessed 21 April 2021).

214 The Criminal Code secs 533 and 534.

215 Moukouri (n 36).

216 Personal Data Protection Law, art 12. Although this is not clarified in the report, presumably this means all children aged under 18 years.

217 The Data Protection Act 24 of 2019.

appropriate mechanisms for age verification and consent in order to process the personal data of a child. Appropriate mechanisms are to be determined on the basis of available technology; the volume of personal data processed; the proportion of such personal data likely to be that of a child; and the possibility of harm to a child arising out of the processing of personal data. Interestingly, the DPA provides that a data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent. In addition to section 33, the DPA categorises the names of a person's children as 'sensitive personal data'.

The Data Protection (General) Regulations of 2021 contain further child-sensitive provisions. Section 12 places a duty on data controllers/processors to take extra steps when processing a child's personal data – the person exercising a right on behalf of the child is appropriately identified, profiling a child that is related to direct marketing is prohibited, and the parent or guardian must be informed of the inherent risks of processing and the safeguards which have been put in place. Section 22 stipulates that data controllers/processors must develop a policy on their data handling practices, which includes a section on the collection of personal data from children and other vulnerable segments of the community.

Apart from data protection, Kenya considers children's privacy rights and online protection in several other ways. The National Children Policy acknowledges that the potential harm which can be caused to children through digital technology and the need to institute legislation on internet use by children, particularly in respect to pornographic material, uncontrolled media, and 'other criminal related exposures'. The National Plan of Action for Children in Kenya 2015 to 2022 does not unequivocally declare that children have the right to privacy. However, and similar to the National Children Policy, the Plan of Action focuses on the 'new forms of abuse' children are exposed to as a result of ICTs. It also concedes that there are inadequate measures to prevent and respond to this nature of child abuse.

In Ghana, anyone whose rights have been violated has the right to complain to the Data Protection Commission. The Child Rights Act of 1998, only requires consent from children in the case of adoption. The are no rules as to what images and information parents may share online about their children.

In the DRC, too, there are no limitations on what images or information parents may share about their children and there are no privacy laws considering the evolving capacities of children.[218]

In Mauritius, section 30 of the Data Protection Act, as already quoted earlier, in this report, regulates children's consent. In Benin, the new Digital Code guarantees consent as a principle prior to the recognition of the legitimacy of any processing of personal data, exception in certain derogatory conditions provided. It establishes the consent of the child as a person under the age of 16 in some cases, and at least 16 years old in others cases. Parental involvement is required when the child is under 16 years old.

Thus, article 446 states,

> with regard to the direct offer of information society services to minors, the processing of personal data relating to a minor is lawful when the minor is at least sixteen (16) years old. When the minor is under sixteen (16) years of age, this processing is only lawful if, and insofar as, the consent is given or authorized by the holder of parental responsibility with regard to the minor. The controller makes reasonable efforts to verify, in such a case, that consent is given or authorized by the holder of parental responsibility for the child, given the technological means available.[219]

In January 2014, the CNDP (data protection authority, the Commission nationale de contrôle de la protection des données à caractère personnel) in Morocco launched its first control operation to verify the compliance with the law of Moroccan websites and online businesses, including online shopping websites, with the provisions of Act 09-08 on the protection of personal information. In January 2016, CNDP issued recommendations regarding unsolicited electronic marketing. It called for the creation of a national opt-out list in

218 DP Zongwe, F Butedi & PM Clément 'Update: Overview of the legal system of the Democratic Republic of the Congo (DRC) and research' New York University School of Law (July/August 2020) https://www.nyulawglobal.org/globalex/Democratic_Republic_Congo1.html (accessed 15 April 2021).

219 Digital Code, art 446.

which consumers would register to stop receiving commercial marketing messages.[220]

In Senegal, while parent's representation is expressively required in certain conditions such as eCommerce transactions, privacy-related laws do not address child's consent, and there are no limitations of what images or material parents may share of their children online.[221]

In South Africa, MMA's recent submissions to the Portfolio Committee recommend the following wording to be included in the Children's Amendment Act, currently under debate:

> Where the personal information of a child is collected, the child must be informed about how the data is collected and used. Information on the processing of personal information shall be provided in a simple, clear and accessible manner, considering the evolving capacities of children, to ensure that a child will be able to understand what will happen to their personal data.
>
> Any person or entity processing the personal information of children must adopt privacy policies for such purposes. Such policies must be user-friendly and accessible for parents and caregivers with diverse digital literacy and literacy skills. All privacy policies must be accompanied by child-friendly versions, considering the evolving capacities of children, and must be drafted in a manner that enables a child to make informed decisions about their personal data.

Apart from this, and the provisions of POPIA discussed elsewhere I this report, above there are no specific measures in place that address terms and conditions.

Over the past year, there has been a rise in media attention surrounding 'sharenting' in South Africa, with different journalists and experts providing various tips and tricks for parents who are inclined to share the content of their children online.[222]

In Zimbabwe, the Freedom of Information Bill was introduced in 2019. This Bill seeks to repeal the Access to Information and Protection of Privacy Act, and give effect to the constitutionally protected rights to access information and freedom of expression. This Bill requires appeals in relation to access to information requests to go through the Zimbabwe Media Commission. Reports on access to information request are also set through the Zimbabwe Media Commission. There are some provisions in the Bill relevant to children. The first key reference is in relation to data protection. The processing of personal information of children is subject to the consent of a competent person. Section 26 provides 'where the data subject is a child, his or her rights pursuant to this law may be exercised by his or her parents or legal guardian'. The second notable references to children are found under Part XII of the Bill, under consequential amendments and Part III under offence against children and procedural law, providing a definition of a child as a person below 18 and amending (expanding) the definition of child pornography.[223]

However, the Zimbabwe report records that

> it is likely that the Bill does not sufficiently safeguard the rights of children. The provisions relating to data subjects do not sufficiently acknowledge that children are deserving of particular protection when it comes to the processing of their personal data, nor do they give effect to the principle of the best interests of the child by requiring that the processing of personal data of children must protect and advance their rights and best interests. In addition, the personal information relating to children is not defined as sensitive data in the Bill and accordingly the processing of such information is not prohibited, nor is it protected by additional safeguards, save for where their parents or caregivers may exercise certain rights.[224]

220 Privacy International 'State of Privacy Morocco' (26 January 2019) https://privacyinternational.org/state-privacy/1007/state-privacy-morocco (accessed 9 February 2022).

221 Personal Data Protection Act, art 4.4.

222 See for example P Gabriel 'Why you should be careful about posting pictures of your child on social media' *Daily Maverick* 12 March 2020 https://www.dailymaverick.co.za/opinionista/2020-03-12-why-you-should-be-careful-about-posting-pictures-of-your-child-on-social-media/ (accessed 9 February 2022); 'The downside of sharenting' *eNCA* 8 April 2019 https://www.enca.com/life/downside-sharenting (accessed 9 February 2022), and 'You really shouldn't be posting pictures of your kids online' *The Daily Vox* 23 February 2021 https://www.thedailyvox.co.za/you-really-shouldnt-be-posting-pictures-of-your-kids-online/ (accessed 9 February 2022).

223 Freedom of Information Bill HB 6, 2019.

224 As above.

8 Other initiatives

Although Burkina Faso is yet to ratify the African Union Convention on Cyber Security and Personal Data, the country has set a National Cyber Security Strategy 2019-2023 which cites this Convention as a benchmark, and whose pillars at the national level include national laws on the protection of personal data, on the regulation of electronic services and transactions, on general regulation of electronic communications networks and services.[225] There are no explicit safeguards on filtering and monitoring, no mechanisms to avoid child profiling as in relation to membership of specific groups such as extremist groups. However, the CIL has set a whole programme to instruct youth on the risks of using the internet and social networks inappropriately.[226]

In Egypt, the National Child Online Protection Committee was re-established in June 2013 with a Ministerial Decree 257. It is a multi-stakeholder's committee. One of its objectives is setting a national strategy for raising awareness of Children Internet Safety.[227] Also in Egypt, the Law 180 of 2018 Regulating the Press and Media authorises the Supreme Media Council to suspend or block any personal website, blog, or social media account that has over 5 000 followers if its publications incite the violation of a specific law or violate public order and public morals, or incite discrimination, violence, racism, hatred or intolerance or insulting the monotheistic religions or religious beliefs. In 2018, the Supreme Council for Media Regulation, formed a committee called 'Daily Follow-up Committee for Social Networking Sites', a committee responsible for the daily follow-up of the social networking pages of various social sectors, including youth and adults, in order to identify daily the changes and developments in the prevailing ideas on these pages.[228]

In Kenya, in 2020, the Ministry of Education, in partnership with the Terre des Hommes Netherlands, ChildLine Kenya, and the African Institute for Children Studies recognised the need to advance safety online for children, and launched, with the approval from the Kenya Institute of Curriculum Development a children and facilitators manuals for training on online safety and security. Notably, the National Plan of Action for Children in Kenya 2015 to 2022 takes cognisance of the new forms of abuses which ICTs have exposed children to and, in this regard, gives examples of harmful material, cybercrimes, child trafficking and kidnapping. Further, the Plan of Action concedes that Kenya still has some way to go as law enforcement is not adequately responsive to new harms.[229] The establishment of the National Kenya Computer Incident Response Team – Coordination Centre (KE-CIRT/CC) enables the Communications Authority of Kenya to investigate cybercrimes, including those perpetrated against children. In a bid to raise awareness, a campaign called 'Child Online Protection Campaign' has been used as a means to raise awareness on online abuse against children and how to prevent it. Prosecutions may be brought in terms of the Data Protection Act, the Computer Misuse and Cybercrimes Act, as well as the Kenya Information and Communications Act.

