Module 4

Privacy and Security Online

Advanced Modules on Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

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

Originally published in November 2022
Revised in March 2024

TABLE OF CONTENTS

MODULE 4

PRIVACY AND SECURITY ONLINE

The objectives of this module are:

- **To provide an overview of the right to privacy;**
- **To set out data protection principles and explain data retention;**
- **To identify emerging issues in communications surveillance;**
- **To explain the rights-related concerns about biometrics and facial recognition;**
- **To unpack the relationship between encryption and anonymity;**
- **To set out the principles of journal source protection; and**
- **To identify emerging issues in online harassment.**

1. INTRODUCTION

In the current data-driven era, the right to privacy has gained increasing recognition as a fundamental right, both in itself and as an enabler of other rights. This includes enabling the right to freedom of expression, for instance by allowing individuals to share views anonymously in circumstances where they may fear being censured for those views, by allowing whistle-blowers to make protected disclosures, and by enabling members of the media and activists to communicate in a secure manner beyond the reach of unlawful government interception.

The key provision under international law regarding the right to privacy is contained in article 17 of the International Covenant on Civil and Political Rights (ICCPR):

- Sub-article (1) provides that no one shall be subjected to arbitrary or unlawful interference with his (or her) privacy, family, home or correspondence, nor to unlawful attacks on his (or her) honour and reputation.
- Sub-article (2) goes on to provide that everyone has the right to the protection of the law against such interference or attacks.

As technology rapidly evolves so do the considerations for the right to privacy, which has remained high on the international human rights law agenda in recent years. In 2016, the United Nations (UN) General Assembly passed a resolution advocating for the protection of the right to privacy, particularly in the digital realm, urging states to enact measures to prevent

violations of this right.[1] In 2018, the United Nations High Commissioner for Human Rights released a report emphasizing the challenges facing privacy in the digital age.[2] This report outlined key issues such as growing digital footprints, data sharing, and biometric projects lacking adequate safeguards. Additionally, it highlighted concerns about mass surveillance, cybercrimes, and attempts to undermine encryption and anonymity. In 2020, the High Commissioner's report on the impact of new technologies on human rights in assemblies underscored the importance of secure communications in organizing peaceful protests.[3] It cautioned against technology-enabled surveillance, which poses significant risks to human rights during assemblies and contributes to the constriction of civic space in many countries.

In 2021, the UN High Commissioner for Human Rights presented the report on Privacy in the Digital Age, which builds on reports from previous reports but focuses on artificial intelligence (AI) in recognition that "AI systems can facilitate and deepen privacy intrusions".[4] Such intrusions could include "entirely new applications as well as features of AI systems that expand, intensify or incentivize interference with the right to privacy, most notably through increased collection and use of personal data."

The 2022 report on Privacy in the Digital Age focused on the misuse of intrusive hacking tools; the critical role of encryption in safeguarding the right to privacy and other rights; and extensive monitoring of public areas.[5] The report underscores the potential dangers of establishing pervasive surveillance and control systems, which could jeopardize the cultivation of vibrant and rights-respecting societies. Also 2022, in reaction to the swift and extensive gathering of personal data purportedly aimed at addressing the COVID-19 crisis between 2020 and 2022, the United Nations Special Rapporteur on Privacy published a document detailing the application of principles such as restricting data usage to specific purposes, erasing data, and exhibiting or pre-emptively ensuring accountability in the handling of personal information collected by governmental bodies during the pandemic.[6]

In the African context, the African Charter on Human and Peoples' Rights (African Charter) does not contain an express provision for the right to privacy. However, it has been argued that the right can – and should – be read into the African Charter through to the right to respect for life and integrity of the person, the right to dignity, and the right to liberty and security of the person.[7] This argument is based on the approach taken by the African Commission on Human and Peoples' Rights (African Commission) in *Social and Economic Rights Action*

[1] UN General Assembly, 'The right to privacy in the digital age' (2016) (accessible here).
[2] UNHRC, 'Report of the United Nations High Commissioner for Human Rights - The right to privacy in the digital age' (2018) (accessible here).
[3] UNHRC, 'Report of the Office of the United Nations High Commissioner for Human Rights - Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (2020) (accessible here).
[4] UNHRC, 'Report of the United Nations High Commissioner for Human Rights - The right to privacy in the digital age' (2021) (accessible here).
[5] UNHRC, 'Report of the United Nations High Commissioner for Human Rights - The right to privacy in the digital age' (2022) (accessible here).
[6] UNHRC' 'UNSR on Privacy: 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' (2022) (accessible here).
[7] Singh & Power, 'The privacy awakening: The urgent need to harmonise the right to privacy in Africa' African Human Rights Yearbook 3 (2019) 202 at p 202, (accessible here).

Centre and Another v Nigeria and the comparative jurisprudence from the Supreme Court of India in *Justice KS Puttaswamy (Retd) and Another v Union of India and Others*.[8]

It bears mention that other African regional instruments do recognise the right to privacy.[9] For example, article 10 of the African Charter on the Rights and Welfare of the Child 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."

In February 2021, the African Commission on Human and Peoples' Rights (ACHPR) passed Resolution No. 473, highlighting the imperative to confront the human rights ramifications of AI, robotics, and other emerging technologies in Africa.[10] The resolution underscores apprehension regarding the extensive impact of AI technologies, robotics, and other emerging technologies on human rights, including the right to privacy.

Notably, the long-awaited African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) was enacted in 2023. It recognises in its preamble the commitment of the AU to build an information society and to protect "the privacy of its citizens in their daily or professional lives while guaranteeing the free flow of information". If further endeavours to establish a comprehensive legal structure for electronic commerce, data protection, and the regulation of cybercrime and cybersecurity across the continent. It mandates member states to adopt domestic legislation in each of these policy domains, aligning with the diverse standards and principles delineated within the convention. At the domestic level, more than 50 African constitutions, inclusive of amendments and recent reviews, include reference to the right to privacy.[11] Out of 55 African states, 36 have data protection laws, with 3 states having draft laws.[12]

It is highly likely that fighting for the right to privacy will continue to be a pressing battle as new and more complex digital advancements attempt to erode this fundamental right and all it enables. It is equally likely that the regulation of technology may have implications for the right to privacy – both positive and negative.

2. DATA PROTECTION

2.1. Key principles of data protection

Data protection is one of the primary measures through which the right to privacy is given effect. Data protection laws are aimed at protecting and safeguarding the processing of personal information (or personal data).

[8] Id.
[9] Singh & Power 'Understanding the privacy rights of the African child in the digital era' *African Human Rights Law Journal* (2021) (accessible here).
[10] ACHPR, 'Resolution 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' (2021) (accessible here).
[11] Singh & Power above n 2.
[12] See ALT Advisory, 'Data Protection Africa' (accessible here).

Although the specific definitions and terms may vary, most data protection laws set out similar basic concepts:

- **Personal information** or an equivalent term generally refers to any information relating to an identified or identifiable natural person which can be used to identify them, whether directly or indirectly, such as their name, contact details, age, race, gender, sexual orientation, health information, financial information, employment details, political or religious views, or biometric information.

- A **data subject** is any person to whom this information relates – in other words, a person whose rights are at stake.

- A data controller, which can typically be either a public or private body, is the person or entity responsible for processing the personal information about the data subject.

- **Processing** usually refers to a wide range of actions that can be performed on personal information including collection, organisation, storage, alteration, retrieval, sending, or deletion, and includes both manual and automated means.

- A **data protection** authority is a type of independent authority or public body established to monitor and enforce compliance with a data protection framework. This module explores data protection authorities in more detail below under Use of data protection authorities to vindicate the right to privacy.

While there may be differences across jurisdictions, there are also several governing principles that appear in most data protection frameworks. The Personal Data Protection Guidelines for Africa[13] (**Data Protection Guidelines**), a joint initiative of the Internet Society (**ISOC**) and the AU, sets out key data protection principles that appear across most frameworks:[14]

- **Collection limitation**: Personal data must be obtained and processed lawfully, fairly, and, to the extent possible, transparently.

- **Data Quality**: Personal data must be accurate at the point of collection, and reasonable steps must be taken to ensure its accuracy is maintained over the period of retention.

- **Purpose specification**: Personal data must be collected only for specified, explicit, and legitimate purposes. Personal data should only be used for such other purposes as are compatible with applicable laws, such as archiving data that is in the public interest, or for scientific research.

- **Use limitation**: Personal data must not be disclosed, made available, or used for other purposes except with the consent of the individual or where authorised by law.

[13] ISOC and AU, 'Personal Data Protection Guidelines for Africa' (2018) (accessible here).
[14] Data Protection Principles at pp 9-10.

- **Security safeguards**: Personal data should be protected by reasonable security safeguards to maintain its integrity and confidentiality.

- **Openness**: There should be a general policy of openness about developments, practices, and policies with respect to personal data.

