Module 4

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

ISBN 978-0-9935214-1-6
Published by Media Legal Defence Initiative: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in April 2024

TABLE OF CONTENTS

MODULE 4

DATA PRIVACY AND DATA PROTECTION

- **The right to privacy and data protection is a growing concern due to increasing data flows and the resulting need for the protection of personal information.**
- **In the African context, there has been progress with the passage of several new data protection laws in recent years, and the coming into force of the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention).**
- **The right to be forgotten continues to be an issue of contestation through the courts, although case law in Africa is limited.**
- **Nevertheless, attacks against encryption and anonymity continue, and there are many new threats to privacy and data protection including the expansion of surveillance capabilities and the growth of artificial intelligence (AI).**
- **Journalistic activity warrants particular protections from threats to encryption as well as communications surveillance by both state and private actors because of the special risks this poses for freedom of expression due to the potential disclosure of confidential sources and the risk of a chilling effect on media freedom.**

1. INTRODUCTION

The right to privacy and the concomitant requirement to protect personal information has become increasingly relevant in the information age. As access to the internet has expanded and many parts of public and private life have become increasingly digitised, there has been a sharp increase in online information-sharing and data collection, with the associated risk that this information can be accessed and abused by hostile actors. At the same time, legislative developments have failed to keep pace and adequately protect personal information. However, in recent years, the passing of data protection legislation by many African states, as well as the development of guidelines and instruments by regional and continental bodies, have provided some protections to remedy and vindicate the privacy rights of African peoples.

This module focuses on the right to privacy in the digital age in Africa by evaluating the state of data protection, the related concepts of the 'right to be forgotten' and encryption assesses the growing risks of government and commercial surveillance as well as the emerging challenges of the use of artificial intelligence (AI) to perpetrate privacy violations, and sets out emerging principles and safeguards in this rapidly advancing digital environment.

2. THE RIGHT TO PRIVACY

Around the world, there is an increasing recognition that the right to privacy is vital both in itself and due to its role in facilitating the right to freedom of expression. For instance, the right to privacy allows individuals to share views anonymously in circumstances where they may face repression or discrimination for those views; it also allows whistle-blowers to make protected disclosures and enables journalists and activists to communicate securely beyond the reach of unlawful government interception. It is also an inherent part of the right to dignity.

The right to privacy is contained in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which provides:

> "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> (2) Everyone has the right to the protection of the law against such interference or attacks."

Although the right to privacy is not explicitly contained in the African Charter on Human and Peoples' Rights (African Charter), article 9 of the Charter does encode protections for the right to receive information and express opinions:

> "1. Every individual shall have the right to receive information.
> 2. Every individual shall have the right to express and disseminate his opinions within the law."

These, in addition to the African Charter's protections for freedom against discrimination, liberty and security, freedom of assembly, health, and others, have prompted the argument that the implicit right to privacy should be 'read into' the African Charter as an inalienable component of those other rights.[1]

'Reading in' the right to privacy: the example of India

While this approach has not been tested in relation to the African Charter, it would follow the approach of the Supreme Court of India in its 2017 ruling that the right to privacy is protected as an intrinsic part of the right to life and personal liberty, and as part of the fundamental freedoms guaranteed by Part III of the Constitution of India.[2] As such, although the Constitution of India does not expressly contain a right to privacy, the right can nevertheless be read when considered in the context of the other rights and freedoms that are constitutionally guaranteed.

[1] Ayalew, 'Untrodden Paths Towards the Right to Privacy in the Digital Era under African Human Rights Law' *12 International Data Privacy Law 1* (2022) (accessible here).
[2] *Justice K.S. Puttaswamy and Another v Union of India and Others*, Petition No. 494/2012 (2017) (accessible here).

The right to privacy of children is, however, explicitly contained in other regional and continental instruments. For example, article 10 of the African Charter on the Rights and Welfare of the Child (ACRWC) provides that:

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

The revised 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa, adopted by the African Commission on Human and Peoples' Rights (ACHPR), also explicitly acknowledges the right to privacy and calls on states to provide extensive protections for privacy and personal information.[3] Moreover, all but one African state guarantees this right under their domestic constitutions.[4]

As with the right to freedom of expression, a limitation of the right to privacy must comply with the three-part test for a justifiable limitation. According to the South African Constitutional Court:[5]

> "A very high level of protection is given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual's activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation."

Set out below, we consider specific aspects of the right to privacy and the impact of the internet on the enjoyment of this right.

3. DATA PROTECTION

Data protection is one of the primary ways through which the right to privacy is given effect. At least 36 African states have so far enacted data protection laws, and more are in the process of doing so.[6] In addition to giving effect to the right to privacy, data protection legislation also facilitates trade among states, as many data protection laws restrict cross-border data transfers in circumstances where the state receiving the information does not provide an adequate level of data protection. Framed more positively, data protection laws enable the regulated transfer of personal information across borders where both jurisdictions have put in place adequate data protection laws and procedures to protect data subjects' rights.

---

[3] ACHRP, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019' (2019) (accessible here) at Principles 40-42.
[4] ALT Advisory, 'Data Protection Africa,' (accessible here).
[5] *NM and Others v Smith and Others*, [2007] ZACC 6 (accessible here) at para 33, citing with approval *Bernstein and Others v Bester NO and Others*, [1996] ZACC 2 (accessible here) at para 77.
[6] See https://dataprotection.africa/ for more information.