At the advocacy level, the wife of Malawian deputy president has recently been appointed to champion online protection of girls from harassment.[230] While there does not appear to be adequate protection for children's privacy rights or protection of their personal information, there have been notable efforts to advance children's online safety in Malawi recent years. In 2017, Malawi Communication Regulatory Authority entered into a partnership with the International Telecommunications Union (ITU) to develop Malawi's national Child Online

225 Burkina Faso Stratégie nationale de cyber sécurité 2019-2023 (SNCS-BF).

226 CIL 'Youth & digital' http://www.cil.bf/index.php/jeunesse-numerique (accessed 9 February 2022).

227 Arab Republic of Egypt https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Documents/Presentation%20for%20Uganda%20.pdf (accessed 9 February 2022).

228 'Social Media Follow-Up Committee' http://scm.gov.eg/%D9%84%D8%AC%D9%86%D8%A9-%D9%85%D8%AA%D8%A7%D8%A8%D8%B9%D8%A9-%D9%85%D9%88%D8%A7%D9%82%D8%B9-%D8%A7%D9%84%D8%AA%D9%88%D8%A7%D8%B5%D9%84-%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%89/ (accessed 9 February 2022).

229 National Plan of Action for Children in Kenya 2015-2022, at 30.

230 J Moyo 'Mary Chilima appointed ambassador against girls' online harassment' *Nyasa Times* 6 October 2020 https://www.nyasatimes.com/mary-chilima-appointed-ambassador-against-girls-online-harassment-plan-malawi/ (accessed 2021).

Protection (COP) framework. In 2018, Malawi, in collaboration with Internet Watch Foundation (IWF) launched a public reporting system that enables Malawians to anonymously report child sexual abuse imagery. Towards the end of 2020, Malawian Minister of Information Gospel Kadzako announced his intention to amend the Communications Act as a means to enhance the protection of children from cyberbullying. [231]

In order to raise awareness of the danger of misuse of the internet, to strengthen protection mechanisms and to promote coordination between all actors, the 'E-salama' programme has been launched in Morocco. It includes revitalising the debate around this issue and building the capacity of actors who must respond to it.[232] The reporting of cases of child abuse online can be done through a helpline or the National Observatory of Child Rights website. The National observatory of childhood has set up the National Centre for Listening, Reporting and Protection of Children Victims of Violence, Exploitation and Abandonment.[233]

In 2018, Mozambique joined the growing list of countries that relies on the IWF system for reporting child sexual abuse content. It appears that IWF is working with INCM on this initiative.

In Tanzania, the Cybercrimes Act enacted to criminalise offences related to computer systems and information communication technologies does not explicitly provide for the right to privacy, whilst the National Information and Communications Technology Policy of 2016 issued by the Ministry of Work, Transport and Communication, recognises the need for improvements in the privacy protection landscape in Tanzania.[234] Tanzania similarly to other countries on the continent has partnered with the IWF to develop a reporting portal for child sexual abuse images. The portal, which has been accessible since 2017, seeks to help protect victims and survivors of child sexual abuse. Further to this, UNICEF has provided funding to strengthen child protection work in Tanzania by establishing and supporting the national Child Online Safety Task Force, which seeks to enhance the capacity of frontline service providers in responding to cases of online exploitation.[235]

In Senegal, Reinforcing Children Protection Online is one of the main priorities in the national digital strategy's action plan, and aims to set a 'Protection mechanism for children online'. The government validated a 'National Plan for the Protection of Children on the Internet' since February 2018, in partnership with its Child Protection Support Unit and UNICEF. However, information on the implementation and monitoring of said plan has not made public to date.[236] The Commission for the Protection of Personal Data (CDP) has placed general information on its website. This platform develops available and accessible child-friendly information to educate on a safe use of the internet to in order to prevent from harm and guarantee personal data protection. The site explains in simple terms the practices such as grooming, made by malevolent adults who use social networks, discussion forums, gaming sites, to contact a child in order to obtain sexual acts (via webcam for example) or to meet offline to abuse him sexually. It also explains phishing and psychological hacking. The site also has a pictorial educational sheet, giving practical advice for safe and responsible use of the internet.[237]

231 'Malawi government planning to amend laws to tackle cyber bullying' *DigWatch* 24 December 2020 https://dig.watch/updates/malawi-government-planning-amend-laws-tackle-cyber-bullying (accessed 9 February 2022).

232 D Oussama, M Tridane & S Belaaouad 'Bibliographic study on child protection software for the internet' (August 2018) https://www.researchgate.net/publication/346042166_Bibliographic_Study_on_Child_Protection_Software_for_the_Internet (accessed 9 February 2022).

233 National Observatory of Child Rights https://2511.ma/ (accessed 9 February 2022).

234 National Information and Communications Technology Policy, 2016.

235 End-violence Against Children 'UNICEF Tanzania: Preventing and responding to online child sexual exploitation and abuse' (March 2018) https://www.end-violence.org/grants/unicef-tanzania (accessed 9 February 2022).

236 Stratégie nationale 'Sénégal Numérique 2016-2025'; Plan d'actions actualisé Actualisation de la stratégie Sénégal numérique 2025 (SN2025) https://tinyurl.com/2hvs64c (accessed 9 February 2022); République du Sénégal 'Validation of a National Plan for the Protection of Children on the Internet' (*Cellule d'Appui à la protection de l'Enfance*) 28 February 2018 https://tinyurl.com/3ruze8xe (accessed 9 February 2022).

237 Le grooming, une nouvelle dérive (7 April 2021) https://www.cdp.sn/content/le-grooming-une-nouvelle-dérive (accessed 9 February 2022); COP Piratage psychologique (ingénierie sociale), ne te laisse pas berner ! (28 April 2021) https://www.cdp.sn/content/piratage-psychologique-ingénierie-sociale-ne-te-laisse-pas-berner (accessed 9

In April 2021, 15-year-old Lufuno Mavhunga committed suicide in South Africa shortly after videos of her being bullied went viral on social media. Commentators have stated that this is a stark reminder that more needs to be done to combat digital harm, such as cyberbullying.[238]

In Tunisia, the National Centre for Technologies in Education (CNTE), under the supervision of the Ministry of Education, is responsible for developing and integrating information and communication technologies into the Tunisian education system. Tunisia's Ministry of Education launched its digital school programme 'Solution Numérique Pour Tous' in May 2015, as part of its wider programme of reform. Tunisia took a truly consultative approach to designing its national development plan with input from thousands of citizens. One of its projects is the Educanet platform, a collaborative platform that forms a link between the management of the establishment, the teaching staff, parents and pupils or students. Educanet covers levels of study from primary grades through to university. [239]

In addition, in 2021, the Ministry of Women, Family and Seniors in Tunisia launched in collaboration with the UNICEF office in Tunisia an awareness campaign under the slogan 'Together to end online violence with regard to children'. This campaign is aimed primarily at children, adolescents and their families and to raise awareness among the general public about the forms of online violence against children. The Ministry has set up a free helpline to provide children and families with listening, psychological assistance and guidance and also to receive reports of violence in the home, including on the internet, while respecting the personal data and confidentiality of each child. As part of a partnership between the National Computer Security Agency (ANSI) and a Tunisian startup, an educational and interactive game using Augmented Reality technology, entitled 'Vigilant Use of the Internet' was announced. It is a game that is part of a set of components of the 'Toufoula Kids' mobile application, developed by the same startup. This educational game features a set of tips, information and awareness content, as well as a Quiz to be played by parents and their children.[240]

The president of the National Authority of Personal Data Protection has warned parents in Tunisia not to share photos of their kids on social media (sharenting) in case it puts the child in danger. The use of a child image requires a legal guardian's consent and family judge authorisation. A parent is not essentially a legal guardian and can be infringing the law by sharing their children's images or other material making them identifiable online. According to the report on Tunisia, these provisions are frequently overlooked.

In Uganda, a toll-free number and online portal have been established by the National Information Technology Authority in partnership with UNICEF for the reporting of online child exploitation materials. The National Information Technology Authority-Uganda (NITA-U) has further been working to promote safer internet access for children and has conducted multiple initiatives to advocate for increased safeguards on the internet and reporting mechanisms. In February 2021, the NITA-U, the National Computer Emergency Response Team of Uganda (CERT.UG), Internet Society Uganda Chapter, the Ministry of Internal Affairs with support from Facebook and MTN, along with UK-based IWF launched a new campaign 'Help Children Be Children' to protect children from online sexual abuse.[241] Also, U-Report, the free tool for community participation, began as a local tool in Uganda to help young Ugandans engage on issues that affect their lives, has become a global network of nearly 4 million users.[242]

February 2022).

238 N Sonjica 'Limpopo pupil allegedly commits suicide after being bullied at school' *Sunday Times* 13 April 2021 https://www.timeslive.co.za/news/south-africa/2021-04-13-limpopo-pupil-allegedly-commits-suicide-after-being-bullied-at-school/ (accessed 9 February 2022).

239 Educanet platform https://educanet.pro/default.html (accessed 9 February 2022).

240 Ansi www.ansi.tn (accessed 9 February 2022); http://enfants.ansi.tn. (accessed 9 February 2022).

241 'Uganda launches online portal to report child sexual abuse' *DigWatch* 1 February 2021 https://dig.watch/updates/uganda-launches-online-portal-report-child-sexual-abuse. See IWF 'Help children be children' (2021) https://www.stopit.ug/ (accessed 9 February 2022).

242 UNICEF 'Children in a digital world' (2017) https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf (accessed 9 February 2022).