- **Individual participation**: Individuals must have the right to obtain information about their personal data held by others. This data must be provided within a reasonable period of time, in a form that is readily intelligible, and at a cost that is not excessive. Data subjects have the right to challenge their data and to have it amended if it is inaccurate, or erased if that is appropriate.

- **Accountability**: Those who collect and process personal data must be able to demonstrate their compliance with these principles.

In addition to giving effect to the right to privacy, data protection laws also typically facilitate a right of access to information. Most data protection laws provide 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.

Another key principle of data protection frameworks is that personal data should not be transferred to a country that does not ensure an adequate level of protection for the rights and freedoms of data subjects when it comes to the processing of personal information.[15]

Cross-border data transfers: The case of Max Schrems

In *Maximillian Schrems v Data Protection Commissioner*, Mr Schrems – a European citizen – lodged a complaint with the Irish Data Protection Commissioner that some or all of the data that he had provided to Facebook was transferred from Facebook's Irish subsidiary to servers located in the United States of America (US), where it was processed. As the US does not have a comprehensive data protection law, Mr Schrems argued that the law and practice in the US did not offer sufficient protection against surveillance by the US public authorities and did not meet the test for adequacy as contemplated under European law.

The Court of Justice of the European Union (CJEU) upheld the claim, noting that the protective rules laid out in the data sharing arrangement between the European Union (EU) and the US (known as the 'Safe Harbour Agreement') could be disregarded by the US where they conflicted with national security, public interest and law enforcement requirements of the US. The CJEU held that any legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the right to privacy. Furthermore, the CJEU found that legislation that does not provide for an individual to pursue legal remedies to access their personal information, or to have such information rectified or erased, compromises the essence of the right to effective judicial protection.

[15] Information Commissioner's Office, 'Data protection principles', (accessible here).

Accordingly, the CJEU declared the Safe Harbour Decision invalid, with immediate effect. In line with this judgment, the threshold that has been established for determining the adequacy of protection is to ascertain whether it is "essentially equivalent."

This decision was subsequently followed up by another dubbed 'Schrems II' which speaks to the use of "standard contractual clauses" to transfer data between Europe and the US.

In 2023, Ireland's Data Protection Commissioner (DPC) issued Meta (formerly Facebook) a substantial $1.3 billion fine for actively breaching the EU's data privacy laws, particularly regarding the transfer of data across borders.[16] This penalty stands out as one of the most significant regulatory actions under the General Data Protection Regulation (GDPR) in the past five years since its enactment. Meta was given a five-month grace period to halt the transfer of data collected from European Facebook users to the US. Additionally, within six months of the DPC's notification to Meta, the company must cease the unlawful processing and storage of personal data in the US. However, this ruling does not affect data transfers on Instagram and WhatsApp, other major platforms owned by Meta. Meta has stated its intention to appeal the decision and the fine, deeming them unjustified and unnecessary. The ruling emphasised that Meta violated Article 46(1) of the GDPR by persisting in cross-border data transfers to the US from the EU/EEA, contrary to the European Court of Justice's judgment in *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Schrems II).

2.2. Data protection frameworks in Africa

A growing number of African states have enacted data protection laws, and more are in the process of doing so. In addition to giving effect to the right to privacy, data protection legislation also has a key role to play in facilitating trade amongst 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.

Data protection in Africa

As of January 2024, 36 out of 55 African countries (65%) have implemented data protection laws, signifying significant progress. Additionally, three countries (**Ethiopia**, **Namibia**, and **Malawi**) are currently considering draft legislation in this regard. However, 16 countries (29%) in Africa have yet to make headway in enacting data protection laws, highlighting an area for improvement. Over the past decade, there has been a notable increase in the adoption of data protection laws across Africa, with the number more than doubling. Remarkably, a third of these laws were enacted within the last five years. Regional disparities exist, with some areas demonstrating greater success in passing this vital legislation. Notably, 75% of traditionally Francophone countries have implemented data protection laws, with many among the earliest adopters. While Southern African countries have more recently embraced

[16] Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR) (accessible here).

data protection laws, 73% now have such legislation in place. In contrast, only 54% of East African countries have enacted similar laws.[17]

For a full overview of the data protection landscape in Africa, visit Data Protection Africa here.

As noted in the Data Protection Guidelines, in considering the relevant data protection framework, it is necessary to understand the African context and the particular characteristics that arise:[18]

- Significant cultural and legal diversity across the continent, with different privacy expectations.
- Variations in access to technology and online services among member states.
- Sensitivities regarding ethnicity and profiling of citizens without consent.
- Different levels of capability in areas such as technology and technology-related law and governance.
- Risks arising from high dependency on non-African manufacturers and service providers, including the limited ability of African states to influence the behaviour of external service providers, and the potentially increased risk of data misuse where content and services are solely provided by foreign companies.

According to the Data Protection Guidelines, this context presents unique challenges to the enforcement of local data protection laws that may make such enforcement more difficult.

The Malabo Convention provides useful guidance at the regional level to states looking to implement data protection frameworks at the domestic level. Chapter II of the Malabo Convention sets out the principles relevant to data protection. As set out in article 8(1), the objective of the Convention is for each state party to commit itself to establishing a legal framework "aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy with prejudice to the principle of the free flow of personal data."

Article 13 of the Malabo Convention sets out the following basic principles governing the processing of personal data:

- Principle 1: Principle of consent and legitimacy of personal data processing.
- Principle 2: Principle of lawfulness and fairness of personal data processing.
- Principle 3: Principle of purpose, relevance and storage of processed personal data.
- Principle 4: Principle of the accuracy of personal data.
- Principle 5: Principle of transparency of personal data processing.
- Principle 6: Principle of confidentiality and security of personal data processing.

Articles 16 to 19 of the Malabo Convention set out the rights of data subjects, namely the right to information; the right of access; the right to object; and the right of rectification or erasure.

[17] Data Protection Africa, 'Mapping the progress (and delays) for data protection in Africa' (2024) (accessible here).
[18] Data Protection Principles at p 7.

Articles 20 to 23 go on to set out the obligations of personal data controllers, namely the confidentiality obligations; the security obligations; the storage obligations; and the sustainability obligations.

In respect of cross-border data transfers, article 14(6)(a) provides that: "The data controller shall not transfer personal data to a non-Member State of the African Union unless such a State ensures an adequate level of protection of the privacy, freedoms and fundamental rights of the persons whose data are being or are likely to be processed". Sub-article (b) goes on to provide that the prohibition does not apply if the data controller has requested authorisation for the transfer from the relevant data protection authority before the data has been transferred.

Processing for journalistic, research, artistic or literary purposes

Article 14(3) of the Malabo Convention provides for a specific exemption that applies to the processing of personal data for journalistic, research, artistic or literary purposes. It provides that: "Personal data processing for journalistic purposes or for the purposes of research or artistic or literary expression shall be acceptable where the processing is solely for literary or artistic expression or for the professional exercise of journalistic or research activity, in accordance with the code of conduct of these professions."

Article 14(4) goes on to provide that the provisions of the Convention "shall not preclude the application of national legislations with regard to the print media or the audio-visual sector, as well as the provisions of the criminal code which provide for the conditions for the exercise of the right of reply, and which prevent limit, compensate for and, where necessary, repress breaches of privacy and damage to personal reputation."

2.3. Extra-territorial application of data protection frameworks in Europe

There are two key European instruments with respect to data protection that have extra-territorial application for African states: **Convention 108** and the **GDPR**.

The Convention for the Protection of Individuals with regard to the Processing of Personal Data[19] – commonly referred to as Convention 108 – is an instrument of the Council of Europe (**COE**). Convention 108 opened for signature in 1981 and was the first legally binding instrument in the data protection field.[20] The purpose of Convention 108 is to "protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy".[21] Convention 108 provides for the free flow of personal data between states parties to the Convention.

[19] Accessible at here.
[20] COE, 'Convention 108 and protocols: Background', (accessible here).
[21] Article 1 of Convention 108.

A key feature of Convention 108 is that, in addition to the members of the COE, it also provides that non-European states may accede to it. For example, in the African context, Cape Verde, Mauritius, and Senegal have all acceded to it. This is of relevance for several reasons: it is a recognition of the adequacy of their data protection frameworks; it adds an additional bulwark of protection for persons within those states, and; it can serve to facilitate cross-border data transfers between those African states and Europe. Convention 108 remains open for accession to other African states that meet the necessary requirements.

Modernisation of Convention 108

In May 2018, the COE published Convention 108+, in an effort to update and modernise Convention 108 given that it was opened for signature over 35 years previously. The modernisation effort gives new considerations to automated processing, cross-border data flows, and the need to strengthen the Convention's evaluation and follow-up mechanisms.

The second key instrument, the European Union General Data Protection Regulation 2016/679[22] (**GDPR**), is an effort to harmonise all data protection laws across the European Union and has been applicable to all EU member states since 25 May 2018. As explained in article 1 of the GDPR, its purpose is to lay down rules relating to the protection of natural persons with regard to the processing of personal data, as well as rules relating to the free movement of personal data. In particular, article 1(2) makes clear that the GDPR is intended to protect "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".