3.1. Key data protection principles

Data protection laws are aimed at protecting and safeguarding the processing of personal information (also sometimes called personal data). Personal information is typically defined as any information relating to an identified or identifiable natural person — i.e. the data subject — by which the data subject can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity. A data controller, also sometimes called the responsible party, can typically be either a public or private body and is the person or entity responsible for processing personal information about the data subject.

Key data protection principles

Most comprehensive data protection laws in Africa make provision for a core set of principles which can be summarised as follows:[7]

- Personal information must be processed fairly and lawfully and must not be processed unless the stipulated conditions are met.
- Personal information must be obtained for a specified purpose (or purposes) and must not be further processed in any manner incompatible with that purpose.
- Personal data must be adequate, relevant, and not excessive in relation to the purpose (or purposes) for which it was collected.
- Personal information must be accurate and, where necessary, kept up to date.
- Personal information must not be kept for longer than is necessary for the purpose.
- Personal information must be processed in accordance with the rights of data subjects provided for under the data protection law.
- The data controller must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to another country that does not ensure an adequate level of protection for the rights and freedoms of data subjects.

In addition, most data protection laws establish a regulatory body to monitor and enforce the provisions of the law: this type of regulatory body is often referred to as a data protection authority (DPA).

3.2. International law standards

The United Nations Special Rapporteur (UNSR) on the Right to Privacy released a report in 2022 providing an in-depth analysis of the principles of legality, lawfulness and legitimacy, consent, transparency, purpose, fairness, proportionality, minimisation, quality, responsibility,

[7] Information Commissioner's Office, 'A guide to the data protection principles' (accessible here).

and security in the context of data protection legislation, which serves as a seminal guide for the development and harmonisation of data protection regulations around the world.[8]

In relation to the protection of personal information, General Comment No. 16 on Article 17 of the ICCPR (General Comment No. 16) provides as follows:[9]

> "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."

In 2023, in response to the rapid and widespread collection of personal information ostensibly to combat the COVID-19 pandemic from 2020-2022, the UNSR on Privacy released a report elaborating on the implementation of the principles of purpose limitation, deletion of data and demonstrated or proactive accountability in the processing of personal data collected by public entities in the context of the pandemic.[10]

3.3. Regional law standards

There are several African regional instruments that deal with data protection:

- **The African Union (AU) Convention on Cyber Security and Personal Data Protection 2014**[11] (the Malabo Convention): This instrument, aimed at a continental level, includes provisions relating to data protection, e-transactions, cybercrimes and cybersecurity. The provisions relating to data protection are contained in Chapter II and contain the conditions for the lawful processing of personal information, as well as the rights afforded to data subjects. After finally receiving ratification from the required 15th state, the Malabo Convention came into force in 2023.[12]

[8] UNSR on Privacy, 'Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms' (2022) (accessible here).
[9] UNHCHR, 'CCPR General Comment No. 16: Article 17 (Right to Privacy)' (1988) (accessible here) at para 10.
[10] UNSR on Privacy, 'A/HRC/52/37: Implementation of the principles of purpose limitation, deletion of data and demonstrated or proactive accountability in the processing of personal data collected by public entities in the context of the COVID-19 pandemic - Report of the Special Rapporteur on the right to privacy' (2023) (accessible here).
[11] AU, 'African Union Convention on Cyber Security and Personal Data Protection' (2014) (accessible here).
[12] ALT Advisory, 'Africa: AU's Malabo Convention set to enter force after nine years' (2023) (accessible here).

- **EAC Legal Framework for Cyberlaws 2008**[13] (EAC Legal Framework): This instrument covers topics relating to data protection, electronic commerce, data security and consumer protection. It is not intended to be a model law but instead provides guidance and recommendations to states to inform the development of their laws. Data protection is dealt with briefly in paragraph 2.5 of the EAC Legal Framework, as part of Phase I which was adopted by the EAC Council of Ministers in 2010.[14]

- **Supplementary Act on Personal Data Protection within ECOWAS 2010**[15] (ECOWAS Supplementary Act): This instrument is designed to be directly transposed into a domestic context among West African states and provides in detail the conditions for the lawful processing of personal information and the rights of data subjects. Importantly, it is also legally binding on ECOWAS States. ECOWAS also adopted the Directive on Fighting Cyber Crime in 2011 in an effort to harmonise member states' cybercrime legislation.

- **SADC Data Protection Model Law 2013**[16] (SADC Model Law): This is a model law that can be adapted into domestic contexts among southern African states. It seeks to ensure the harmonisation of information and communications technologies (ICT) policies and recognises that ICT developments impact the protection of personal data, including in government and commercial activities. It also deals with whistle-blowing, by providing that the data protection authority must establish rules to govern the whistleblowing system that preserve data protection principles, including the principles of fairness, lawfulness, purpose specification, proportionality, and openness.

In addition to giving effect to the right to privacy, data protection laws also often further facilitate a right of access to information, by providing for data subjects to request, and be given access to, the information being held about them by a controller. This mechanism can enable data subjects to determine whether their personal information is being processed in line with applicable data protection laws and whether their rights are being upheld.

Mapping the state of data protection in Africa

Given the importance of data protection legislation in protecting the right to privacy in the digital age, as well as the rapid progression of legislation and regulation in this area, it can be hard to keep up to date with the state of data protection in Africa. Data protection is an open, online resource that aims to provide a detailed analysis of the governance of data protection across the continent, mapping and analysing the legislation in place in all 55 member states of the African Union.