In Mauritius, the Child Development Unit (CDU), established in 1995, is responsible for ensuring that the survival, protection, development and participation rights of Mauritian child are upheld as per the Convention on the Rights of the Child whereby the best interests of the child shall be of primary consideration in all policies, programmes and actions pertaining to children's welfare. The CDU must, among other things:

- provide for Protection Services to victims of violence, abuse and neglect;
- provide a hotline service with respect to reporting of a case and counselling as appropriate;
- provide victims with follow-up sessions to ensure recovery from trauma and thereafter their re-insertion in society; and
- provide community safety and community actions in Child Protection and Child Welfare in general through Community Child Protection Programme and Outreach Programmes.[243]

Zimbabwe has made some notable strides in advancing children's rights online, including, the 2020 Child Online Safety Guidelines launched by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). The guidelines are based on the International Telecommunication Union's (ITU) Guidelines on Child Online Protection.[244]

One of the few country reports to include any concrete information about games, Zimbabwe reports that The Child Online Safety Guidelines includes a section on 'playing games online'. The Guidelines encourage children to be mindful of how much they play and who they play with and further encourage children to protect their privacy and not share their personal information with other gamers. In the event there is uncertainty around the suitability of a game, children are advised to approach parents, guardian, or a trusted adult to check its classification and reviews. The Guidelines provide five tips to children:

1. If another player is behaving badly or making you uncomfortable, block them from your players list. You may also be able to report them to the game site operator.
2. Limit your game play time so you can still do other things like homework, jobs around the house and hanging out with your friends.
3. Keep personal details private.
4. Remember to make time offline for your friends, your favourite sports, and other activities.
5. Remember it is easily addictive to always stay online, which can make you vulnerable to internet dangers, you should, therefore, exercise self-discipline.[245]

9 Advertising

In Algeria, the General Provisions: Law 09 of 10 June 2018, amending and supplementing Law 09-03 of 25 February 2009, on Consumer Protection and Fraud Prevention, was published in the Official Gazette. Law 18-09 introduces a consumer's right of withdrawal claimed by the Algerian Federation of Consumers for a long time. Direct Marketing is prohibited except by email under certain conditions.

In Cameroon, the state regulates advertising with the support of the National Advertising Board. Section 27 of the Law on Advertising 2006/018 says:

1. Where advertising is targeted at children it must not be to jeopardise their upbringing, not carry any written, visual or oral statement that may cause them physical, material, mental or moral injury.
2. It must not exploit, spoil or undermine the special trust or respect that minors have for their parents, their educators or other persons on whom they depend for their moral or intellectual upbringing.

However, there is no legislation specifically regulating the use of children's data for marketing purposes.[246]

In Kenya, section 12(2) of the Data Protection (General Regulations) of 2021 provides:

> In relation to processing personal data relating to a child, a data controller or data processor shall ensure that:

243 Ministry of Gender Equality and Family Welfare 'Child development unit' https://gender.govmu.org/Pages/Child-Development-Unit.aspx (accessed 9 February 2022).

244 'POTRAZ launches online safety guidelines for children' *Herald* 30 November 2020 https://www.herald.co.zw/potraz-launches-online-safety-guidelines-for-children/ (accessed 9 February 2022).

245 POTRAZ 'Child online protection guidelines for children' (December 2015) http://www.potraz.gov.zw/wp-content/uploads/2015/05/POTRAZ_COP.pdf (accessed 9 February 2022).

246 The Law on Advertising 2006/018, sec 27.

(a) a person exercising the right is appropriately identified.
(b) profiling of a child that is related to direct marketing is prohibited, and
(c) the parent or guardian is informed of the inherent risks in processing and the safeguards put in place.

Additionally, the Code of Advertising Practice, prohibits advertising which exploits a child's credulity, or which contains physically, mentally, or morally harmful content.

In Mozambique, the Advertisement Code and the Electronic Transactions Law address advertising and electronic marketing. The former requires an opt-out portion for direct marketing, and the latter requires express consent from the recipient. Apart from this, there are limited available resources regarding children and advertising.[247]

The Media Council of Tanzania has a Code of Ethics for Media Professions. This code offers guidelines to media advertising agents and the relevant portion of our purposes declares that children may not be used 'exploitatively in advertisements that concern adults. Also, children should not be exposed to products that are harmful'. The Code further places restrictions on content, prohibiting any portal of violence and aggression in advertisements aimed at children. Advertisements with menacing or horrific themes, unsafe acts, pictures or sound likely to disturb children, or that encourage anti-social behaviour by children are also prohibited.[248]

Apart for the Data Protection Act of 2019 cited above, the Ugandan Communications Commission's Advertising Standards make specific reference to children, including the following:

- Advertisements addressed to or likely to influence children shall not contain any statement or visual presentation which might result in harming them, mentally, morally, physically or emotionally. Particular attention and care shall be taken in an advertisement that is aimed at or is likely to be viewed by Minors (below 13 years).
- Commercial communications shall not cause or be to the moral, mental or physical detriment to children, and shall comply with the following criteria for their protection, and shall not:
- Directly exhort children to buy or hire a product or a service by exploiting their inexperience or credulity;
- Directly encourage children to persuade their parents, guardians or others to purchase the products or services being promoted;
- Exploit the special trust children place in parents, guardians, teachers or other persons of stature in society; or
- Unreasonably show children in dangerous situations.
- Telemarketing shall not exhort or encourage children to contract for the sale or rental of products and services.

These standards are enforced by the Uganda Communications Commission.

Advertising is strongly regulated in Nigeria. Specific consent is required for the use of personal data for marketing purposes, according to the NDPR Implementation Framework. Other relevant laws and guidelines are the Nigerian Code of Advertising Practice (Advertising Code), Advertising Practitioners Council of Nigeria (APCON) Vetting Guidelines, Federal Competition and Consumer Protection Act (FCCPA) and Standards Organisation of Nigeria Act 2015 (SONA). APCON is the main body that regulates advertising, while NCC monitors whether the telecoms sector complies with advertising rules, and can impose sanctions on service providers. [249]

The Advertising Code has specific provisions relating to products or services aimed at children. Article 77 stipulates that marketing communications that are unsuitable for children should be clearly identified in the message subject line; products unsuitable for children (condoms, alcohol) cannot be advertised during children's programmes; parental consent is required for disclosing children's identifiable information to third parties; and parents

247 DLA Piper 'Data protection laws of the world: Mozambique' (28 January 2019) https://www.dlapiperdataprotection.com/index.html?t=law&c=MZ (accessed 9 February 2022).
248 Code of Ethics for Media Professions, 2016 at 3.9.
249 B Scott 'Nigeria: General principles and requirements for advertising in Nigeria' (6 January 2020) https://www.mondaq.com/nigeria/advertising-marketing-branding/880690/general-principles-and-requirements-for-advertising-in-nigeria (accessed 21 April 2021).

and guardians are encouraged to participate in and/or supervise children's activities.[250]

In Ghana, section 40 of the DPA entitles data subjects, by giving notice in writing, to require a data controller not to process personal data for purposes of direct marketing. This right is not child specific, nor is it child friendly. In Morocco, it is reported that the Blue Whale game has allegedly caused the death of two Moroccan children, in 2017. [251]

There are no institutions or strategies in place to face these threats and protect children. The Advertising Association of Ghana (AAG) regulates advertising. Article 8 of the AAG Standards states that:

> Special care shall be taken in advertisements directed to or featuring children. These advertisements shall not undermine positive social behaviour, lifestyle and attitude. Products suitable for children shall be advertised in media targeted at them. Advertisements directed at children shall not be inserted in the media where the editorial matter is unsuitable for them. Materials unsuitable for children shall be clearly identified as being unsuitable for them.

There are also specific prohibitions on advertising alcohol, condoms or unhealthy food to children. In practice, however, children in Ghana who use the internet have access to all kinds of inappropriate content.[252]

In Mauritius, the Code of Advertising Practice, developed by the Independent Broadcasting Authority in terms of the Independent Broadcasting Authority Act, includes a chapter on the protection of children. The chapter provides several protections including the following:

- A prohibition on advertisements on a programme intended for children may result in physical, mental, moral or emotional harm to them.
- Advertisements must not lead children to believe that unless they acquire or use the product advertised they will be inferior in some way.
- Advertisements must not misguide minors towards obvious abuse or excess.
- Care and restraint are recommended when showing naked or partly undressed children in advertisements.
- In no circumstances should gambling advertisements target minors.
- Any situation in which children are to be seen in television advertisements should be carefully considered from the point of view of safety.

The Independent Broadcasting Authority Act, amended in 2019, makes provision for digital broadcasting which is defined as the 'practice of using advanced digital compression techniques to encode and transmit audio, text, data, images and video signals resulting in more efficient bandwidth usage'.[253]

In the DRC, there are no measures in place concerning the processing of children's personal data for advertising purposes. Children are not legally protected against age-related discrimination in relation to services, information or goods. There are no measures in place to protect children from invasive or inappropriate advertisements. The processing of children's personal data for advertising purposes is not substantially regulated in Burkina Faso. Nonetheless, the Information Code prohibits specialised publication or general information that contains advertisement or advertisement likely to support juvenile delinquency or the depravity of morals and the eTransactions Act addresses consumer's rights towards online advertising under its sections 47-54. It requires compliance with legal requirements for privacy protection, but does not have special conditions for children.[254]

In Senegal, advertising is regulated by the eTransactions Act and the Decree relating to eCommerce. Although the age of the minor is not specified, this decree deals with the processing of children's/minor's personal data for advertising purposes and guarantees the child protection in this particular matter. The state can limit or prohibit an

250 As above.

251 'Suicide game "Blue Whale Challenge" allegedly kills two Moroccan children' *moroccoworldnews* 29 December 2017https://www.moroccoworldnews.com/2017/12/237428/blue-whale-kills-moroccan-children/ (accessed 9 February 2022).

252 UNICEF 'Ghana: Child online protection' (2018) https://www.unicef.org/ghana/child-online-protection (accessed 9 April 2021).

253 The Independent Broadcasting Authority Act, sec 1.

254 eTransactions Act, secs 47-54.

eCommerce activity for reasons of 'public security, protection of minors, consumers, public health or the preservation of national defense interests'. All online advertising is required to be duly informed, considering the incapacity of minors, and take care not to harm their physical and moral integrity.