Chapter II of the GDPR sets out the following principles:

- Article 5: Principles relating to the processing of personal data.
- Article 6: Lawfulness of processing.
- Article 7: Conditions for consent.
- Article 8: Conditions applicable to a child's consent in relation to information society services.
- Article 9: Processing of special categories of personal data.
- Article 10: Processing of personal data relating to criminal convictions and offences.
- Article 11: Processing which does not require identification.

The conditions for consent bear special emphasis. Importantly, the data controller bears the burden of demonstrating that the data subject has consented to the processing of his or her personal data.[23] Where written consent is sought, the GDPR provides that this request for consent "shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language" in order for it to be binding.[24] The data subject has the right to withdraw consent at any time, and it is required that it be made as easy to withdraw consent as it is to give consent.[25] Added to this,

[22] Accessible at here.
[23] Article 7(1) of the GDPR.
[24] Article 7(2) of the GDPR.
[25] Article 7(3) of the GDPR.

the GDPR provides that when assessing whether consent is freely given, utmost account must be taken of whether the performance of a contract or provision of a service "is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".[26]

A unique and notable inclusion in the GDPR is that, per Article 3, it seeks to apply extra-territorially, to data controllers that are not established in the EU, regardless of whether the processing takes place in the EU or not. Failure to comply with the GDPR carries significant penalties, including administrative fines of up to €20 000 or 4% of the transgressor's total worldwide turnover of the preceding year, whichever is higher.[27]

Influence of the GDPR on African Data Privacy Laws

According to data protection experts, several African countries have implemented data protection laws that bear similarities to the GDPR:[28]

- In Rwanda, the Protection of Personal Data and Privacy law follows a framework akin to the GDPR.
- Uganda's Data Protection and Privacy Act aims to safeguard individual privacy and personal data, drawing inspiration from the GDPR in certain limited aspects.
- In Mauritius, the Data Privacy Act aligns with international standards, including the GDPR and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. However, certain provisions in the Act differ from those in the GDPR. For instance, it does not include the hefty administrative penalties found in the GDPR, mandates registration with the Data Protection Office prior to data processing, and lacks automatic transfer to countries offering an adequate level of protection determined by the Data Protection Office.
- The Nigerian Data Protection Regulation closely resembles the GDPR in its structure and core principles. Both laws aim to afford data subjects a certain level of protection concerning their personal data, with consistent definitions and principles regarding the processing of personal data.

2.4. Use of data protection authorities to vindicate the right to privacy

Data protection frameworks typically provide for the establishment of a data protection authority (**DPA**) to oversee and enforce the relevant framework. Such DPAs are typically given a range of powers, including to be notified in the event of a data breach, to adjudicate complaints, and to impose penalties where a data controller is found to be non-compliant with the data protection framework.

[26] Article 7(4) of the GDPR.
[27] Article 83 of the GDPR.
[28] Webb du Preez, 'How the European Union's General Data Protection Regulations influenced data privacy law in Africa' (2022) (accessible here).

In states with established DPAs, this may be an avenue to vindicate the right to privacy. In the event of a data breach or another infringement of the data protection framework, data subjects may be assisted with lodging complaints to the relevant DPA. This quasi-judicial forum can present a relatively quick and cost-effective remedy for the data subject.

In 2023, Tools for Humanity initiated a trial of a fresh cryptocurrency initiative known as Worldcoin.[29] This campaign offered individuals a small sum of cryptocurrency in exchange for allowing their biometric data to be gathered. Thousands of people participated in this opportunity, despite having limited information about how their data would be utilised. In May, Kenya's Office of the Data Protection Commissioner (OPDC) instructed the company to cease processing data, a directive that allegedly went unheeded. It wasn't until August, when the Ministry of the Interior intervened and ordered the suspension of Worldcoin's activities in the country due to data protection concerns, that the company finally ceased data collection. Subsequently, the OPDC initiated legal proceedings against Tools for Humanity in the High Court.[30]

Data protection litigation in Africa

Because many data protection laws, and accompanying authorities, are relatively new in Africa and have often faced implementation challenges, there has been limited data protection litigation on the continent to date. However, cases are beginning to appear from various countries, setting a reassuring precedent for the protection of human rights.

- In **Uganda**, the Initiative for Social and Economic Rights, The Unwanted Witness, and the Health Equity and Policy Initiative - have taken legal action against the Ugandan Attorney General and the National Identification Registration Authority (NIRA), which is responsible for issuing IDs in Uganda.[31] Ugandan law recognises the concept of 'Amicus Curiae', allowing individuals or organizations not directly involved in a lawsuit to participate by providing the court with pertinent information to aid in its decision-making process. In a brief submitted to the court, these organisations requested permission to present information addressing three crucial questions in the ongoing case. These questions pertain to the national digital ID programs' impact on the right to privacy, freedom of expression, and related economic, social, and cultural rights. The organisations emphasise that any court ruling must consider the human rights implications of the mandatory, yet exclusionary, digital ID system.

- In **Ghana**, lawyer Francis Kwarteng Arthur filed a suit challenging the government's collection of personal data from mobile phone subscribers. In August 2021, the High Court ruled that the National Communications Authority (NCA) had to stop collecting personal information from mobile phone subscribers and ordered the government to delete data already collected within fourteen days of the judgement.[32]

[29] Kenya Ministry of Interior, 'Statement on Worldcoin,' (2023) (accessible here).
[30] TechCrunch, 'Worldcoin ignored initial order to stop iris scans in Kenya, records show,' (2023) (accessible here).
[31] Access Now "Privacy first: Ugandan court hears civil society's human rights warnings on digital identity system" 2023 (accessible here).
[32] Kwarteng v Ghana Telecommunications Company and Others, (2021) (accessible at here).

- In **Kenya**, a series of successful legal challenges to a new national biometric identity programme known as the Huduma Namba, led to the courts ordering delays and conditions to the programme's rollout.

3. DATA RETENTION

Data retention is typically described as "the process through which governments and businesses (especially telecommunication and internet providers) record and store various data (usually related to individuals)."[33] As explained by Privacy International:[34]

> "The practice of data retention involves the gathering and storing of communications data for extended periods for the purpose of future access. Metadata tells the story about your data and answers the who, when, what, and how of a specific communication."

While the specific terms and definitions vary, most legal frameworks on data retention relating to communications provide for two categories of information – the 'content' of the communication itself, and information *about* the communication. This second category, often called communication data or communication metadata, includes a wide range of information which is often deeply revealing, such as the identities or identifiers of those involved, the times and durations of their interactions, locational information, and any technology or services involved. While data retention can be important for criminal investigations, it also gives more power to governments to monitor the public and takes away their rights to online privacy.[35] The practice of mandating the retention of communications data raises significant privacy, transparency and security concerns. In turn, this may affect the ways in which people exercise their rights online and pose a risk of leading to self-censorship.

It has been noted that: "Data retention laws are different from country to country, but they ultimately have the same goal: A better grip on the digital world at the expense of privacy and freedom of speech".[36] Privacy International explains that the mass retention of individuals' communications records, outside the context of any criminal investigation or business purpose, "amounts to the compilation of dossiers on each and every one of us, our friends, family and colleagues".[37] Privacy International goes on to explain that:

> "The potential harms associated with data retention and access are significant. In a context where the gathering and exploitation of data by private companies become increasingly privacy intrusive and widespread, data retention poses serious risks to individual privacy and data security. The data opens the door for governments and third parties to make intimate inferences about individuals, to engage in profiling and to otherwise intrude on people's private lives. If the information is not properly protected there is the potential of unauthorised access to troves of information by third parties, including cyber-criminals."

[33] Cactus, 'What is data retention and how does it affect online privacy?', (2018) (accessible here).
[34] Privacy International, 'National data retention laws since the CJEU's Tele-2 / Watson judgment: A concerning state of play for the right to privacy in Europe', (2017) (accessible here).
[35] Id.
[36] Id.
[37] Privacy International, 'Communications data retention', (accessible here).

Most data protection frameworks provide that data should only be collected for specified, explicit and legitimate purposes and that such data should, in the ordinary course, be deleted when this is no longer the case. Additionally, data ought not to be kept for longer than it is needed. For example, article 5(1)(e) of the GDPR provides that personal data shall be–

> "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes … subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')".

In general, there are two key factors that determine an appropriate data retention period: (i) the purpose for processing the data; and (ii) any legal or regulatory requirements for retaining it. In respect of the latter, various countries have mandatory data retention laws that require telecommunication and internet service providers to retain certain types of data – such as metadata – for stipulated periods of time.