As of February 2024, it notes that 36 out of the 55 AU-recognised states have passed data protection legislation, with three draft bills also being under consideration.

[13] EAC, 'EAC Legal Framework for Cyberlaws' (20228) (accessible here).
[14] UNCTAD, 'Harmonizing Cyberlaws and Regulations: The experience of the East African Community' (2012) (accessible here).
[15] ECOWAS, 'Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWS' (2010) (accessible here).
[16] HIPSSA, 'Data Protection: SADC Model Law' (2013) (accessible here).

3.4. Emerging challenges to data protection

As more states across the continent have passed data protection legislation, so too have the risks and challenges of regulating and protecting privacy in the digital age become more complex. Many states, particularly those in West Africa, passed their laws some time ago,[17] raising concerns that they may no longer be suited to the challenges of the modern age. In South Africa, for example, the Protection of Personal Information Act was passed in 2013 but only came into effect in July 2020 with a further grace period given for full compliance. This has raised concerns among critics that the Act already requires amendments to stay up to date with new issues such as AI.[18]

In addition, the enforcement challenges of these many new data protection laws have become increasingly apparent. For example, research has found that 14 countries' laws provide for the data protection authority to be established within or to receive instructions from another public body, such as a government ministry, raising questions about regulatory independence.[19] 11 countries were found not to have adequate protections in place to prevent the undue removal of members of the Authority for political or other reasons.[20]

Enforcement challenges: example from Kenya

Many data protection authorities across the content have struggled to meaningfully hold accountable violators of data protection legislation, particularly powerful multinational corporations.

For example, in 2023, Tools for Humanity piloted a new cryptocurrency campaign called Worldcoin that paid people a small sum of money in the cryptocurrency to have their biometric data collected, resulting in thousands taking up the opportunity,[21] with very little information about how the data would be used. In May, **Kenya's** Office of the Data Protection Commissioner (OPDC) ordered the company to halt processing,[22] an order which was reportedly ignored. The company finally stopped data collection only when, in August, the Ministry of the Interior ordered the suspension of Worldcoin's operations in the country, citing data protection concerns.[23] The OPDC subsequently launched litigation against Tools for Humanity in the High Court.[24]

This demonstrates the challenges data protection authorities face in holding these powerful international companies to account.

[17] Data Protection Africa, 'Standing Alone: The Independence of African Data Protection Authorities' (2024) (accessible here).
[18] IT Web, 'POPIA principles must align with AI governance, say experts,' (2023) (accessible here).
[19] See above n 17.
[20] *Id*.
[21] Njenga, Schmitz, 'Worldcoin: Thousands flock KICC to have eyeballs scanned for Ksh.7k' (2023) (accessible here).
[22] TechCrunch, 'Worldcoin ignored initial order to stop iris scans in Kenya, records show' (2023) (accessible here).
[23] Kenya Ministry of Interior, 'Statement on Worldcoin' (2023) (accessible here).
[24] See above n 22.

Another barrier to the advancement of data protection on the continent is the limited scope of data protection laws, with many containing extensive national security or private sector exemptions that undermine their efficacy. In this regard, it is also important to note the track record on the continent of national security justifications being abused, as detailed in Module 9 in this series.

4. THE RIGHT TO BE FORGOTTEN

4.1. Definitions

The 'right to be forgotten'[25] — which can also be described as 'the right to erasure' or 'the right to be de-listed' — entails the right of a data subject to request that commercial search engines or other websites that gather or publish personal information remove links to the personal information relating to the subject on request. The issue is highly contextual and often fraught because it usually involves a complicated balancing of public and individual interests. The right to be forgotten progresses from the right of data subjects contained in many data protection laws that personal information held about a person should be erased in circumstances in which it is inadequate, irrelevant, no longer relevant, or excessive in relation to purposes for which it was collected. However, in some cases, there may be a valid justification for keeping the information in the public domain because it is in the public interest.

4.2. A growing body of jurisprudence

Establishing the right to be forgotten in the CJEU

The right to be forgotten was established in a 2014 ruling of the Court of Justice of the European Union (CJEU) in the case of *Google Spain v Gonzalez*.[26] Mr Gonzalez, a Spanish national, lodged a complaint in 2010 with the Spanish information regulator. The cause of Mr Gonzalez's complaint was that any search for his name on Google's search engine prominently displayed old news articles about debt proceedings against him. Mr Gonzalez requested that the personal data relating to him, which was over a decade old, be removed or concealed because the proceedings had been fully resolved and the reference to him was now irrelevant.

The CJEU upheld the claim, relying on the **European Union** data protection law in effect at the time. The CJEU noted that the very display of personal information on a search results page constitutes the processing of the information[27] and that there was no reason why a search engine should not be subject to the obligations and guarantees laid out under the law.[28] Further, it was noted that the processing of personal information carried out by a

[25] For more on this topic see Media Defence 'Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa' (accessible here).
[26] *Google Spain SL and Another v Agencia Española de Protección de Datos (AEPD) and Another*, Case No. C-131/12, (2014) (accessible here).
[27] *Id* at para 57.
[28] *Id* at para 58.

search engine can significantly affect the fundamental rights to privacy and the protection of personal data when a search is carried out of a person's name, as it enables any internet user to establish a profile of the person.[29] According to the CJEU, the effect of the interference "is heightened taking into account the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous."[30]

With regard to de-listing, the CJEU held that the removal of links from the list of results could, depending on the information at issue, have effects on the legitimate interests of internet users seeking access to that information.[31] This would require a fair balance to be struck between those interests and the data subject's fundamental rights, taking into account the nature of the information, its sensitivity to the data subject's private life, and the interest of the public in having that information, which may vary according to the role played by the data subject in public life.[32]

The CJEU went on to hold that a data subject is permitted to request that information about them be removed from search results where, having regard to all the circumstances, the information appears to be inadequate, irrelevant or no longer relevant, or excessive in relation to purposes of the processing carried out by the operator of the search engine.[33] In such circumstances, the information and links concerned in the list of results must be erased.[34]

Since then, the jurisprudence on the right to be forgotten has developed significantly, particularly in the EU. See the European Court of Human Rights' Guide to the Case Law on Data Protection for some examples of the nuances that have since been developed.