There are no express measures specified to protect children from exposure to economic exploitation through embedded ads, privacy-invasive practices, age-inappropriate content, as well as the exploitation of their incredulity and inexperience resulting in economic risks such as overspending or online fraudulent transactions. However, children are protected against discrimination in access to certain services through parental coverage. For example, advertising message that directly solicits minors and incites a financial expenditure, like the subscription to a paid service or the use of a premium rate number must be addressed to parents or legal guardians. The collection of personal data concerning a third person through a minor is also prohibited.[255]

In South Africa, Section II of the Code of Advertising Practice revised in 2021 by the Advertising Regulating Board, provides a comprehensive section on children. The provision includes, among other things, the following protections for children:

- Advertisements addressed to or likely to influence children should not contain any statement or visual presentation which might result in harming them, mentally, morally, physically or emotionally.
- Advertisements should not exploit the natural credulity of children or their lack of experience and should not strain their sense of loyalty.
- Children should not be portrayed as sexually appealing, provocative or in any manner which involves any form of sexual innuendo.

In Tunisia, article 30 of the Personal Data protection law prohibits the processing of personal data for advertising purposes without an explicit and special consent from the data subject. It also states that the consent given for a specific form and purpose could not apply to other forms and purposes.

If the data subject is a child, the provisions of article 28 apply. This means that children's personal data for advertising purposes requires the explicit and special consent of their guardians and the authorisation of a family judge. The family judge can at any moment discard the authorisation.[256] In Zimbabwe, UNICEF[257] explains that:

> There are no known regulations on marketing to children in Zimbabwe. There is a self-regulatory body, the Advertising Standards Authority (ASAZIM), which has a Code of Standards drafted on the basis of the International Code of Advertising Practice prepared by the International Chamber of Commerce. Members of ASAZIM are required to adhere to the Code, but the Code does not address marketing to children.

10 Responding to breaches of children's privacy

In Benin, the Digital Code and the Child Code both include express child-sensitive provisions and safeguards. While there are no specific safeguards on filtering and monitoring, both the Digital Code and the Child Code provide for prison sentences and financial penalties against various violations of children's rights online.[258] Under the Digital Code, operators providing internet access and online service providers must work together to combat infringements including those relating to children's rights. To this end, they are required to establish an easily accessible and visible system allowing any person to notice and report unlawful activities. They also have the obligation to promptly inform the competent authorities of any illicit activities and make public the resources they devote to the fight against these illicit activities. The Digital Code punishes manufacturing, transportation, dissemination of a violent or pornographic content likely incite minors to engage in games involving them physically in danger.[259]

It is reported that in Cameroon, prosecutions for some data privacy crimes against children could be brought under the Cybersecurity and Cybercrime Law 2010.

255 Decree on eCommerce, art 28.
256 Personal Data Protection Law, art 28.
257 UNICEF 'Zimbabwe: Child rights and business guidance for Chinese companies operating in Zimbabwe' https://www.unicef.cn/en/csr/zimbabwe (accessed 2021).
258 Digital Code, art 518.
259 Digital Code, art 520.

In Morocco, article 87 of the telecommunication law states that anyone who considers himself the victim of defamation, injury, invasion of privacy or image rights, by direct publication or by reproduction, as long as it is identifiable by expressions used in the written or electronic journal concerned, including audio-visual content, and who has suffered damage as a result may claim compensation under the conditions and modalities provided for by the legislation in force.

In Tanzania, section 18 of the Electronic and Postal Communications Regulations Online Content Regulations, which came into effect in 2020, states that:

A person who provides has access to, hosts, uses online contents or operates an internet café shall take all possible measures to ensure that:

(a) Children do not register, access, or contribute to prohibited content; and
(b) Users are provided with content filtering mechanisms and parental control.

The Regulations require immediate takedown of allegedly illegal content. Concern has been raised with this, noting that the provisions fail to comply with international human rights standards for content governance.[260]

However, clear civil and criminal remedies for holding private actors to account were not evident.[261] In Tunisia, the oversight authority on the audio-visual sector, the Independent High Authority for Audio-visual Communication, has warned and sanctioned TV and radio stations for the diffusion of inappropriate content for children and required changes of the material and diffusion hours. HAICA also intervened in cases of non-respect to child privacy on multiple occasions and required stations to stop the diffusion of the concerned programs and removal of material from their websites and social media pages.[262]

In Uganda, Freedom House has recorded that the government continues to block pornography sites, and communication platforms and Virtual Private Networks (VPNs) are blocked under-enforcement of the tax on Over the Top Tax (OTT) services. The blockages at the behest of the state have been condemned by various human rights organisations as a violation of the right to freedom of expression and other internet rights freedoms.[263]

In Senegal, the Orientation Law on the Information Society also calls on stakeholders to prevent abusive use of ICT, as for the collection or misuse of personal data in criminal acts dictated by racism, racial discrimination and xenophobia, intolerance, hatred, violence and terrorism, as well as all forms of child abuse, like child pornography. Further to this, the Code of Criminal Procedure provides that the investigating judge or the judicial police officer may request

> content publishers, even hosted abroad, for the purpose of removing or making impossible access to clearly illegal content, including child pornography, acts racist and xenophobic, content that infringes on privacy (Article 90-14).

Civil liability of content intermediaries like ISPs, content producers, purveyors of digital goods, is not incurred when an unlawful content is stored on their platform, if they had no evidence of the unlawful nature of the content, or if they remove it as soon as they are aware of it.[264]

11 Recommendations and analytical inferences

11.1 Applicable regional law

States that have not done so should be encouraged to ratify the African Union Convention on Cyber

260 B Taye 'Internet censorship in Tanzania: The price of free expression online keeps getting higher' *AccessNow* 22 October 2020 https://www.accessnow.org/internet-censorship-in-tanzania/ (accessed 9 February 2022).

261 Tanzanian Commission for Human Rights and Good Governance et al 'Voices From Tanzania – Case studies on business and human rights' 1 (2019) at 7 https://ipisresearch.be/wp-content/uploads/2019/04/1904-Voices-from-Tanzania-Business-and-Human-Rights-WEB.pdf (accessed 9 February 2022).

262 High Independent Authority for Audiovisual Communication https://haica.tn/ (accessed 9 February 2022); Decree-Law 116 of 2011 http://www.inric.tn/fr/decret.pdf (accessed 9 February 2022).

263 A Kalemera 'State of internet freedom in Uganda 2016: Charting patterns in the strategies African governments use to stifle citizens' Digital Rights' *CIPESA* (December 2016) http://cipesa.org/?wpfb_dl=235 (accessed 9 February 2022).

264 Law N° 2008-08 of 25 January 2008 on electronic transactions, art 3. 2.

Security and Personal Data Protection (Malabo Convention).

The ACERWC could be encouraged to develop a guidance note on children's rights to privacy in the context of the ACRWC, also for sharing with states parties and for drawing attention more closely to the implications of the digital environment for children's rights to privacy. Links should be drawn between children's rights to freedom of expression, and more narrowly their participation rights, as enhancing children's right to participate has particular significance for African children.

The ACERWC could also review the implication of the collection of children's biometric data upon their rights to privacy, as suggested in the context of recent proposals to do this in South Africa. It is not just a local issue, but could have continental ramifications too.

11.2 Legislation

Many country reports question the extent to which children's privacy rights have been accommodated in national law and policy. Whilst noting considerable variation across the country reports, it is to be welcomed that there are several recent law reform endeavours relating to protection of personal information, and standards in countries such as Kenya have become increasingly elaborate. In some quarters, such as Malawi and Zimbabwe, Bills are pending, and Parliaments considering these Bills should be supported with information and access to best practice examples. Dated legislation which is no longer fit for purpose as digital developments have occurred over the past decade should be revisited and revised.

Legislation applicable to the various domains (data protection, cyber security, etc) discussed in the report should expressly take children's rights in general, and their rights to privacy, into account for more usually than has occurred thus far.

11.3 Child laws

Benin's Digital Code seems to provide one example of special efforts to address children's right to privacy in the digital sphere. It is a national framework document and devotes its entire Fifth Book (articles 379-490) to the protection of individual's privacy. Article 379 specifies that its provisions: 'are intended to set up a legal framework for the protection privacy and professional life following the collection, processing, transmission, storage and use of personal data'. It also directly addresses children's privacy protection, especially with regard to the digital environment. Several of its provisions focus on children's right to privacy, especially those relating to consent, lawful processing, service supply or direct marketing. Dealing with transparency in the processing of personal data, article 418 requires the data controller to communicate in a clear and simple, meaningful, transparent, understandable and accessible manner vis-à-vis the child as a data subject in the processing of his personal data. Even so, the Benin report concludes that the protection of children's privacy in the digital environment does not seem to be clearly integrated as a priority by the Beninese law. Given the notorious vulnerability of children in Benin and the security issues facing digital developments, it is essential to rethink the child protection policy with a focus on their online safety…[the Digital Code] principles relating to his protection and participation are evaded or slightly addressed. In addition, the Personal Data Protection Authority (APDP's) missions do not include clearly and oriented specific actions in favour of children.

Countries which have not enacted comprehensive child protection laws, such as Senegal, Ethiopia and Zambia, should do so.

11.4 Judicial protection of the right to privacy

There is seemingly emerging a (small) body of jurisprudence on protection of children's privacy rights. It would be useful for a body such as the Centre for Human Rights to maintain an online repository of cases from around the continent, as and when they are decided by courts.

11.5 Advertising

There have been several examples provided of advertising standards which clearly reflect a child rights lens, Uganda being one. These enactments of codes can be emulated in countries where such standards do not exist, or where they are too limited given the range of potential rights-violations that children may face through digital advertising.

11.6 Remedies

The possible remedies for unlawful interference with the child's privacy rights are multifarious, and range from criminal prosecutions, to civil lawsuits,

to damages claims, and injunctions or 'take down' type orders.