Importantly, there have been at least two significant judgments of the CJEU – *Digital Rights Ireland*[38] and *Tele2 Sverige AB*[39] – that have reaffirmed the requirement that all data retention regimes must comply with the principles of legality, necessity and proportionality.[40] Appropriate safeguards are also needed to protect the data that has been retained.

Case note: No legal restrictions on the retention of data

In the *Nubian Rights Forum v Attorney General* case, the High Court of **Kenya** ruled against the gathering of DNA and GPS data, deeming it a violation of the right to privacy and unconstitutional.[41] This decision followed a challenge by three non-governmental organizations to amendments to the Registration of Persons Act, which sought to establish a centralized database of biometric information and introduce unique identification numbers. The petitioners emphasized the sanctity of the right to privacy, arguing that state intrusion required substantial justification. Notably, they contended that the collection of DNA and GPS data lacked legal restrictions on retention and lacked clarity on purpose. Moreover, they highlighted risks of unauthorized access and potential misuse of biometric technologies for discrimination and surveillance. While the Court recognised the importance of certain biometric data collection, it found the risks associated with DNA and GPS data unjustifiable. Despite the introduction of the Data Protection Act during the proceedings, the court deemed the existing regulatory framework insufficient and mandated the adoption of a more comprehensive data protection framework before implementing the proposed system.

[38] Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources et al (C-293/12); Kärntner Landesregierung and Others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014).
[39] Tele2 Sverige AB v Post-Och telestyrelsen (C-203/15); Secretary of State for the Home Department v Tom Watson et al (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (2016).
[40] Privacy International, above n 34 at p 4.
[41] Nubian Rights Forum v Attorney General consolidated petitions no. 56, 58 and 59 of 2019 (accessible here).

4. SURVEILLANCE

4.1. Government-led digital surveillance

Communications surveillance encompasses the monitoring, intercepting, collecting, analysing, retention, or similar actions, of a person's communications in the past, present, or future.[42] Online surveillance has been a central issue for human rights activists for years, but the Snowden revelations about the extent and scope of global mass surveillance brought new urgency and awareness to the issue and sparked a wave of policy change and jurisprudence in many jurisdictions.

Surveillance constitutes an obvious interference with the right to privacy. Further, it also infringes on 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, can create a chilling effect by deterring a person from accessing information, particularly where such surveillance leads to repressive outcomes. The knowledge, or even the perception, of being surveilled can lead to self-censorship. Accordingly, emerging jurisprudence on communications surveillance has also often paid special attention to media freedom considerations:

- **United Kingdom**: In *Big Brother Watch and Others v. the United Kingdom* the Grand Chamber of the ECtHR found *inter alia* that the UK's bulk surveillance regime contravened article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms because it did not adequately protect confidential journalistic material from collection and inspection in the course of bulk monitoring of communications data undertaken by UK intelligence agencies.

- **South Africa**: In *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* (discussed in further detail below), the High Court of South Africa found that the need of journalists and their sources for confidential communications required special protections against surveillance abuses, remarking that:

> "In a country that is as wracked by corruption in both our public institutions and in our private institutions as ours is, and where the unearthing of wrongdoing is significantly the work of investigative journalists, in an otherwise, seemingly, empty field, it is hypocritical to both laud the press and ignore their special needs to be an effective prop of the democratic process."

- **India**: In *Sharma v Union of India* the Supreme Court of India, in ordering an independent inquiry into allegations that the government deployed the Pegasus spyware against various journalists, politicians and dissidents, similarly found that the free press's democratic function was at stake, and that "such chilling effect on the freedom of speech

[42] Necessary and proportionate: International principles on the application of human rights to communications surveillance, 2014 (Necessary and Proportionate Principles) at p 4 (accessible here.

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."[43] 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.[44]

It has been noted that many frameworks create a legal distinction between communications information that is deemed to be 'content' and information that is *about* the communication (communication data or metadata). This second category is often subject to fewer legal and social protections than information deemed to be 'content'. Yet communication data may give detailed insights into a person's behaviour, social relationships, private preferences and identity – either when analysed in bulk or in some cases in individual parts.[45] In addition, the two legal distinctions are arbitrary and ill-suited to many types of communication information in the context of the modern digital age, where certain types of data could fall into either legal category.[46]

Right to Privacy in the Digital Age

The 2016 UN Resolution on the Right to Privacy in the Digital Age urges states to review their procedures, practices, and legislation related to communication surveillance and personal data collection, ensuring alignment with international human rights standards. It emphasizes the establishment of independent oversight mechanisms to enhance transparency and accountability in state surveillance activities.[47] Furthermore, the resolution emphasizes the importance of providing effective remedies for individuals whose privacy rights are violated and calls for the development of legislation with robust sanctions to safeguard against privacy violations.

The 2018 Report of the UN High Commissioner for Human Rights on the Right to Privacy in the Digital Age, highlighted that numerous States persist in clandestine mass surveillance and communications interception.[48] This involves the collection, storage, and analysis of data from all users across various communication channels such as emails, phone calls, text messages, and website visits. While some States argue that such indiscriminate surveillance is necessary for national security, it is emphasized that this practice violates international human rights law. The report underscores that individualized necessity and proportionality assessments are rendered impossible within the context of such broad measures.

In the 2022 Report on the Right to Privacy in the Digital Age expresses ongoing concerns regarding mass surveillance, particularly the bulk interception of communications.[49] Despite some states enhancing safeguards, the troubling practice of surveilling large segments of the population persists. States were reminded of their obligation to ensure that any

[43] Accessible here.:
[44] Amnesty International, 'India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists,' (2023) (accessible here).
[45] ACLU of California, 'Metadata: Piecing together a privacy solution,' 2014, at p 5 (accessible here).:
[46] Id., at p 3-4.
[47] UN General Assembly, above n 1.
[48] UNHRC, Right to Privacy in the Digital Age (2018) above n 2.
[49] UNHRC, Right to Privacy in the Digital Age (2022) above n 5.

interference with the right to privacy complies with international human rights law, emphasizing principles such as legality, necessity, proportionality, and non-discrimination, without compromising the essence of the right to privacy.

African Declaration on Internet Rights and Freedoms

Principle 9 of the African Declaration on Internet Rights and Freedoms (African Declaration) – a civil-society-led initiative that has been endorsed by the African Commission on Human and Peoples' Rights – provides that "[u]nlawful surveillance, monitoring and interception of users' online communications by state or non-state actors fundamentally undermine the security and trustworthiness of the Internet." The African Declaration goes on to explain that:

- Mass or indiscriminate surveillance of individuals or the monitoring of their communications, constitutes a disproportionate interference, and thus a violation, of the right to privacy, freedom of expression and other human rights, and shall be prohibited by law.

- The collection, interception and retention of communications data amounts to an interference with the right to privacy and freedom of expression whether or not the data is subsequently examined or used.

- Targeted surveillance of online communications must be governed by clear and transparent laws which comply with the following basic principles:

    - Communications surveillance must be both targeted and based on reasonable suspicion of commission or involvement in the commission of a serious crime;
    - Communications surveillance must be judicially authorised and individuals placed under surveillance must be notified that their communications have been monitored as soon as practicable after the conclusion of the surveillance operation
    - The application of surveillance laws must be subject to strong parliamentary oversight to prevent abuse and ensure the accountability of intelligence services and law enforcement agencies.

- Individuals must be protected from unlawful surveillance by other individuals, private entities or institutions, including in their place of work or study and in public internet access points.

General Comment No 16 to the ICCPR 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".[50] In the digital age, Information

[50] General Comment No 16 at para 8.

and Communications Technologies (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. Surveillance – both bulk (or mass) collection of data or targeted collection of data – interferes directly with the privacy and security necessary for freedom of opinion and expression. As such, in all its forms surveillance must be considered against the three-part test established in international law to assess the permissibility of a restriction on human rights, namely that the limitation is:

- Provided by law.
- Pursues a legitimate aim.
- Necessary and proportionate to achieving the aim.

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. For instance, in the judgment of *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*, the Constitutional Court of South Africa upheld a ruling of the High Court that the exercise of bulk surveillance in South Africa was unlawful because of the absence of any empowering legal framework to authorise such surveillance to take place.

4.2. The rise of Spyware

In recent years, Spyware has emerged as a significant concern, enabling covert access to information on target computer systems or devices. Predator and Pegasus are prominent spyware programs capable of clandestinely infiltrating mobile phones and other devices running Android and iOS, exploiting the latest mobile operating systems. Journalists, politicians, government officials, chief executives, and directors are often targeted. Notable Incidents include:

- In 2019, Amnesty International documented network injection attacks in Morocco, infecting human rights defenders and journalists with NSO Group's Pegasus spyware.
- In 2021, Egyptian exiled politician Ayman Nour and an anonymous news program host were hacked with Predator spyware developed by Cytrox.
- In 2023, the Predator Files global investigation revealed the widespread use of surveillance technologies and government failures in regulation.
- The Citizen Lab reported a similar system targeting a political opposition figure in Egypt with Intellexa's Predator spyware in September 2023.
- As of 2024, 11 nations, including Angola, Armenia, Botswana, Egypt, Indonesia, Kazakhstan, Mongolia, Oman, the Philippines, Saudi Arabia, and Trinidad and Tobago, are suspected Predator customers.