The right to be forgotten has also been recognised in domestic contexts, although not as yet in sub-Saharan Africa. However, it has been recognised in South America in, for example, the State Court of Appeals of São Paulo, **Brazil**.[35] Of relevance to the media, the Supreme Court of Chile, in 2019, made an order requiring several digital media outlets to update the information they had published about a person involved in a criminal case in order to achieve a balance between the right to information that was in the public interest and the right to honour.[36]

4.3. Non-consensual dissemination of intimate images (NCII)

[29] *Id* at para 80.
[30] *Id.*
[31] *Id* at para 81.
[32] *Id.*
[33] *Id* at para 94.
[34] *Id* at para 94.
[35] *De Queiroz v. Google Brasil Internet Ltd.* Case No. 0004144-77.2015.8.26.0297 (2016) (accessible here).
[36] *Surgeon v. Court of Appeals of Santiago*, Case No. RoI No. 1279-2019 (2019) (accessible here).

A growing body of case law is also beginning to recognise the right to be forgotten in cases of the non-consensual sharing of intimate images (NCII), such as *X v. Union of India* and *X v. YouTube*, both in the High Court of Delhi in India.

Litigating 'Non-Consensual Distribution of Images: Kenya

In 2016, the High Court of Kenya determined a case, *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* (2016), involving the non-consensual distribution of the petitioner's nude photographs by an ex-boyfriend, resulting in her dethronement as Miss World Kenya 2015.[37]

The Court held that Ebrahim had a legitimate expectation of privacy, that she did not waive her right to protection of privacy by taking nude photographs, and did not consent to their dissemination to third parties, and as such, her right to privacy under Article 31 of the Constitution of Kenya had been violated. It further ordered the ex-boyfriend to pay damages and directed the organisers of the Miss World Kenya not to publish the nude photographs in their possession.

The case provides valuable insights into the 'reasonable expectation of privacy,' whether images are obtained in an intrusive manner, and whether the presence of illegalities may invalidate a right to privacy claim.[38]

4.3. Limits on the right to be forgotten

As jurisprudence around the world has developed, lines have begun to be drawn identifying the limits of the right to be forgotten. In 2017, the CJEU declined to uphold a request to erase, anonymise, or block any data linking the plaintiff to the liquidation of his company contained in the companies register in the case of *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni.*[39] The CJEU held that in light of the range of possible legitimate uses for data in company registers and the different limitation periods applicable to such records, it was impossible to identify a suitable maximum retention period. Accordingly, the CJEU declined to find that there is a general right to be forgotten from public company registers.

Furthermore, other jurisdictions have refused to uphold a right to be forgotten against search engines:

- In **Brazil**, for example, it was held that search engines cannot be compelled to remove search results relating to a specific term or expression.[40]

[37] *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* [2016] eKLR (accessible here).
[38] For further information on the use of the 'tort of invasion of privacy,' the public disclosure of embarrassing facts, breaches of the torts of breach of confidence and intentional infliction of mental distress, see: *Jane Doe 464533 v. D. (N.)* (accessible here); see also: Equality Project 'Technologically-Facilitated Violence: Non-Consensual Distribution of Intimate Images Case Law' (2019) (accessible here).
[39] Case No. C-385-15, (2017) (accessible here).
[40] *Ministra Nancy Andrighi v Google Brasil Internet Ltd and Others*, 2011/0307909-6, (2012) (accessible here).

- Similarly, the Supreme Court of **Japan** declined to enforce the right to be forgotten against Google, finding that deletion "can be allowed only when the value of privacy protection significantly outweighs that of information disclosure".[41]

According to the Global Principles of Freedom of Expression and Privacy (Global Principles),[42] the right — to the extent that it is recognised in a particular jurisdiction — should be limited to the right of individuals under data protection law to request search engines to delist inaccurate or out-of-date search results produced on the basis of a search for their name[43] and should be limited in scope to the domain name corresponding to the country where the right is recognised and the individual has established substantial damage.[44] It states further that de-listing requests should be subject to ultimate adjudication by a court or independent adjudicatory body with relevant expertise in freedom of expression and data protection law.[45]

5. ENCRYPTION AND ANONYMITY ON THE INTERNET[46]

5.1. Definition

Encryption refers to a mathematical process of converting messages, information or data into a form unreadable by anyone except the intended recipient, and in doing so protecting the confidentiality and integrity of content against third-party access or manipulation.[47] With "public key encryption" — the dominant form of end-to-end security for data in transit — the sender uses the recipient's public key to encrypt the message and its attachments, and the recipient uses her or his own private key to decrypt them.[48] It is also possible to encrypt data at rest that is stored on one's device, such as a laptop or hard drive.[49]