Although there are remedies that a child might use to prevent 'sharenting' and to secure the removal of 'sharented' information, include a range of legal avenues potentially available to anyone who objects to the online dissemination of their personal, private or confidential information, including a breach of confidence action or a tort of misuse of private information, in practice, where a child's privacy has been violated by their parents, their ability to obtain a remedy is far more limited than that of adults. Children rarely have the financial means to bring court proceedings. Additionally, they must prove that their information was confidential, that the parent was subject to a duty of confidence, and that the 'sharenting' was unjustified. Probably the only way to address this is through education initiatives that explain to parents why they should not share the private information of their child.

However, several reports note the complications of language in their respective countries (Burkina Faso and Senegal) where the majority of citizens are not versed in the official language, French.

11.7 Other measures

Education of children on digital citizenship and their rights seems the most useful tool to address the challenges discussed in this report. Therefore, national authorities should identify the various stakeholders who would appropriately lead on developing national and subnational programmes to enhance this goal.

Bibliography

Books

Assim, UM 'Civil rights and freedoms of the child' in Kilkelly, U & Liefaard, T *The international human rights of children* (Springer 2018)

Boezaart, T *Introduction to child law* (Juta Cape Town 2009)

Gose, M *The African charter on the rights and welfare of the child* (Community Law Centre, Cape Town 2002)

Nabenyo, E 'Kenya' in *Paradigm Initiative* (ed) *Digital rights and inclusion in Africa report* (2020)

Ndongmo, K 'Cameroon digital rights landscape report' in Roberts, T (ed) *Digital rights in closing civic space: Lessons from ten African countries* (Institute of Development Studies 2021)

Nwankwo, IS 'Information privacy in Nigeria' in Makulilo, AB (ed) *African data privacy laws* (Springer International Publishing: New York 2016)

Tobin, J & Field, SM 'Article 16: The right to protection of privacy, home, family, correspondence, honour and reputation' in Tobin, J & Alston, P *A Commentary on the Convention on the Rights of the Child* (Oxford University Press 2019)

Journals

Adeto, Y 'Preventing violent extremism in the Horn: The case of ethnic extremism in Ethiopia' *Policy Paper: European Institute of Peace* (2019)

Adeto, Y 'Violent ethnic extremism in Ethiopia: Implications for the stability of the Horn of Africa' (2020) 2 *AJCR*

Ayalew, Y 'Assessing the limitations to freedom of expression on the internet in Ethiopia against the African Charter on Human and Peoples' Rights' (2020) 20 *African Human Rights Law Journal* 315

Borainea, A & Ngaundje, LD 'The fight against cybercrime in Cameroon' (2019) 35 *International Journal of Computer* 91

Kravchuk, N 'Privacy as a new component of "the best interests of the child" in the new digital environment' (2021) 29 *The International Journal of Children's Rights* 99

Livingstone, S; Stoilova, M & Nandagiri, R 'Children's data and privacy online: Reviewing the existing evidence' (2018) *London: London School of Economics and Political Science*

Ministry of Gender, Children and Social Protection 'Children's online safety concerns in Ghana: A position paper on legislative and policy gaps' (July 2018)

Nyst, C; Gorostiaga, A & Geary, P 'Children's online privacy and freedom of expression' UNICEF (2018) 8

OneTrust DataGuidance™ '*GDPR v Nigeria* Data Protection Regulation' (2019) *Comparing Privacy Laws* 5

Raab, C & Goold, B 'Protecting information privacy' (2011)

Right2Know Campaign 'Submission to the Director-General of the Department of Home Affairs on the Draft Official Identity Management Policy' (2020)

Shade, LR & Singh, R '"Honestly, we're not spying on kids": School surveillance of young people's social media' (October 2016) *Social Media + Society*

Sibidla, T 'Data protection and privacy regulation: A roundup of developments in Africa in 2021' (2021)

Turianskyi, Y 'Africa and Europe: Cyber governance lessons' (2020) 77 *Policy Insights* 10

Case law

AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services 2021 (3) SA 246 (CC)

Jamii Media Company Ltd v The Attorney General (2017) TLS LR 447

Kenya Human Rights Commission v Communications Authority of Kenya 86 of 2017

Kenya, Okoiti v Communications Authority of Kenya [2017] eKLR

Madhewoo v the State of Mauritius [2016] UKPC 30

SM v ABB case 20/1732 (11 September 2020, Gauteng Local division)

Legislation

2009 Law of the Child Act of the Mainland

2011 Zanzibar Children's Act

Anti-Cyber and Information Technology Crimes Law 175 of 2018

Anti-Pornography Act, 2014

Book V of the 2017 Digital Code of the Republic of Benin

Bulletin Officiel 'Law 24-96 governing the post and telecommunications' (16 October 1975)

Bulletin Officiel 'Decree 2-09-165 du joumada 11430' (21 May 2009)

Burkina Faso; Law 015-2014 / AN of 13 May 2014 on the Protection of Children in Conflict with the Law or in Danger

Burkina Faso 'Stratégie nationale de cyber sécurité 2019-2023' (SNCS-BF)

Cameroonian Criminal Code

Chapter 12:50 Act 2 of 2000

Child Protection Bill of 2020

Code of Ethics for Media Professions, 2016

Convention on the Rights of the Child, UN General Assembly, 20 November 1989, United Nations, Treaty Series, vol 1577, p 3

Côte d'Ivoire; Law 2013-450 of 19 June 2013 on the protection of personal data

Criminal Code of the Federal Democratic Republic of Ethiopia 414 of 2004

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007

Data Protection Act 2012 (DPA)

Data Protection Law

Decree 4506 of 2013, relating to the creation of the Technical Agency telecommunications and fixing its administrative, financial organisation and the modalities of its operation

Decree on eCommerce

Digital Code

Electronic Transactions and Cybersecurity Act 33 of 2016

eTransactions Act

Freedom of Information Bill HB 6, 2019

Information and Communication Technologies Act 2001

Kenya Data Protection Act, 2019

Law 12 of 1996 amended by Law 126 of 2008

Law n ° 2008-08 of 25 January 2008 on electronic transactions

Law n ° 2017-20 of 20 April 2018, on the Digital Code in the Republic of Benin

Law n. ° 24/2019

Law n° 2008-12 of 25 January 2008 on the protection of personal data

Law 01 0-2004 / AN of 20 April 2004

Law 18-07 of 25 Ramadhan 1439 Corresponding to 10 June 2018

Law of the Child, 2009

Penal Code Article

Personal Data Protection Act

Personal Data Protection Law

RÉPUBLIQUE DU BÉNIN Loi n° 2017-20 du 20 avril 2018 portant code du numérique en République'

Telecommunications Law 10 of 2003

The Children (Amendment) Act 2016

The Code for the Protection of Children

The Computer Misuse Act 2011

The Constitution of the Democratic Republic of the Congo, 2005

The Criminal Code

The Data Protection Act 24 of 2019

The Independent Broadcasting Authority Act

The Law 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data

The Law on Advertising 2006/018

The Law on the Promotion and Protection of the Rights of the Child 7 of 2008

The Law on the Protection of Personal Data issued under Resolution 151 of 2020

The Mauritius Computer Misuse and Cybercrime Act, 2003

The Organic Act No. 26 of 2015 of Relating to the Fight Against Terrorism and the Suppression of Money Laundering (7 August 2015)

Internet sources

African Union Convention on Cyber Security and Personal Data Protection 'List of Countries which signed, ratified/acceded' 18 June 2020 https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (accessed 7 February 2022)

Agence nationale de réglementation des télécommunications 'ANRT' 2022 https://www.anrt.ma/en/ (accessed 2021)

Ahram Online 'A young nation: 40% of Egypt's population are under 18' 20 November 2017 https://english.ahram.org.eg/NewsContent/1/0/281848/Egypt/0/A-young-nation--of-Egypts population-are-under-.aspx (accessed 2 February 2022)

Aldgate, J & Rose, W 'Assessing and managing risk in getting it right for every child' https://lx.iriss.org.uk/sites/default/files/resources/0069411.pdf (accessed 10 February 2022)

ALT Advisory 'Data Protection Africa: South Africa' 3 August 2020 https://dataprotection.africa/wp-content/uploads/2020/08/South-Africa-Factsheet-updated-20200803.pdf (accessed 7 February 2022)

ALT Advisory 'Factsheet Mauritius' Data Protection Africa 31 March 2020 https://dataprotection.africa/wp-content/uploads/2020/03/Mauritius-Factsheet-updated-20200331.pdf (accessed 7 February 2022)

ALT Advisory 'Factsheet: Tanzania' 31 March 2021 https://dataprotection.africa/wp-content/uploads/2020/03/Tanzania-Factsheet-updated-20200331.pdf (accessed 7 February 2022)

Amnesty International 'Nigeria: Bills on hate speech and social media are dangerous attacks on freedom of expression' 4 December 2019 https://www.amnesty.org/en/latest/news/2019/12/nigeria-bills-on-hate-speech-and-social-media-are-dangerous-attacks-on-freedom-of-expression/ (accessed 7 February 2022)

ANSSI Bénin | Agence Nationale de la Sécurité des Systèmes d'Information https://anssi.bj/ (accessed 12 June 2021) (accessed 9 February 2022)

Arab Republic of Egypt https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Documents/Presentation%20for%20Uganda%20.pdf (accessed 9 February 2022)

ARTICLE 19 'The government' 19 January 2021 https://www.article19.org/resources/ethiopia-hate-speech-and-disinformation-law-must-not-be-used-to-supress-the-criticism-of-the-government/ (accessed 8 February 2022)

AVIS COP 'Quarterly Notice No 03-2018 of the Personal Data Protection Commission of Senegal (CDP)' 7 November 2018 https://www.cdp.sn/content/avis-trimestriel-n%C2%B0-03-2018-de-la-commission-de-protection-des-donnees-personnelles-du (accessed 10 February 2022)

Broughton, T 'Joburg teen sues Facebook for name of Insta stalker who threatened rape & murder' 27 Times Live July 2020 https://www.timeslive.co.za/news/south-africa/2020-07-27-joburg-teen-sues-facebook-for-name-of-insta-stalker-who-threatened-rape-murder/ (accessed 9 February 2022)