Legal Action Against Commercial Surveillance Targeting Journalists: NSO Group

In 2021, the Pegasus Project revealed that more than 180 journalists across 20 countries have been potentially targeted for surveillance by governments relying on spyware produced by NSO Group Technologies. Pegasus, NSO's premier spyware tool, breaks encryption protections for communications devices before proceeding to infect the devices with spyware to monitor communications.[51] NSO Group sells this software on a subscription basis to law enforcement and intelligence agencies around the world.[52]

Legal action has been taken against NSO Group by several actors with varying legal bases. In 2020, Amnesty International unsuccessfully approached an Israeli District Court seeking to have NGO Groups' export license revoked.[53] In India, the Supreme Court ordered an investigation in 2021 into the government's alleged use of the spyware to illegally surveil journalists, activists, and political opponents.[54] In 2022, the committee concluded its investigation but did not release its findings publicly beyond noting that the Indian authorities "did not cooperate" with the investigators, and new incidents of the use of technology to spy on journalists continue to be revealed.[55]

4.3. Necessary and proportionate

The Necessary and Proportionate Principles are a set of 13 international principles on the application of human rights to communications surveillance, especially in the context of the ever-advancing mass surveillance capabilities shown by states and private-sector operators in the modern digital era.[56] The principles advise among other things that all powers of communications surveillance must be prescribed and regulated by law, be necessary and proportionate to pursue a legitimate aim, and be subject to certain safeguards, including that the powers are subject to a competent judicial authority, and necessary transparency and public oversight measures.

- **Principle 3** establishes *necessity*, explaining that surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. As such, surveillance should only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification rests on the state.

[51] ARTICLE 19, 'Rwanda: Surveillance revelations opportunity to reform legal and encryption environment', 26 July 2021 (accessible here).
[52] Ronen Bergman & Mark Mazzetti, 'The Battle for the World's Most Powerful Cyberweapon', 28 January 2022 (accessible here).
[53] Amnesty International, 'Israel: Court rejects bid to revoke notorious spyware firm NSO Group's export licence,' (2020) (accessible here).
[54] The Guardian, 'Indian supreme court orders inquiry into state's use of Pegasus spyware,' (2021) (accessible here).
[55] Amnesty International, 'India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists,' (2023) (accessible here).
[56] Accessible here. The Necessary and Proportionate Principles were drafted by Access Now, the Electronic Freedom Foundation and Privacy International, and launched at the UN Human Rights Council in 2013. It has since been endorsed by more than 400 organisations around the world.

- **Principle 5** establishes *proportionality*: 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:[57]

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

4.4. Safeguards and oversight

Privacy International sets out the following ten safeguards that should be implemented for any government hacking or surveillance regime:[58]

Legality: Government hacking powers must be explicitly prescribed by law and limited to those strictly and demonstrably necessary to achieve a legitimate aim. That law must be accessible to the public and sufficiently clear and precise to enable people to

- foresee its application and the extent of the interference. It should be subject to periodic review by means of a participatory legislative process.

- **Security and integrity of systems**: Prior to carrying out a hacking measure, government authorities must assess the potential risks and damage to the security and integrity of the target system and systems generally, as well as of data on the target system and systems generally, and how those risks and/or damage will be mitigated or corrected. Government authorities must include this assessment in any application in support of a proposed hacking measure. Government authorities must not compel hardware or software manufacturers or service providers to facilitate government hacking, including by compromising the security and integrity of their products and services.

[57] Principle 5 of the Necessary and Proportionate Principles.
[58] Privacy International, 'Government hacking and surveillance: 10 necessary safeguards', (accessible here).

- **Necessity and proportionality**: Prior to carrying out a hacking measure, government authorities must, at a minimum, establish a high degree of probability that: (i) serious crime or act(s) amounting to a specific, serious threat to national security has been or will be carried out; (ii) the system used by the person suspected of committing the serious crime or act(s) amounting to a specific, serious threat to national security contains evidence relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security interest alleged; and (iii) evidence relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security alleged will be obtained by hacking the target system.

- **Judicial authorisation**: Prior to carrying out a hacking measure, government authorities must make an application, setting forth the necessity and proportionality of the proposed measure to an impartial and independent judicial authority, who shall determine whether to approve such measure and oversee its implementation. The judicial authority must be able to consult persons with technical expertise in the relevant technologies, who may assist the judicial authority in understanding how the proposed measure will affect the target system and systems generally, as well as data on the target system and systems generally. The judicial authority must also be able to consult persons with expertise in privacy and human rights, who may assist the judicial authority in understanding how the proposed measure will interfere with the rights of the target person and other persons.

- **Integrity of information**: Government authorities must not add, alter or delete data on the target system, except to the extent technically necessary to carry out the authorised hacking measure. They must maintain an independently verifiable audit trail to record their hacking activities, including any necessary additions, alterations or deletions. Where government authorities rely on data obtained through an authorised hacking measure, they must disclose the method, extent and duration of the hacking measure and their audit trail so that the target person can understand the nature of the data obtained and investigate additions, alterations or deletions to information or breaches of the chain of custody, as appropriate.

- **Notification**: Government authorities must notify the person(s) whose system(s) have been subject to interference pursuant to an authorised hacking measure, regardless of where the person(s) reside, that the authorities have interfered with such system(s). Government authorities must also notify affected software and hardware manufacturers and service providers, with details regarding the method, extent and duration of the hacking measure, including the specific configurations of the target system. Delay in notification is only justified where notification would seriously jeopardise the purpose for which the hacking measure was authorised or there is an imminent risk of danger to human life and authorisation to delay notification is granted by an impartial and independent judicial authority.

- **Destruction and return of data**: Government authorities must immediately destroy any irrelevant or immaterial data that is obtained pursuant to an authorised hacking measure. That destruction must be recorded in the independently verifiable audit trail of hacking activities. After government authorities have used data obtained through an authorised

hacking measure for the purpose for which authorisation was given, they must return this data to the target person and destroy any other copies of the data.

- **Oversight and transparency**: Government authorities must be transparent about the scope and use of their hacking powers and activities and subject those powers and activities to independent oversight. They should regularly publish, at a minimum, information on the number of applications to authorise hacking approved and rejected; the identity of the applying government authorities; the offences specified in the applications; and the method, extent and duration of authorised hacking measures, including the specific configurations of target systems.

- **Extraterritoriality**: When conducting an extraterritorial hacking measure, government authorities must always comply with their international legal obligations, including the principles of sovereignty and non-intervention, which express limitations on the exercise of extraterritorial jurisdiction. Government authorities must not use hacking to circumvent other legal mechanisms – such as mutual legal assistance treaties or other consent-based mechanisms – for obtaining data located outside their territory. These mechanisms must be clearly documented, publicly available, and subject to guarantees of procedural and substantive fairness.

- **Effective remedy**: Persons who have been subject to unlawful government hacking, regardless of where they reside, must have access to an effective remedy.

Impugned provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (RICA) declared unconstitutional

In the case of *amaBhungane Centre for Investigative Journalism NPC v. Minister of Justice and Correctional Services*, the Constitutional Court of South Africa considered a challenge to South Africa's interception law, RICA, brought by an investigative journalism outfit whose co-founder had been subject to communications surveillance by the intelligence services. The Court declared various provisions of RICA to be unconstitutional, on the grounds that the law:

- Fails to provide safeguards to ensure the independence of a judge designated to oversee interception requests;
- Fails to provide for "post-surveillance notification" of people whose communications are intercepted.
- Does not adequately provide safeguards to address the fact that interception directions are sought and obtained *ex parte* (i.e. necessarily without the knowledge and participation of the person whose communications would be intercepted);
- Does not detail procedures to ensure that data obtained in the interception of communications is managed lawfully, including steps to be followed for examining, sharing, storing, or destroying the data; and
- Does not provide adequate safeguards where the subject of surveillance is a practising lawyer or journalist. For example, RICA fails to prescribe an appointment

mechanism and terms for a designated judge (any judge mandated to oversee interception requests), which ensures the judge's independence.

The Constitutional Court also upheld an order of the High Court that bulk surveillance activities and foreign signals interception undertaken by the South African government were unlawful and invalid, in that they were not subject to any enabling law.