Anonymity can be defined either as acting or communicating without using or presenting one's name or identity, as acting or communicating in a way that protects the determination of one's name or identity or as using an invented or assumed name that may not necessarily be associated with one's legal or customary identity.[50] Anonymity may be distinguished from pseudo-anonymity: the former refers to taking no name at all, while the latter refers to taking an assumed name.[51]

---

[41] The Japan Times, 'Top court rejects 'right to be forgotten' demand' (2017) (accessible here).
[42] Article19 'The Global Principles' (accessible here). The Global Principles were developed by civil society, led by ARTICLE19, in cooperation with high-level experts from around the world.
[43] *Id* at Principle 18(1).
[44] *Id* at Principle 18(4).
[45] *Id* at Principle 18(2).
[46] For more on this topic see Media Defence 'Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa' (accessible here).
[47] Report of the UNSR on Freedom of Expression, 'Report on anonymity, encryption and the human rights framework', A/HRC/29/32, (2015) (accessible here) at para 7. For further discussion and resources, see UCI Law International Justice Clinic, 'Selected references: Unofficial companion report to Report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and freedom of expression' (accessible here).
[48] *Id*.
[49] *Id.*
[50] Electronic Frontier Foundation, 'Anonymity and encryption' (2015) (accessible here) at p 3.
[51] *Id*.

5.2. Importance of freedom of expression

Encryption and anonymity are necessary tools for the full enjoyment of digital rights and deserve protection by virtue of the critical role that they play in securing the rights to freedom of expression and privacy. As described by the UNSR on FreeEX:[52]

> "Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also a society that does not tolerate unconventional opinions or expression."

Encryption and anonymity are especially useful for the development and sharing of opinions online, particularly in circumstances where a person fears that their communications may be subject to interference or attack by state or non-state actors. These are therefore specific technologies through which individuals may exercise their rights, and are particularly important for journalists communicating online to be protected from surveillance and to maintain the confidentiality of journalistic sources. Accordingly, under international human rights law, restrictions on encryption and anonymity must meet the three-part test to justify the restriction.

5.4. Balancing security with freedom of expression

According to the UNSR on FreeEX, while encryption and anonymity may have the potential to frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public safety justifications to support any restrictions or to identify situations where the restriction has been necessary to achieve a legitimate goal.[53] Outright prohibitions on the individual use of encryption technology disproportionately restrict the right to freedom of expression as they deprive all online users in a particular jurisdiction of the right to carve out a space for opinion and expression, without any particular claim of the use of encryption being for unlawful ends.[54] Likewise, state regulation of encryption may be tantamount to a ban, for example, through requiring licences for encryption use, setting weak technical standards for encryption, or controlling the import and export of encryption tools.[55]

The use of encryption and anonymity by journalists

[52] See above UNSR Report on Anonymity and Encryption n 47 at para 12.
[53] *Id* at para 36.
[54] *Id* at para 40.
[55] *Id* at para 41.

In the 2015 case of *Federal Prosecutor v Soleyana Shimeles Gebremariam and others (Zone 9 Bloggers)* in **Ethiopia**, in which nine bloggers were charged with planning, preparing, conspiring, and inciting to execute terrorism, it is notable that the prosecutor in the case cited the bloggers' use of encryption tools to protect the confidentiality of their data as evidence that they were undertaking covert acts against the government. Ultimately, all charges were either dropped or the defendants were acquitted due to a lack of evidence.[56]

Since 2015, awareness and understanding of the use of encryption tools has advanced, and it is, in most cases, no longer seen as an inherent indication of having something to hide. However, journalists continue to face many challenges in using fully secure and protected encryption and anonymity tools in practice, with constant threats from law enforcement agencies seeking 'back doors' into such tools.

Regardless, the principle of the confidentiality of journalistic sources is well established in case law, including in Africa. In the 2023 case of *Mazetti Management Services. amaBhungane Centre for Investigative Journalism* in **South Africa** the High Court set aside an interim injunction ordering a media organisation to return documents in its possession and confirmed that the confidentiality of sources is a key and important feature of investigative journalism.[57] An *amicus curiae* in the case made submissions on the importance of the confidentiality of journalistic sources as set out in international human rights law.

The UNSR on FreeEX has, therefore, called on states to promote strong encryption and anonymity, and noted that decryption orders should only be permissible when they result from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (not to a mass of people), and subject to a judicial warrant and the protection of due process rights.[58]

The 2019 ACHPR Declaration of Principles on Freedom of Expression and Access to Information likewise provides that states should not adopt laws or other measures prohibiting or weakening encryption, including backdoors or key escrows unless such measures are justifiable and compatible with international human rights law and standards.[59]

Despite this clear mandate, many countries in sub-Saharan Africa continue to regulate or limit the use of encryption. For example, some require the registration and licensing of encryption service providers or have laws that compel service providers to hand over secret codes to state authorities.[60] According to the Global Partners Digital World Map of Encryption, at least

[56] *Federal Prosecutor v. Soleyana Shimeles Gebremariam and others (Zone 9 Bloggers)* (2015) (accessible here).
[57] *Mazetti Management Services v. amaBhungane Centre for Investigative Journalism* (2023) (accessible here).
[58] *Id* at paras 59-60.
[59] See above n 3 at Principle 40.
[60] CIPESA, 'How African Governments Undermine the Use of Encryption' (2021) (accessible here).