Bulletin Officiel 'Decree 2-09-165 du joumada 11430' (21 May 2009) https://www.cndp.ma/images/lois/Decret-2-09-165-Fr.pdf

Burkina Faso LOI No 051-2015/CNT Portant Droit D'acces a l'information Publique et aux Documents Administratifs (2015) https://tinyurl.com/uebdc72c (accessed 7 February 2022)

Children Parliament; Law no 0001-2009 / PDE of July 8, 2009 Protecting the rights of children and adolescents in the media in Burkina Faso https://tinyurl.com/24365rkz (accessed 8 February 2022)

CIL 'Youth & digital' http://www.cil.bf/index.php/jeunesse-numerique (accessed 9 February 2022)

Commonwealth Telecommunications Organisation 'Stratégie Nationale de Cybersécurité du Sénégal' (SNC2022)' November 2017 http://www.numerique.gouv.sn/sites/default/files/SNC2022-vf.pdf (accessed 2 February 2022)

Committee on the Rights of the Child, General Comment 25 (2021) on children's rights in relation to the digital environment (2021) UN Doc CRC/C/CG/25 dated 2 March 2021 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en (accessed 8 February 2022)

Communications Authority of Kenya 'Second Quarter Sector Statistics Report for the Financial Year 2020/2021)' December 2020 https://ca.go.ke/wp-content/uploads/2021/03/Sector-Statistics-Report-Q2-2020-2021-1.pdf (accessed 27 April 2021)

COP Piratage psychologique (ingénierie sociale), ne te laisse pas berner! (28 April 2021) https://www.cdp.sn/content/piratage-psychologique-ingénierie-sociale-ne-te-laisse-pas-berner (accessed 9 February 2022)

Defy Hate Now 'The state of digital rights in Cameroon' 21 January 2020 https://defyhatenow.org/the-state-of-digital-rights-in-cameroon-2/ (accessed 12 April 2021)

Dehnarain, N 'Trouble in paradise: Facebook spread of hate speech as Mauritius oil spill crisis continues' Forbes 20 September 2020 https://www.forbes.com/sites/nishandegnarain/2020/09/20/trouble-in-paradise-facebook-spread-of-hate-speech-as-mauritius-oil-spill-crisis-continues/?sh=58811af927a5 (accessed 9 February 2022)

Department of Justice Egypt 'Freedom on the net 2019' 2019 https://www.justice.gov/eoir/page/file/1333771/download (accessed 7 February 2022)

Dictionary.com https://www.dictionary.com/browse/privacy#:~:text=the%20state%20of%20being%20

free,See%20also%20invasion%20of%20privacy (accessed 10 February 2022)

DigWatch 'Malawi government planning to amend laws to tackle cyber bullying' 24 December 2020 https://dig.watch/updates/malawi-government-planning-amend-laws-tackle-cyber-bullying (accessed 9 February 2022)

DigWatch 'Uganda launches online portal to report child sexual abuse' 1 February 2021 https://dig.watch/updates/uganda-launches-online-portal-report-child-sexual-abuse (accessed 9 February 2022)

DLA Piper 'Mozambique' 28 January 2019 https://www.dlapiperdataprotection.com/index.html?t=law&c=MZ (accessed 9 February 2022)

DPC 'About the commission' https://www.dataprotection.org.gh/ (accessed 9 April 2021)

ECPAT 'Country overview: A report on the scale, scope and context of the sexual exploitation of children in Mauritius' June 2019 https://www.ecpat.org/wp-content/uploads/2019/06/Mauritius-ECPAT-Country-Overview-Mauritius-July-2019.pdf (accessed 9 February 2022)

ECPAT International and Rede da Criança 'Supplementary report on "Sexual Exploitation of Children in Mozambique" to the third and fourth periodic reports of Mozambique on the implementation of the Convention on the Rights of the Child and the Optional Protocol on the sale of children, child prostitution and child pornography' 1 November 2018 https://www.ecpat.org/wp-content/uploads/2018/07/Convention-on-the-Rights-of-the-Child-report-on-Sexual-Exploitation-of-Children-to-the-Committee-on-the-Rights-of-the-Child-Mozambique-English-2018.pdf (accessed 8 February 2022)

Educanet platform https://educanet.pro/default.html (accessed 9 February 2022)

EIPR Press release 'EIPR condemns five-year prison sentence for children on blasphemy charges: 12 defendants convicted in 9 cases since January 2015; 11 cases pending before courts and more cases pending before disciplinary bodies' (September 2020) https://eipr.org/en/press/2016/02/eipr-condemns-five-year-prison-sentence-children-blasphemy-charges-12-defendants (accessed 25 February 2016)

EIPR Press release 'After Menna Abdel Aziz's release and the prosecution's decision that there are no grounds in bringing a case for the charges against her, EIPR calls on the prosecution to take the same approach in similar cases to protect victims of sexual violence' (September 2020) https://eipr.org/en/press/2020/09/after-menna-abdel-aziz%E2%80%99s-release-and-prosecutions-decision-there-are-nogrounds?fbclid=IwAR3OCLusWZsQgE0pUeJySEdKzWNi4gBBkBL6Zo9zBzypyXFCmFMw2RLcsB4 (accessed 9 February 20220)

eNCA 'The downside of sharenting' 8 April 2019 https://www.enca.com/life/downside-sharenting(accessed 9 February 2022)

End-violence Against Children 'UNICEF Tanzania' March 2018 https://www.end-violence.org/grants/unicef-tanzania (accessed 9 February 2022)

Famsville Solicitors 'Developing a child online privacy protection framework in Nigeria' 29 November 2018 https://www.lexology.com/library/detail.aspx?g=5509490a-b51d-4a66-8f8f-b57de3209acb (accessed 10 February 2022)

Film and Publication Board https://www.fpb.org.za/ (accessed 7 February 2022)

Freedom House 'Freedom on the Net: Ethiopia' 2020 https://freedomhouse.org/country/ethiopia/freedom-net/2020 (accessed 7 February 2022)

Freedom House 'Freedom on the Net: Kenya' 2020 https://freedomhouse.org/country/kenya/freedom-net/2020 (accessed 7 February 2022)

Freedom House 'Freedom on the Net 2020: Zimbabwe' 2020 https://freedomhouse.org/country/zimbabwe/freedom-net/2020 (accessed 2 February 2022)

Freedom House 'Freedom on the net 2021: Morocco' 2021 https://freedomhouse.org/country/morocco/freedom-net/2021 (accessed 8 February 2022)

Freedom House 'Freedom in the world 2021: Tanzania' 2021 https://freedomhouse.org/country/tanzania/freedom-world/2021 (accessed 7 February 2022)

Freedom House 'Tunisia: Freedom on the Net 2020 Country Report, 2020' 2020

Gabriel, P 'Why you should be careful about posting pictures of your child on social media' Daily Maverick 12 March 2020 https://www.dailymaverick.co.za/opinionista/2020-03-12-why-you-should-be-careful-about-posting-pictures-of-your-child-on-social-media/ (accessed 9 February 2022)

Gillwald, A; Mothobi, O & Rademan, B 'The state of ICT in Mozambique' Research ICT Africa (January 2019) https://researchictafrica.net/wp/wp-content/uploads/2019/07/2019_After-Access_The-state-of-ICT-in-Mozambique.pdf (accessed 2 February 2022)

Government of Mauritius 'Mauritian Cybercrime Online Reporting System' 2020 http://maucors.govmu.org/English/Reporting/Pages/default.aspx (accessed 12 June 2021)

Herald 'POTRAZ launches online safety guidelines for children' 30 November2020 https://www.herald.

co.zw/potraz-launches-online-safety-guidelines-for-children/ (accessed 9 February 2022)

High Independent Authority for Audiovisual Communication https://haica.tn/ (accessed 9 February 2022)

Information and Communication Technologies Authority 'ICTA' 2022 https://www.icta.mu (accessed 12 June 2021)

ICTA 'Statistics cybersecurity' https://www.icta.mu/csa-filtering/ (accessed 8 February 2022)

Inclusive Internet Index 'Ethiopia' 2021 https://theinclusiveinternet.eiu.com/explore/countries/ET/ (accessed 2 February 2022)

INCM 'INCM creates entity responsible for the control of telecommunications traffic' 12 June 2020 https://www.arecom.gov.mz/index.php/sala-de-imprensa/noticias/380-incm-cria-entidade-responsavel-pelo-controle-de-trafego-de-telecomunicacoes (accessed 7 February 2022)

Information & Communication Technologies Authority 'Consultation Paper on proposed amendments to the ICT Act for regulating the use and addressing the abuse and misuse of Social Media in Mauritius' (Consultation Paper) 14 April 2021 https://www.icta.mu/docs/2021/Social_Media_Public_Consultation.pdf (accessed 7 February 2022)

INPDP 'Loi organique numéro 63 en date du 27 juillet 2004 portant sur la protection des données à caractère personnel' 27 July 2004 http://www.inpdp.nat.tn/ressources/loi_2004.pdf (accessed 7 February 2022)

International Telecommunication Union 'First Meeting of the Council Working Group on Child Online Protection (CWG-CP)' 17-18 March 2010 https://www.itu.int/council/groups/wg-cop/first-meeting-march-2010/Contribution%20on%20Child%20Safety%20Online%20Activities%20in%20Mauritius%2011%2003%2010.docx (accessed 10 February 2022)

International Union of Telecommunications 'Global Cybersecurity Index 2019' 2020 https://tinyurl.com/4u2vrd8r (accessed 9 February 2022)

International Union of Telecommunications 'Global Cybersecurity Index 2019' 2019 https://tinyurl.com/4u2vrd8r (accessed 7 February 2022); Bienvenue sur le site de l'ANSSI Bénin

Internet World Stats 'Internet penetration in Africa' (2020) https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/ (accessed 15 April 2020)