In 2023, South Africa introduced a Bill to amend the unconstitutional defect. However, this has generated much public outcry, with commentators arguing that the Bill falls short of what was demanded by the judgment and fails to address other long-standing issues.[59] Despite this, the Bill has been passed by Parliament and is awaiting signature by the President.[60]

4.5. Covert recordings

There are various domestic laws and international standards that require that individuals be notified of covert recordings, including video surveillance.[61] However, there is no consistent position on this issue. There are two key recent decisions of the Grand Chamber of the ECtHR that are relevant in this regard:[62]

- *Antović and Mirković v Montenegro* (2017): This case concerned an invasion of privacy complaint by two professors at the University of Montenegro's School of Mathematics after video surveillance had been installed in areas where they taught. They stated that they had no effective control over the information collected and that the surveillance had been unlawful. The domestic courts rejected a compensation claim, finding that the question of private life had not been at issue as the auditoriums where the applicants taught were public areas. The ECtHR made the following findings:
    - It held that there had been a violation of article 8 of the European Convention, finding that the camera surveillance had not been in accordance with the law.
    - The ECtHR rejected the government's argument that the case was inadmissible because no privacy issue had been at stake as the area under surveillance had been a public, working area, noting that it had previously found that private life might include professional activities and considered this to apply to the applicants' situation. Article 8 of the European Convention was therefore applicable.
    - On the merits of the case, the ECtHR found that the camera surveillance had amounted to an interference with the applicants' right to privacy and that the evidence showed that the surveillance had violated the provisions of domestic law. According to the ECtHR, the domestic courts had not considered any legal justification for the surveillance because they had decided from the outset that there had been no invasion of privacy.

[59] Intelwatch, 'Submission: What's wrong with the RICA bill' (2023) (accessible here).
[60] Parliamentary Monitoring Group, 'Regulation of Interception of Communications and Provision of Communication-related Information Amendment Bill' (2023) (accessible here).
[61] International Justice Resource Centre, 'European Court holds secret surveillance did not violate employees' privacy', (2019) (accessible here).
[62] ECtHR Press Unit, 'Surveillance at workplace', (accessible here)

- *Ribalda and Others v Spain* (2019): This case concerned covert video surveillance of a group of employees at a supermarket, which led to their dismissal. The applicants complained about the covert video surveillance and about the Spanish courts' use of the footage to find that their dismissals had been fair. Several applicants who had signed settlement agreements also complained that the agreements had been made under duress owing to the video material and should not have been accepted as evidence that their dismissals had been fair. The Grand Chamber made the following findings:

    - It held that there had been no violation of article 8 of the European Convention in respect of the five applicants. It found in particular that the Spanish courts had carefully balanced the rights of the applicants – who had been suspected of theft by their employer – and those of the employer and thoroughly examined the justification for the video surveillance.
    - A key argument by the applicants was that they had not been given prior notice of the surveillance, despite such a legal requirement, but the ECtHR found that the measure was justified owing to a reasonable suspicion of serious misconduct and to the losses involved, taking account of the extent and the consequences of the measure.
    - The ECtHR concluded that, in the present case, the domestic courts had not exceeded their power of discretion or margin of appreciation in finding that the covert video surveillance was proportionate and legitimate.

In respect of the media, considerations of public interest and the public status of individuals are key in determining whether information should be published. This was affirmed, for instance, in *Radio Twist v Slovakia*, where the ECtHR had cause to consider the unlawful recording of a telephone call that had been broadcast on the radio. The recording was of a conversation among several senior government officials about the privatisation of an insurance company. The recording had been shared anonymously with the radio station. The ECtHR had particular regard for the context and content of the conversation being clearly political in nature and the subject matter of the conversation being of general interest. As to whether the recording was illegal, the ECtHR stated that it was not convinced that the mere fact that the recording had been obtained by a third party contrary to the law justified the applicant's being deprived of their right to freedom of expression. The ECtHR, therefore, held that the radio station had not violated the rights of the persons who were recorded.

Uganda's Intelligent Transport Monitoring System

In August 2023, Uganda's government announced the implementation of an Intelligent Transport Monitoring System to monitor the real-time location of all vehicles in the country, citing national security and public interest as reasons.[63] This system adds to Uganda's existing extensive mass surveillance infrastructure. For instance, the government reportedly acquired 5,552 Huawei CCTV cameras for deployment in public areas, arguing it's essential for national security.[64]

[63] Uganda Infrastructure, Intelligent Transport Monitoring System (ITMS) (accessible here).
[64] Biryabarema,Elias. Uganda's cash-strapped cops spend $126 million on CCTV from Huawei (accessible here).

These actions are significant considering the backdrop. In 2019, the Ugandan government faced accusations of collaborating with Huawei to spy on members of the opposition party, allegedly intercepting their communications, as reported by The Wall Street Journal.[65] Despite strong denials from the government, this incident underscores the dangers to human rights when a government can easily access individual'' data, especially sensitive and personally identifiable information. Such authority in the hands of an authoritarian regime could potentially jeopardize people's lives.

Principle 12(a) of the Global Principles lists the following factors to consider in balancing the rights to freedom of expression and privacy, in situations concerning the publication of personal information:

- The extent to which the publication contributes to a debate of public interest; the degree of notoriety or vulnerability of the person affected;
- The subject covered by the publication and the extent of the private nature of the information at issue;
- The prior conduct of the person concerned;
- The content, form, and consequences of the publication;
- The way in which the information was obtained;
- The intent of the individual or entity disseminating the information at issue, and in particular whether it was malicious; and
- The extent to which the individual whose privacy is at issue is a public figure.[66]

Furthermore, Principle 12 provides that when dealing with the publication of photographs, video footage, or sound recordings, there should be consideration of whether the recording was made voluntarily and with consent. The use of privacy-invasive techniques, such as hidden cameras or undercover reporting, should only be permitted where there is an overriding public interest in the dissemination of the information sought or discovered which could not have been obtained by less invasive means, and where efforts have been made to address or minimise any privacy implications.[67]

5. COLLECTION OF BIOMETRIC DATA AND FACIAL RECOGNITION

Despite the nascent use of biometrics, including facial recognition technology (FRT), many African states lack sufficient regulatory measures.[68] Instead, authorities in various instances are moving towards integrating biometric surveillance into SIM card registration systems, a longstanding concern for digital rights advocates. For instance:

- In **Malawi**, the National Registration and Identification System has been operational since 2017, linking biometric data to voter registration, revenue collection, immigration records, and SIM card registration, as well as banking and financial inclusion

[65] Parkinson, Bariyo. Chin Huawei technicians helped African governments spy on political opponents (accessible here)
[66] ARTICLE 19, 'Global principles on freedom of expression and privacy: A policy brief', (2017) (accessible here).
[67] Principle 12(c) of the Global Principles of Freedom of Expression and Privacy.
[68] Centre for Human Rights, 'The Digital Rights Landscape' (2022) (accessible here) at 28-9.

programs.[69] This system, criticized for its mass data collection without data protection legislation, enables widespread surveillance.

- Similarly, **Tanzania** mandates SIM card registration under the Electronic and Postal Communications (SIM Card Registration) Regulations, 2020, requiring verification against the National Identification Authority (NIDA) database.[70]

5.1. Mandatory SIM card registration

Mandatory SIM card registration is a widespread policy that requires real-name registration for online activity.[71] Mandatory SIM card registration laws typically require that people link their identity to their SIM card in order to activate it, by providing personal information such as a valid identity document, proof of address or biometrics, when purchasing a SIM card for a mobile device.[72] As noted by Privacy International, "[p]repaid SIM card use and mandatory SIM card registration laws are especially widespread in African countries: these two factors can allow for a more pervasive system of mass surveillance of people who can access pre-paid SIM cards, as well as exclusion from important civic spaces, social networks, and education and health care for people who cannot."[73]

Mandatory SIM card registration severely undermines the ability to be anonymous online. It has been explained that: "If almost every mobile device has its SIM card registered to a particular person, and the government can get access to that mobile subscriber information, the people who own and use such devices can be more easily tracked and monitored. Not all people with mobile devices may fall equally under the watchful eye of such surveillance systems: people advocating for change, people who disagree with the government's policies, religious or ethnic minorities, journalists, and human rights defenders are particularly vulnerable."[74]

As of 2022, at least 51 countries in Africa had introduced laws or regulations mandating SIM card registration,[75] with **Lesotho** and **Namibia** beginning rollouts in 2022.[76] Among African states, **Cabo Verde** and **Comoros** were reported not to be considering SIM registration policies, while the situation in **Djibouti** was inconclusive.[77]

Collection of biometric data for the National Integrated Identity Management System (NIIMS) in Kenya

The collection and retention of biometric data present a unique set of privacy concerns. As biometric data can remain relevant for the course of a person's life, the security of this data

[69] Id.
[70] Id.
[71] Id at paras 49-52.
[72] Privacy International, 'Africa: SIM card registration only increases monitoring and exclusion', (2019) (accessible here).
[73] Id.
[74] Id.
[75] GSMA, 'Access to Mobile Services and Proof of Identity 2021', (2021) (accessible here).
[76] BiometricsUpdate.com, 'Lesotho, Namibia join trend of SIM card registration with biometrics' (2022) (accessible here).
[77] GSMA, above n 75, at p 54.

is paramount. Biometric data breaches can result in serious harm to people's rights and interests, including identity theft or fraud, financial loss or other damage.