27 countries in Africa have laws and policies enabling widespread restrictions on the use of encryption tools.[61]

A new form of surveillance: SIM card registration[62]

In virtually all African countries, there is mandatory SIM card registration, during which a horde of identifying data is collected. While the surge in cybercrimes prompted SIM registration, the data requirements for registration are huge yet the data protection practices are poor with no specific data protection laws. Even in countries with data protection laws, implementation is often poor and many laws fall short of established human rights standards. Moreover, the trends in data collection seem to be changing with several countries increasingly pegging service delivery to data which is collected and stored in various databases. Of itself, SIM registration in effect eradicates the ability of mobile phone users to communicate anonymously and facilitates mass surveillance, making tracking and monitoring of all users easier for law enforcement and security agencies.

Another concern relates to the growing preference for African governments to implement data localisation regulations which mandate that personal data be stored within the country. While ostensibly this is to ensure the protection of personal information, it may also enable easier access to data for decryption and surveillance.[63]

6. GOVERNMENT AND COMMERCIAL SURVEILLANCE[64]

6.1. Definition

Communications surveillance encompasses the monitoring, intercepting, collecting, analysing, retention, or similar actions, of a person's communications in the past, present, or future.[65] This relates to both the content of communications and communication *metadata* – which is information *about* a communication, such as the identities of the parties, the time or duration or location of the communication, and technical services used. It has been noted that even communication metadata can give detailed insights into an individual's behaviour, social relationships, private preferences and identity. Taken as a whole, it may allow very precise conclusions to be drawn concerning the private life of the person.

In recent years, the use of sophisticated surveillance technology on mobile phones has gained increasing prominence amidst concerns about its extensive abuse to monitor political opponents and activists.

[61] Global Partners Digital, 'World Map of Encryption' (accessible here).
[62] See above n 60.
[63] *Id*.
[64] For more on this topic see Media Defence 'Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa' (accessible here).
[65] Article19 et al, 'Necessary and proportionate: International principles on the application of human rights to communications surveillance' (2014) (accessible here) at p 4.

The Pegasus scandal

In 2021, news broke that at least 180 journalists as well as political leaders had been targeted for surveillance by Pegasus spyware, a system that can be remotely installed on a smartphone enabling complete control over the device.[66] The news attracted widespread condemnation, including, for example, the Supreme Court of India in 2021 ordered an independent inquiry into allegations that the government deployed the Pegasus spyware against various journalists, politicians, and dissidents because of the deeply chilling effects its use could have on freedom of expression.[67] Although the findings of the Court's investigation have not been made public, evidence has since come to light of the continued use of the Pegasus software to surveil journalists.[68]

In 2019, Meta launched litigation against the NSO Group, the maker of Pegasus software, claiming that it was responsible for a series of cyber-attacks which violated American law.[69] The litigation is as of 2024 still ongoing. In February 2024, NSO Group was ordered to hand over its code for Pegasus and other spyware products, as well as information concerning the full functionality of the relevant spyware.[70]

African activists and journalists were among some of the targets identified in the Pegasus scandal, as were powerful politicians and state officials revealed to be users of the tools. In 2024, Reporters without Borders found spyware traces on the phones of two **Togolese** journalists while they were on trial for defamation against a government minister.[71]

6.2. International law position

General Comment No. 16 provides that "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[72] Surveillance — both bulk (or mass) collection of data[73] or targeted collection of data — interferes directly with the privacy and security necessary for freedom of opinion and expression, and must be considered against

[66] Forbidden Stories, 'Journalists Under Surveillance' (2021) (accessible here).
[67] *Sharma v Union of India and Others*, Writ Petition (CRL.) No. 314 (2021) (accessible here).
[68] Amnesty International, 'India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists' (2023) (accessible here).
[69] Nick Hopkins and Stephanie Kirchgaessner, 'WhatsApp sues Israeli firm, accursing it of hacking activists' phones' *The Guardian* (2019) (accessible here).
[70] Stephanie Kirchgaessner, 'Court orders maker of Pegasus spyware to hand over code to Whatsapp' *The Guardian* (2024) (accessible here).
[71] RSF, 'In first for Togo, RSF identifies spyware on phones of two Togolese journalists' (2024) (accessible here).
[72] See above n 9 at para 8.
[73] Revelations be whistle-blowers, such as Edward Snowden, have revealed that the National Security Agency in the USA and the General Communications Headquarters in the United Kingdom had developed technologies allowing access to much global internet traffic, calling records in the United States, individuals' electronic address books and huge volumes of other digital communications content. These technologies are deployed through a transnational network comprising strategic intelligence relationships between governments and other role-players. This is referred to as bulk or mass surveillance. See above n 47 at para 4.

the three-part test to assess the permissibility of the restriction.[74] In the digital age, ICTs have enhanced the capacity of governments, corporations, and individuals to conduct surveillance, interception and data collection, and have meant that the effectiveness of conducting such surveillance is no longer limited by scale or duration.[75] In Africa, some countries have even passed legislation enabling digital surveillance of targeted groups; for example, the United Nations Special Rapporteur on Privacy has noted with concern the Anti-Cybercrime Law enacted in Egypt in 2018 which reportedly enables surveillance of the LGBTQI community.[76]

In a resolution adopted by the UN General Assembly (UNGA) on the right to privacy in the digital age, the UNGA emphasised that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, are highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression, and may contradict the tenets of a democratic society, including when undertaken on a mass scale.[77] It noted further that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory.[78]

In order to meet the condition of legality, many states have taken steps to reform their surveillance laws to allow for the powers required to conduct surveillance activities. According to the Necessary and Proportionate Principles, a civil society initiative to document the principles that apply to any limitation on freedom of expression, communications surveillance should be regarded as a highly intrusive act, and in order to meet the threshold of proportionality, the state should be required at a minimum to establish the following information to a competent judicial authority prior to conducting any communications surveillance:[79]

- There is a high degree of probability that a serious crime or specific threat to a legitimate aim has been or will be carried out.
- There is a high degree of probability that evidence relevant and material to such a serious crime or specific threat to a legitimate aim would be obtained by accessing the protected information sought.
- Other less invasive techniques have been exhausted or would be futile, such that the technique used is the least invasive option.
- Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a legitimate aim alleged.
- Any excess information collected will not be retained but instead will be promptly destroyed or returned.
- Information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.