Internet World Stats 'Côte d'Ivoire' June 2010 https://internetworldstats.com/af/ci.htm (accessed 2 February 2022)

Intersoft consulting 'GDPR' 25 May 2018 General Data Protection Regulation (GDPR) – Official Legal Text gdpr-info.eu (accessed 10 June 2021)

Journal Officiel de la République Tunisienne 'Decree 4773 of 2014 Fixing the Conditions and Procedures to Grant the Authorization for the Activity of Supplying Internet Services' 23 January 2015 http://www.intt.tn/upload/txts/fr/d%C3%A9cret2014_4773.pdf (accessed 7 February 2022)

Kalemera, A 'State of internet freedom in Uganda 2016: Charting patterns in the strategies African governments use to stifle citizens' digital rights' CIPESA 2016 http://cipesa.org/?wpfb_dl=235 (accessed 9 February 2022)

Kemp, S 'Digital 2020: Cameroon' 17 February 2020 https://datareportal.com/reports/digital-2020-cameroon (accessed 20 April 2021)

Kemp, S 'Digital 2020: Algeria' 17 February 2020 https://datareportal.com/reports/digital-2020-algeria#:~:text=There%20were%2022.71%20million%20internet,at%2052%25%20in%20January%202020 (accessed 2 February 2022)

Law 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data https://anrt.ma/content/dahir-ndeg-1-09-15-du-22-safar-1430-18-fevrier-2009 (accessed 2021)

Le grooming, une nouvelle dérive (7 April 2021) https://www.cdp.sn/content/le-grooming-une-nouvelle-dérive (accessed 9 February 2022)

Ltifi, MA 'Media freedom in Tunisia stirs wide debate' Al-Monitor 13 November 2021 https://www.al-monitor.com/originals/2021/11/media-freedom-tunisia-stirs-wide-debate (accessed 9 February 2022)

Ministry of Communications and Information Technology 'Information and Communication Technology Indicators Bulletin' 2020 https://mcit.gov.eg/En/Publication/Publication_Summary/9260 (accessed 2 February 2022)

Ministry of Gender Equality and Family Welfare 'Child Development Unit' https://gender.govmu.org/Pages/Child-Development-Unit.aspx (accessed 9 February 2022)

Ministry of Gender, Children and Social Protection 'Children's online safety concerns in Ghana: A position paper on legislative and policy gaps' (July 2018) https://www.unicef.org/ghana/media/1806/file/Child%20Online%20Safety%20%20Legislation%20and%20Policy%20Gaps.pdf (accessed 23 April 2021)

Miriri, D 'Kenyan court slams brakes on president's constitutional changes' Reuters 13 May 2021 https://www.reuters.com/world/africa/kenyan-court-slams-brakes-presidents-constitutional-changes-2021-05-13/ (accessed 7 February 2022)

MISA Mozambique 'MISA-Mozambique and government discuss legislative priorities in cybersecurity and data protection' 28 September 2020 https://www.misa.org.mz/index.php/destaques/noticias/97-misa-mocambique-e-governo-discutem-prioridades-legislativas-em-ciberseguranca-e-proteccao-de-dados (accessed 7 February 2022)

Moukouri, D 'Cameroon - Data protection overview' March 2021 https://www.dataguidance.com/notes/cameroon-data-protection-overview (accessed 12 April 2021)

Moyo, J 'Mary Chilima appointed ambassador against girls' online harassment' Nyasa Times 6 October 2020 https://www.nyasatimes.com/mary-chilima-appointed-ambassador-against-girls-online-harassment-plan-malawi/ (accessed 2021)

National Telecom Regulatory Authority 'NTRA' 2020 https://www.tra.gov.eg/en/ (accessed 12 June 2021)

Netblocks 'Facebook and WhatsApp restricted in Cameroon on eve of election results' 21 October 2018 https://netblocks.org/reports/facebook-and-whatsapp-restricted-in-cameroon-on-eve-of-election-results-YkArL1yj (accessed 20 April 2021)

Nigerian Communications Commission 'NCC' 2022 https://www.ncc.gov.ng/ (accessed 2021)

NITDA 'NIGERIA DATA PROTECTION REGULATION 2019: IMPLEMENTATION FRAMEWORK' November 2020 https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf (accessed 7 February 2022)

OneTrust DataGuidance 'Democratic Republic of Congo – Data Protection Overview' August 2021 https://www.dataguidance.com/notes/democratic-republic-congo-data-protection-overview (accessed 8 August 2022)

Organic Act 26 of 2015 relating to the Fight Against Terrorism and the Suppression of Money Laundering (7 August 2015) https://www.bct.gov.tn/bct/siteprod/documents/Loi_2015_26_fr.pdf (accessed 8 February 2022)

Oussama, D; Tridane, M & Belaaouad, S 'Bibliographic study on child protection software for the internet' August 2018 https://www.researchgate.net/publication/346042166_Bibliographic_Study_on_Child_Protection_Software_for_the_Internet (accessed 9 February 2022)

POTRAZ 'Child online protection guidelines for children' http://www.potraz.gov.zw/wp-content/uploads/2015/05/POTRAZ_COP.pdf (accessed 9 February 2022)

President Chakwera 'State of the Nation' 4 September 2020 https://www.malawi.gov.mw/index.php/proud/news-and-media/speeches (accessed 9 February 2022)

President of the Republic Wade A and Prime Minister Soumar C 'Law on Cybercrime' 25 January 2008 https://ictpolicyafrica.org (accessed 8 February 2022)

Privacy International 'Kenyan court ruling on Huduma Namba Identity System: The good, the bad and the lessons' 24 February 2020 https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons#:~:text=Lessons%20%7C%20Privacy%20International-,Kenyan%20Court%20Ruling%20on%20Huduma%20Namba%20Identity%20System%3A%20the%20Good,the%20Bad%20and%20the%20Lessons&text=Kenya%20High%20Court%20fails%20to,to%20equality%20and%20non%2Ddiscrimination (accessed 9 February 2022)

Privacy International 'State of privacy Morocco' 26 January 2019 https://privacyinternational.org/state-privacy/1007/state-privacy-morocco (accessed 9 February 2022)

Refworld 'Freedom on the Net 2012 – Tunisia' 25 September 2012 https://www.refworld.org/docid/5062e897c.html (accessed 9 February 2022)

Raab, C & Goold, B 'Protecting information privacy' (2011) https://www.equalityhumanrights.com/sites/default/files/research-report-69-protecting-information-privacy.pdf (accessed 10 February 2022)

RÉPUBLIQUE DU BÉNIN, Loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin (2018) https://apdp.bj/wp-content/uploads/2019/04/CODE-DU-NUMERIQUE-DU-BENIN_2018-version-APDP.pdf (accessed 9 February 2022)

République du Sénégal Validation of a National Plan for the Protection of Children on the Internet (French) 28 February 2018 https://tinyurl.com/3ruze8xe (accessed 9 February 2022)

Sasu, DD 'Regional distribution of households owning computers in Ghana 2018' 5 January 2021 https://www.statista.com/statistics/1139237/households-owning-computers-in-ghana-by-region/ (accessed 23 April 2021)

Sator, A 'DATA PROTECTION AND CYBERSECURITY LAWS IN ALGERIA' 5 March 2021 https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-

protection-and-cyber-security-laws/algeria (accessed 7 February 2022)

Scott, B 'Nigeria: General principles and requirements for advertising in Nigeria' 6 January 2020 https://www.mondaq.com/nigeria/advertising-marketing-branding/880690/general-principles-and-requirements-for-advertising-in-nigeria (accessed 21 April 2021)

Sénégal Emergent 'Stratégie Sénégal Numérique 2016-2025' October 2016 https://tinyurl.com/f4t6z63s (accessed 2 February 2022)

Sibidla, T 'Data protection and privacy regulation: A roundup of developments in Africa in 2021' https://www.werksmans.com/legal-updates-and-opinions/data-protection-and-privacy-regulation-a-roundup-of-developments-in-africa-in-2021/ (accessed 7 February 2022)

Singh, A 'Why POPIA is about rights – not just compliance" Alt-Advisory 23 June 2020 https://altadvisory.africa/2020/06/23/why-popia-is-about-rights-not-just-compliance/ (accessed 25 November 2020)

Sonjica, N 'Limpopo pupil allegedly commits suicide after being bullied at school' Sunday Times 13 April 2021 https://www.timeslive.co.za/news/south-africa/2021-04-13-limpopo-pupil-allegedly-commits-suicide-after-being-bullied-at-school/ (accessed 9 February 2022)

South African Law Reform Commission 'Sexual Offences (Pornography and Children) Discussion Paper 149' April 2019 https://www.ellipsis.co.za/wp-content/uploads/2015/11/dp149-prj107-SexualOffences-PornographyChildren2019.pdf (accessed 9 February 2022)

Statista 'Digital population in South Africa as of January 2020' (2020) https://www.statista.com/statistics/685134/south-africa-digital-population/ (accessed 2 February 2022)

Statistics South Africa 'General Household Survey' 2018 http://www.statssa.gov.za/publications/P0318/P03182018.pdf (accessed 2 February 2022)

Stratégie nationale 'Sénégal Numérique 2016 – 2025'; Plan d'actions actualisé Actualisation de la stratégie Sénégal numérique 2025 (SN2025) https://tinyurl.com/2hvs64c (accessed 9 February 2022)

'Suicide game "Blue Whale Challenge" allegedly kills two Moroccan children' Moroccoworldnews 29 December 2017 https://www.moroccoworldnews.com/2017/12/237428/blue-whale-kills-moroccan-children/ (accessed 9 February 2022)

Taboor, N 'Malawi puts more focus on protecting children on the Internet' 7 November 2017 iAfrikan https://www.iafrikan.com/2017/11/07/malawi-child-online-protection-cop/ (accessed 7 February 2022)