In January 2020, the High Court of Kenya handed down judgment on the validity of the National Integrated Identity Management System (NIIMS), also known as the Huduma Namba, a national identity registration programme which includes the collection of biometric information. The court ruled that the rollout of NIIMS should not continue without further legislation to guarantee the security of biometric data and to ensure that the system is not exclusionary.[78]

In a subsequent ruling in October 2021, the High Court again halted the NIIMS rollout, albeit temporarily, when it ordered that the programme must be subject to a data impact assessment in terms of Kenya's Data Protection Act.

5.2. Facial recognition

Facial recognition is a form of a biometric system that attracts particular concern for its use in surveillance.[79] Facial recognition technology refers to a wide range of software that can be linked to camera networks; the software analyses live or recorded images and footage of people from a camera network and matches these against images in a pre-existing database in order to identify specific people from the footage.[80] As noted by Privacy International, facial recognition cameras are far more intrusive than regular CCTV: they scan distinct, specific features of your face, such as face shape, to create a detailed map of it – "which means that being captured by these cameras is like being fingerprinted, without your knowledge or consent".[81]

Facial recognition in practice in the United Kingdom

The growing use of facial recognition by police in the United Kingdom has attracted several notable legal challenges.

- In 2019, in *Catt v the United Kingdom*, the European Court of Human Rights found that the UK government had violated the right to privacy in the course of monitoring and profiling a peace activist. In a third-party intervention, Privacy International drew the court's attention to the potential digital technology such as facial recognition to increase any such violation of the right to privacy. The Court noted that the potential for such emerging technologies to violate human rights requires examination "where the powers vested in the state are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated".

[78] Privacy International, , 'Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba', (2022) (accessible here).
[79] American Civil Liberties Union, 'Face recognition technology', (accessible here).
[80] Privacy International 'Facial recognition', (accessible here).
[81] Id.

- In *Bridges v CC South Wales & others*, British civil liberties organisation Liberty acted in a legal challenge against the use of facial recognition technology by police in South Wales. In 2020, the UK Court of Appeal overturned an earlier ruling by finding that the police's use of facial recognition technology breaches privacy rights, data protection laws, and equality laws and that there were "fundamental deficiencies" in the legal framework governing its use.[82]

In this regard, unlike many other biometric systems, facial recognition can be used for general surveillance in combination with public video cameras, and it can be used in a passive way that doesn't require the knowledge, consent, or participation of the subject.[83] As noted by the American Civil Liberties Union, this creates the risk for the technology to be used for general surveillance of a population that is not suspected of any specific wrongdoing. For example, most motor vehicle agencies have high-quality photographs of large numbers of people, which can be a natural source for facial recognition programs and could easily be combined with public or private surveillance camera networks to create a comprehensive system of identification and tracking. Law enforcement agencies also regularly use photographs scraped from social media sites as well.

Interpol has described computerised facial recognition as a relatively new technology which was introduced by law enforcement agencies around the world to identify persons of interest, including criminals, fugitives and missing persons.[84] The Interpol Facial Recognition System contains facial images received from more than 160 countries and coupled with an automatic biometric software application, the system is capable of identifying or verifying a person by comparing and analysing patterns, shapes and proportions of their facial features.[85] Unlike fingerprints and DNA, which do not change during a person's life, facial recognition has to take into account different factors, such as ageing, plastic surgery, cosmetics, the effects of drug abuse or smoking, and the physical pose of the subject.[86]

However, facial recognition technology has also been linked to inaccuracies and biases which raise serious discrimination concerns. A study commissioned by a public agency in the United States found "empirical evidence" that most widely used facial recognition algorithms exhibit "demographic differentials that can worsen their accuracy based on a person's age, gender, or race.[87] Some of the specific findings included the following:[88]

- Facial recognition systems misidentified people of colour more often than white people. Asian and African American people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search.

[82] Liberty, 'Liberty Wins Ground-Breaking Victory Against Facial Recognition Tech,' (2020) (accessible here).
[83] American Civil Liberties Union, 'Face recognition technology', (accessible here).
[84] Interpol, 'Facial recognition', (accessible here).
[85] Id.
[86] Id.
[87] Washington Post, 'Federal study confirms racial bias of many facial recognition systems, casts doubts on their expanding use', (2019) (accessible here)
[88] Id.

- The faces of African American women were falsely identified more often in the kinds of searches used by police investigators, where an image is compared to thousands or millions of others in hopes of identifying a suspect.
- Women were more likely to be falsely identified than men, and the elderly and children were more likely to be misidentified than those in other age groups.

Privacy International notes that the use of facial recognition technology impacts the exercise of at least the following rights:[89]

- **Privacy**: According to Privacy International, "[t]he use of facial recognition in public spaces makes a mockery of our privacy rights". It is a disproportionate crime-fighting technique, as it scans the face of every person who passes by the camera, whether or not they are suspected of any wrongdoing. The biometric data that it collects can be as uniquely identifying as DNA or a fingerprint and is typically done without the consent or knowledge of the data subject.

- **Freedom of expression**: Being watched and identified in public spaces is likely to lead us to change our behaviour, limiting where we go, what we do and with whom we engage. For example, persons might be unwilling to participate in a particular protest action if facial recognition is being used in the area.

- **Equality and non-discrimination**: It has been found that facial recognition software is more likely to misidentify women and black people. There are also concerns that the police use facial recognition to target particular communities.

The roll-out of facial recognition technology is often done without any empowering legal framework to authorise it and is arguably a disproportionate limitation on the right to privacy and other associated rights. In this regard, potential litigation to challenge the use of facial recognition technology may seek to show that it does not meet the threshold of the three-part test for a justifiable limitation, even when used for security purposes.

6. ENCRYPTION AND ANONYMITY ON THE INTERNET

6.1. The interplay between encryption and anonymity

Encryption and anonymity are necessary tools for the full enjoyment of digital rights and protection by virtue of their critical role in securing the rights to freedom of expression and privacy. As described by the United Nations Special Rapporteur (UNSR on FreeEx) on Freedom of Expression:[90]

> "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

[89] Privacy International 'Facial recognition', (accessible here).
[90] Report of the UNSR on Freedom of Expression, 'Report on anonymity, encryption and the human rights framework', A/HRC/29/32, 22 May 2015 (UNSR Report on Anonymity and Encryption) at para 12 (accessible here).

> 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 tools through which individuals may exercise their rights. Accordingly, restrictions on encryption and anonymity must meet the three-part test to justify the restriction.

According to the UNSR on Freedom of Expression, while encryption and anonymity may frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public justification to support any relevant restrictions or to identify situations where the restriction has been necessary to achieve a legitimate goal.[91] The UNSR on Freedom of Expression 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.[92]

6.2. Encryption

Encryption refers to a mathematical process of converting messages, information or data into a form unreadable by anyone except the intended recipient, which in doing so protects the confidentiality and integrity of content against third-party access or manipulation.[93] 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.[94] It is also possible to encrypt data at rest that is stored on one's device, such as a laptop or hard drive.[95]

Outright prohibitions on the individual use of encryption technology disproportionately restrict the right to freedom of expression as it deprives all online users in a particular jurisdiction of the right to carve out a safe space for opinion and expression.[96] 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.[97]

---

[91] Id at para 36.
[92] Id. at paras 59-60.
[93] Id at para 7.
[94] Id.
[95] Id.
[96] Id at para 40.
[97] Id at para 41.

Requirements for cryptography providers in terms of the Electronic Communications and Transactions Act, 2002

Chapter V of the South African Electronic Communications and Transactions Act, 2002 (ECTA) sets out the requirements for cryptography providers. Section 29 of ECTA provides for the establishment and maintenance of a register of cryptography providers, as well as the particulars that must be recorded in the register, including the name and address of the cryptography provider, as well as a description of the type of cryptography service or product being provided. Section 29(3) provides that a cryptography provider "is not required to disclose confidential information or trade secrets in respect of its cryptography products or services."

It should further be noted that some states have implemented – or proposed implementing – so-called 'back door access' in commercially available products, forcing developers to install weaknesses that allow government authorities access to encrypted communications. While the states supporting such measures typically claim that such a framework is necessary to intercept the content of encrypted communications, the UNSR on Freedom of Expression notes that such states have failed to demonstrate that criminal or terrorist use of encryption serves an insuperable barrier to law enforcement objectives.[98] Creating an intentional mechanism to allow a state to bypass security measures would inevitably undermine the security of all users online, with respect to both state and non-state actors.[99]

Further, there is a key role for encryption to play in data protection. It has been noted that companies can reduce both the probability and the harm of a data breach, and thus reduce the risk of fines in the future if they choose to encrypt any personal data in their possession.[100]

Encryption and the GDPR

The GDPR, and many of the data protection laws which follow its model, place responsibility on data controllers and processors to ensure adequate security and protection when processing personal data, which speaks to the role of encryption in data protection. As outlined in an industry advisory:

> "The GDPR deliberately does not define which specific technical and organisational measures are considered suitable in each case, in order to accommodate individual factors. However, it gives the controller a catalogue of criteria to be considered when choosing methods to secure personal data. Those are the state-of-the-art, implementation costs and the nature, scope, context and purposes of the processing. In addition to these criteria, one always has to consider the severity of the risks to the rights and freedoms of the data subject and how likely those risks could manifest. This basically boils down to the following: The

[98] Id at para 42.
[99] Id.
[100] Intersoft Consulting, 'GDPR: Encryption', (accessible here).