---

[74] *Id* at para 20.
[75] *Id* at para 2.
[76] UNSR on Privacy, 'Report prepared pursuant to Human Rights Council resolutions 28/16 and 37/2' (20190 (accessible here) at p 14.
[77] UNGA, 'Resolution on the right to privacy in the digital age' A/C.3/71/L.39/Rev.1, (2016) (accessible here).
[78] *Id.*
[79] See above n 65 at Principle 5.

- The surveillance activities requested, and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

The importance of independent oversight and subject notification

In addition to the principles discussed above, the groundbreaking case of *amaBhungane Centre for Investigative Journalism v Minister of Justice and Correctional Services* emphasised two additional principles that are critical to ensuring legitimate and rights-respecting targeted surveillance. First, the Constitutional Court of **South Africa** emphasised the need for a clear and independent process for appointing the designated judge to oversee requests for surveillance by law enforcement. Second, it highlighted that the law should accommodate the notification of subjects of surveillance that they have been surveilled after the fact and when such notification will no longer threaten the investigation.

In addition, it is notable that the Court reflected on the need for enhanced protections for lawyers and journalists as a result of the importance of confidentiality in these professions, and that legislation should therefore provide additional safeguards in such cases.

Surveillance constitutes an obvious interference with the right to privacy. Further, it also constitutes an interference with the right to hold opinions without interference and the right to freedom of expression. With particular reference to the right to hold opinions without interference, surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes.[80]

As emphasised in the *amaBhungane* case, the interference with the right to freedom of expression is particularly apparent in the context of journalists who may be placed under surveillance as a result of their journalistic activities. The disclosure or surveillance of journalistic sources can have negative consequences for the right to freedom of expression due to a breach of an individual's confidentiality in their communications.[81] This is the same for cases concerning the disclosure of anonymous user data. Once confidentiality is undermined, it cannot be restored. It is therefore of utmost importance that measures that undermine confidentiality are not taken arbitrarily.

The importance of source protection has been well-established. For example, in *Bosasa Operation (Pty) Ltd v Basson and Another*, the **South Africa** High Court held that journalists are not required to reveal their sources, subject to certain exceptions.[82] The court stated in this regard that:

[80] See above n 47 at para 21.
[81] For more, see *Big Brother Watch v United Kingdom* in the ECtHR (2018) (accessible here) and *amaBhungane Centre for Investigative Journalism v Minister of Justice* in South Africa (2019) (accessible here).
[82] [2012] ZAGPJHC 71, (2012) (accessible here).

> "If indeed freedom of the press is fundamental and *sine qua non* for democracy, it is essential that in carrying out this public duty for the public good, the identity of their sources should not be revealed, particularly, when the information so revealed, would not have been publicly known. This essential and critical role of the media, which is more pronounced in our nascent democracy, founded on openness, where corruption has become cancerous, needs to be fostered rather than denuded."[83]

Surveillance activities carried out against journalists have the risk of fundamentally undermining the source protection to which journalists are otherwise entitled.[84]

6.3. Jurisprudence on journalism and the right to privacy

The linkages between journalistic freedoms and the right to privacy are a common theme in emerging litigation and jurisprudence against unlawful or abusive surveillance. For example:

- In two cases both dealing with the planned roll-out by the Communications Authority of **Kenya** of a system to provide it with access to mobile service subscribers' data, the High Court of Kenya held that the system was "a threat to subscribers' privacy," that there were fewer restriction measures to implement the Authority's goals of identifying illicit devices, and that the system was unlawful, unreasonable, and disproportionate.[85]

- In ordering the independent inquiry into allegations that the government deployed the Pegasus spyware against various journalists, politicians and dissidents, the Supreme Court of **India** found that the free press's democratic function was at stake, and that "such chilling effect on the freedom of speech is an assault on the vital public watchdog role of the press, which may undermine the ability of the press to provide accurate and reliable information."[86]

- The European Court of Human Rights (ECtHR) found some aspects of the **United Kingdom's** mass surveillance regime to be in violation of the right to privacy and

---

[83] *Id* at para 38.

[84] According to Principle 9 of the Global Principles, states should provide for the protection of the confidentiality of sources in their legislation and ensure that:

- Any restriction on the right to protection of sources complies with the three-part test under international human rights law.
- The confidentiality of sources should only be lifted in exceptional circumstances and only by a court order, which complies with the requirements of a legitimate aim, necessity, and proportionality. The same protections should apply to access to journalistic material.
- The right not to disclose the identity of sources and the protection of journalistic material requires that the privacy and security of the communications of anyone engaged in journalistic activity, including access to their communications data and metadata, must be protected. Circumventions, such as secret surveillance or analysis of communications data not authorised by judicial authorities according to clear and narrow legal rules, must not be used to undermine source confidentiality.
- Any court order must only be granted after a fair hearing where sufficient notice has been given to the journalist in question, except in genuine emergencies.