Tanzanian Commission for Human Rights and Good Governance et al 'Voices From Tanzania – case studies on Business and Human Rights' 1 (2019) https://ipisresearch.be/wp-content/uploads/2019/04/1904-Voices-from-Tanzania-Business-and-Human-Rights-WEB.pdf (accessed 9 February 2022)

Taye, B & Teshome, R 'Privacy and personal data protection in Ethiopia' CIPESA September 2018 https://cipesa.org/?wpfb_dl=379 (accessed 7 February 2022)

Taye, B 'Internet censorship in Tanzania: the price of free expression online keeps getting higher' 22 October 2020 https://www.accessnow.org/internet-censorship-in-tanzania/ (accessed 9 February 2022)

The Presidency 'Commencement of certain sections of the Protection of Personal Information Act, 2013' 2020 http://www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013 (accessed 7 February 2022)

The Youth Parliament of the Democratic Republic of Congo http://jeunescongo.e-monsite.com/ (accessed 22 April 2021)

Toussi, S 'Building a robust data protection regime in Senegal' 10 March 2020 https://tinyurl.com/2s9dk6s2 (accessed 7 February 2022)

Tsandzana, D 'New privacy law in Mozambique threatens freedom of expression, activists say' Global Voices 16 January 2020 https://globalvoices.org/2020/01/16/new-privacy-law-in-mozambique-threatens-freedom-of-expression-activists-say/ (7 February 2022)

TZ-Cert 'TZ-Cert profile' https://www.tzcert.go.tz/about-us/tz-cert-profile/ (accessed 9 February 2022)

UK Safer Internet Centre 'Age restrictions on social media services' 25 April 2018 https://www.saferinternet.org.uk/blog/age-restrictions-social-media-services (accessed 21 April 2021)

UNICEF 'Children in a digital world' 2017 https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf (accessed 9 February 2022)

UNICEF 'Ghana: Child online protection' (2018) https://www.unicef.org/ghana/child-online-protection (accessed 9 April 2021)

UNICEF 'Zimbabwe: Child rights and business guidance for Chinese companies operating in zimbabwe' https://www.unicef.cn/en/csr/zimbabwe (accessed 2021)

United Nations 'Special Rapporteur on the right to privacy' 2021 https://www.ohchr.org/en/issues/privacy/sr/

pages/srprivacyindex.aspx#:~:text=Current%20mandate%20holder&text=Joseph%20Cannataci%20of%20Malta%20as,on%20the%20right%20to%20privacy (accessed 2021)

Unwanted Witness 'One year on, what has Uganda's Data Protection Law changed?' Privacy International 3 March 2020 https://privacyinternational.org/news-analysis/3385/one-year-what-has-ugandas-data-protection-law-changed (accessed 7 February 2022)

Wanyama, E 'Tanzania entrenches digital rights repression amidst Covid-19 denialism and a looming election' CIPESA 19 August 2020 https://cipesa.org/2020/08/tanzania-entrenches-digital-rights-repression-amidst-covid-19-denialism-and-a-looming-election/ (accessed 7 February 2022)

World Bank 'Individuals using the Internet (% of population) – Mauritius' 2020 https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=MU

York, J & Greene, D 'Proposed new internet law in Mauritius raises serious human rights concerns' Electronic Frontier Foundation 20 April 2021 https://www.eff.org/deeplinks/2021/04/proposed-new-internet-law-mauritius-raises-serious-human-rights-concerns (accessed 7 February 2022)

Youssef, D 'Is Censorship coming back to Tunisia? Court order bans 'Blue Whale' online game' Advox: Global Voices 14 March 2018 https://advox.globalvoices.org/2018/03/14/is-censorship-coming-back-to-tunisia-court-order-bans-blue-whale-online-game/ (accessed 9 February 2022)

Zimbabwe Human Rights NGO Forum, the Digital Society of Zimbabwe, the International Human Rights Clinic at Harvard Law School and Privacy International 'Stakeholder Report Universal Periodic Review 26th Session – Zimbabwe: The Rights to Privacy in Zimbabwe' March 2016 https://hrp.law.harvard.edu/wp-content/uploads/2016/04/zimbabwe_upr2016.pdf (accessed 8 February 2022)

Zimehifadhiwa 'JAMHURI YA MUUNGANO WA TANZANIA MAMLAKA YA MAWASILIANO TANZANIA TAASISI YENYE VIWANGO VYA ISO 9001: 2015' 2022 https://www.tcra.go.tz/ (accessed 12 June 2021)

Zongwe, DP; Butedi, F & and Clément, PM 'Update: Overview of the legal system of the Democratic Republic of the Congo (DRC) and research' July/August 2020 New York University School of Law https://www.nyulawglobal.org/globalex/Democratic_Republic_Congo1.html (accessed 15 April 2021)

Other sources

African Charter on the Rights and Welfare of the Child (1990)

UN Convention on the Rights of the Child (1989)

African Union Convention on Cybersecurity (2014)

CRC Committee General Comment no 25 (CRC/C/GC/25 of March 2021)

ACERWC General Comment 7: article 27 of the ACRWC on sexual exploitation (March 2021)

Appendix: Questionnaire on children's right to privacy and digital technology in Africa for the country reports

1 Protection of children's right to privacy

- Are there laws which directly confront children's right to privacy?
- Is the right to privacy of children (or all persons) constitutionally protected?
- Is there a common law basis for the protection of children's (or people's) right to privacy?
- Is there case law illuminating the scope of privacy rights and permissible limitations of this right?
- If there is a legal framework/case law on right to privacy, does it discuss its applicability and scope in the context of right to privacy online? It this different from offline protection of privacy (for example, letters)?
- Are children's participatory rights and right to autonomy properly recognised in the state?

2 Overarching regulatory environment

- Has the country ratified the African Union Convention on Cyber Security and Personal Data? Are there plans to do so?
- Depending on whether the country follows a monist/dualist approach, has the above Convention been translated into national law and if yes, how has the content of the Convention been adapted?

3 Which body/bodies play a regulatory role with respect to:

- Regulating the internet/ISPs?
- Regulating access to information?
- Regulating data protection generally? Does this cover the state as well as the private sector?
- Regulating the protection of personal information?
- Do privacy and data protection legislation, including surveillance-related legislation, include express child-sensitive provisions and safeguards? If not in specific privacy and data protection regulation, does the children's rights law (for example, a Children's Act) of the country provide such protection?
- Responding to threats or breaches of online child protection, for example online child abuse? Is there a national framework or policy concerning the protection of children from harm in the digital environment?
- What safeguards exist on filtering and monitoring? Are transparency statistics on which content is filtered and blocked, what has been monitored, and their error rates published? What steps are in place to avoid child profiling, for example, in relation to membership of specific groups such as extremist groups?
- What legislation exists under which prosecutions could be brought (for example, child pornography laws/public indecency laws/censorship laws) and is this legislation sufficiently modernised to accommodate online forms of display or distribution of such materials? What is the protocol for the reporting of illegal content (for example, child sexual abuse materials) found on the internet, focusing in particular on the role of internet service providers who might host such material?
- What protocols/laws/structures exist to combat the online radicalisation of children through digital media, namely their solicitation into joining extremist or armed groups?
- What structures exist to combat the digital promotion of racism, sexism, ethnic intolerance, hate speech, cyberbullying, xenophobia or anti LGBTQI sentiments? Under what circumstances can information related to children's online activity be demanded of the private sector by state authorities?
- What measures are in place to ensure that the use of algorithms does not result in discrimination against certain children? Is civil or criminal liability for violation possible?
- In criminal and civil law, is it possible to hold multi-national or transnational corporations

accountable and to obtain remedies for abuses that occur in the context of businesses' global operations?
- What seems to be the general view on end-to-end encryption relating to services affecting children (including social media) in the state concerned?
- Does the state require that the business sector (internet service providers, content producers, purveyors of digital goods) must undertake child rights due diligence and conduct child rights impact assessments?

4 Advertising

- Are there measures (standards, regulations) in place concerning the processing of children's personal data for advertising purposes? Is this protection child specific? At what age or ages does this protection apply?
- Are children as consumers protected against age related discrimination in relation to access to, inter alia, facilities, services, information and goods? Are their known profiling and personalisation techniques at stake in the country which allow service providers to restrict access to certain services to specific (groups of) consumers, such as children?
- Are there measures in place to protect children in the state from exposure to economic exploitation through embedded ads, privacy-invasive practices, age-inappropriate content, as well as the exploitation of their incredulity and inexperience resulting in economic risks such as overspending or online fraudulent transactions? Is this through advertising and marketing standards, codes of conduct, or how it is achieved? To whom is authority for oversight awarded? What remedies or redress mechanisms are in place?

5 Games/play

- Are there safeguards in place to ensure that digital games for children do not promote violence, or the sexualisation of girls or boys, contain age inappropriate content, or reinforce gender and disability stereotypes?

6 Education

- What steps has the state concerned taken to promote children's digital literacy, either as part of school curricula or in other forms of public awareness programmes (for example, on TV or Radio)?
- Is there in the state party easily accessible and child-friendly information on how to report and complain about interferences with privacy rights and how to seek redress available? Are there effective operational-level grievance mechanisms operated by internet service and content providers for children who may be adversely impacted via rights violations? Do children have access to independent complaints procedures (data protection authorities, children's rights commissioners, or ombudspersons) and to the courts with necessary legal and other assistance when their rights appear to have been violated?

7 Consent

- How is children's consent to terms and conditions approached in the jurisdiction generally (when is parental involvement required)? Is this different for online consent?
- Are privacy law and policies child friendly and do they consider for the varying evolving capacities of child?
- Are there any limitations of what images or material parents may share of their children online (sharenting)?

8 Participation

- To what extent have children been (or are being) consulted in the formulation of policy/standards or responses to their online protection? Please give the necessary detail (how, in what format, via which structure etc)
- ITU guidelines requires 'internal and external expertise and consult with key stakeholders, including children, on child online safety mechanisms to obtain ongoing feedback and guidance on company approaches'. Is this in place? Or from time to time does it occur?