[85] *Kenya Human Rights Commission v. Communications Authority of Kenya* (2018) (accessible here) and *Okoiti v. Communications Authority of Kenya* (2018) (accessible here).

[86] Writ Petition (Crl.) No. 314 of 2021, (2021) (accessible here).

the right to freedom of expression under the European Convention on Human Rights, holding that although bulk interception regimes are not in themselves incompatible with those rights, the lack of independent oversight and the fact that the regime's use was not limited to combatting "serious crime" and did not sufficiently protect journalists' confidential communication resulted in it constituting a violation.[87]

7. PRIVACY AND ARTIFICIAL INTELLIGENCE

7.1. The privacy risks of AI

As the sophistication and usage of artificial intelligence (AI) has increased rapidly in recent years, concerns about both the use of personal information in the development of such tools as well as the ability of such tools to implement privacy violations have become more prominent. In particular, the launch of the public ChatGPT, alongside similar models, has raised alarm bells on several fronts.

- First, because such systems rely on **vast quantities of information** to train their algorithms and continuously improve performance, particularly information scraped from the internet, critics have highlighted that even publicly-available information, such as posts on social media, was never posted with the intent, and hence **consent**, of the data subjects for its usage by large-language models.

- Second, the **collection and storage** of such large quantities of information, including personal information, raise concerns about storage security and the implications if such data were to be accessed by unauthorised parties through hacking or other security breaches. Facial recognition technology, which also often relies on sophisticated algorithms to process large quantities of data, is increasingly in use across the continent by governments ostensibly for law enforcement and security purposes, but they also have the potential to be used for **real-time, intrusive tracking and surveillance** that risks several human rights including the rights to privacy, freedom of movement, and freedom of association.

- Third, AI tools such as these are able to **rapidly generate images and content** about a person based on its training data that may have little correlation to the truth, raising concerns about **mis- and disinformation** and the portrayal of personal information in the online ecosystem. AI's ability to rapidly analyse and make sense of large quantities of data can lead to the ability to infer personal information about a person that they never provided themselves, beyond the scope of consent requirements set out in data protection laws.

7.2. Developing international standards

As a result of these risks, AI has recently garnered increased attention from international and regional human rights bodies seeking to provide guidance and standards to protect the

[87] *Big Brother Watch v. The United Kingdom (Big Brother I)* App nos. 58170/13, 62322/14 and 24960/15 (2018) (accessible here).

affected rights and ensure the responsible development of these new technologies. For example:

- In 2021 the UN Special Rapporteur on the Right to Privacy published a report on AI and privacy and children's privacy that provides guidance on data protection standards for AI at the domestic level as well as calls on states and companies to develop AI solutions ethically and responsibly within a human rights framework.[88]

- Also in 2021, the UN High Commissioner for Human Rights released a report on the right to privacy in the digital age that analysed how the widespread use of AI affects the right to privacy and other fundamental rights, noting that issued a set of recommendations for states and businesses to design and implement rights safeguards.[89] The report notes that AI systems "[incentivise] widespread data collection, storage, and processing," contrary to the principle of data minimisation, and highlights concerns in the sectors of law enforcement, public services, employment, and online information management systems.

- Building on this, in 2023 the new Special Rapporteur submitted her report to the United Nations General Assembly (UNGA) that highlighted the need for transparency and explainability in the use of AI in order for data subjects to be able to exercise their rights over the use of their personal information in such systems.[90]

Notably, the African Union Commission on Human and Peoples' Rights (ACHPR) has also taken steps to interrogate the risks of AI by passing Resolution ACHPR/Res. 473 (EXT.OS/ XXXI) 2021: on the need to undertake a Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa in 2021.[91] In it, the ACHPR—

- acknowledges the myriad risks for human rights not limited to privacy;
- calls on states to put in place mechanisms to ensure the rights-respecting development and use of such technologies in Africa, including by working towards a comprehensive legal and ethical governance framework for AI; and
- commits to undertake a study to develop guidelines on AI.

The study officially began in June 2023.[92]

[88] UNSR on Privacy 'Artificial intelligence and privacy, and children's privacy' (2021) (accessible here).
[89] Report of the UN High Commissioner for Human Rights 'The right to privacy in the digital age '(2021) (accessible here).
[90] UNSR on Privacy 'Right to privacy,' (2023) (accessible here).
[91] ACHR, 'Resolution on the need to undertake a Study on huma and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa' ACHR/Res. 473 (EXT.OS/XXXI) (2021) (accessible here).
[92] ACHPR, 'PRESS RELEASE: Inception Workshop and Experts' Consultation on the Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa, 08 - 09 June 2023 Nairobi, Kenya' (2023) (accessible here).

8. CONCLUSION

As more of the world moves online and increasingly sophisticated new tools for processing personal information become more widely available, data protection is becoming ever more necessary. In the African context, some headway has been made in the passing of 36 data protection laws as well as the coming into force of the Malabo Convention in 2023.[93] However, with the growth and increasing sophistication of technologies and practices related to data harvesting and profiling, legislators are some way behind in fully protecting and promoting data privacy and data protection. As we move forward, digital rights activists have a significant role to play in ensuring that states keep step with data protection developments and enact legislative frameworks that fully protect and promote people's rights to privacy.

[93] See https://dataprotection.africa/ for more information.