> higher the risks involved in the data processing and the more likely these are to manifest, the stronger the taken security measures have to be and the more measures must be taken. Encryption as a concept is explicitly mentioned as one possible technical and organisational measure to secure data in the list of Art. 32(1) of the GDPR, which is not exhaustive. Again, the GDPR does not mention explicit encryption methods to accommodate for the fast-paced technological progress."[101]

Encryption of personal data has additional benefits for controllers or processors; for example, the loss of a state-of-the-art encrypted mobile storage medium which holds personal data may not necessarily be considered a data breach that must be reported to the DPA.[102] In addition, if there is a data breach, the authorities must positively consider the use of encryption in their decision on whether and what amount of a fine is imposed as per article 83(2)(c) of the GDPR.[103]

In 2018, the DPAs of the EU, represented in the Article 29 Working Party (**WP29**), published a statement framing strong and efficient encryption as a vital tool for upholding data protection and privacy rights,[104] noting three key points:

- **Strong encryption ensures a secure, free flow of data between citizens, businesses and governments:** The WP29 noted that there is a strong public interest in the implementation of encryption, as it is crucial to ensure a reasonable guarantee that everyday activities – like buying goods online, filing taxes, using banking services, sending or receiving emails or making an appointment with a physician – can be done securely. The WP29 described encryption as "absolutely necessary and irreplaceable for guaranteeing strong confidentiality and integrity when data are transferred across open networks like the Internet or stored in mobile devices like smartphones". According to the WP29, encryption should ideally always cover the entire communication, from the device of the sender to that of the recipient, commonly referred to as end-to-end-encryption.

- **Backdoors and master keys deprive encryption of its utility:** The WP29 countered the argument that law enforcement should be able to access the encrypted data of suspected criminals by requiring technology providers to implement 'back doors' (i.e. security vulnerabilities deliberately built into a particular software) or 'master keys' (i.e. design features to enable the central decryption of all data encrypted with specific software) in encryption software. The WP29 argued that there is significant historical evidence that master keys and backdoors cannot be kept secure and that there is no way for these technological features to be implemented at any scale without significant risks of compromising people's security. The WP29 also raises concerns that imposing backdoors and master keys on the general population would not be an effective measure against criminals, as criminals would use or adapt to the state-of-the-art encryption to

[101] Id.
[102] Id.
[103] Id.
[104] WP29, 'Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU', (2018) (accessible here).

protect their data, which in turn would only harm 'the honest citizen' by making their data vulnerable.

- **Law enforcement agencies already have legal powers and targeted tools to address the challenge of encryption:** According to the WP29, law enforcement agencies can be legally empowered in other ways to obtain access to data otherwise encrypted, including personal data, for investigations in targeted circumstances. While these powers may raise serious privacy concerns in themselves, the WP29 argues that they appear more proportionate and less dangerous than backdoors or master keys.

Based on the above, the WP29 concluded that encryption must remain standardised, strong and efficient, and encryption providers should never be compelled to include master keys and backdoors in their software.

Advice on how to implement encryption

The ICO recommends the following measures when implementing encryption:[105]

- When implementing encryption, it is important to consider four things: choosing the right algorithm, choosing the right key size, choosing the right software, and keeping the key secure.
- Over time, vulnerabilities may be discovered in encryption algorithms that can eventually make them insecure. You should regularly assess whether your encryption method remains appropriate.
- It is important to ensure that the key size is sufficiently large to protect against an attack over the lifetime of the data. You should therefore assess whether your key sizes remain appropriate.
- The encryption software you use is also crucial. You should ensure that any solution you implement meets current standards, such as FIPS 140-2 and FIPS 197.
- Advice on appropriate encryption solutions is available from a number of organisations.

6.3. Anonymity

In digital contexts, 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 using an invented or assumed name that may not necessarily be associated with one's legal or customary identity.[106] 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.[107]

[105] Information Commissioner's Office (ICO), 'Encryption' (accessible here)
[106] Electronic Frontier Foundation, Anonymity and encryption, (2015) at p 3 (accessible here).
[107] Id.

Anonymity has been recognised for the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation, and debate. As explained by the American Civil Liberties Union (**ACLU**):[108]

> "The right to remain anonymous is a fundamental component of our right to free speech, and it applies every bit as much in the digital world as it does in the physical one. In the words of the U.S. Supreme Court in *McIntyre v. Ohio Elections Commission*, "Anonymity is a shield from the tyranny of the majority."
>
> Unfortunately, the right to remain anonymous has been under steady attack in the online world. Governments and corporations have attempted to unmask unpopular speakers through subpoenas directed at the websites they visit."

Anonymity as an enabler of fundamental rights

Association for Progressive Communications explains:[109]

- Anonymity is closely tied to the right to privacy:
  - Control over shared information and its usage is essential for ensuring privacy protection.
  - Lack of privacy, or even the perception of it, can lead to self-censorship, thus inhibiting freedom of expression.
- Anonymity facilitates the exercise of other rights:
  - It enables the right to freedom of association and assembly online.
  - Provides protection from discrimination.
- The internet's anonymity empowers various groups in the following ways:
  - Enables individuals and minorities to associate on sensitive topics like sexual orientation or religion.
  - Facilitates support for stigmatized issues such as drug addiction, HIV/AIDS, or sexual abuse.
  - Allows engagement in online associations that might be illegal in certain countries, such as LGBT groups, political opposition, or religious minorities.

A number of courts have protected anonymity, both of individual users and of journalistic sources. However, there are also a number of states that prohibit or interfere with anonymity online. In Brazil, for example, anonymity is prohibited by Article 5 of the Federal Constitution, which states that "free expression of thought is assured, prohibiting anonymity," without specifying in which situations this should apply.[110] Although this restriction was designed to prevent individuals from offending and causing damage to the honour and image of third

[108] ACLU, 'Online anonymity and identity', (accessible here).
[109] Association for Progressive Communications (APC), 'The right to freedom of expression and the use of encryption and anonymity in digital communications', February 2015, accessible here).
[110] APC above n 112.

parties, without leaving any trace for identification, it has generated confusion and been used to limit the right to privacy and freedom of expression online and offline.[111]

Anonymity is especially critical in repressive environments in which certain types of protected expression are outlawed, and a lack of anonymity could lead to criminal charges or other consequences.[112] Attempts to ban anonymous speech have particularly been seen during times of protest as a measure aimed at protestors and activists.[113]

Intermediary liability is again of concern in relation to anonymous users, as some states have moved towards imposing responsibilities on internet service providers (ISPs) and media platforms to regulate online comments by anonymous users. For instance, in *Delfi v Estonia*, the ECtHR upheld an Estonian law that imposes liability on a media platform for anonymous defamatory statements posted on its site.[114] However, the ECtHR has also upheld that, while there is no absolute guarantee of online anonymity, the right of freedom of expression should be taken into consideration in decisions to revoke anonymity. This informed the ECtHR's 2021 finding that an Austrian news site should not have been forced to disclose the identity of online commenters who had posted offensive and hateful messages to the platform.[115] In its third-party submissions in that case, Media Defence had previously argued that a court should only order an ISP to disclose user data where:[116]

- An applicant is able to demonstrate to a sufficient degree that a wrongful act has been committed against them and that the information is sought to enable them to seek redress for that wrongful act;
- The anonymous user has been notified, and has had an opportunity to respond to the application;
- There is no less restrictive means of obtaining the information sought; and
- The applicant's interest in disclosure has been sufficiently balanced against the rights to freedom of expression and privacy.

7. SOURCE PROTECTION AND THE PROTECTION OF JOURNALISTIC MATERIALS

7.1. Impact on media freedom

The confidentiality of journalistic sources is central to journalists' ability to properly investigate stories and to the protection of individuals and whistleblowers who provide information to them.[117] Efforts to compel the disclosure of sources have a chilling effect on freedom of speech and media freedom and hinder the free flow of information.[118]

[111] Id.
[112] APC above n 112.
[113] Id. at para 53.
[114] Application No. 64569/09. (2015) (accessible here).
[115] Application No. 39378/15, (2022) (accessible here).
[116] See MLDI's third party intervener submissions in Standard Verlagsgesellschaft MbH, Application No. 39378, (accessible here).
[117] UNESCO, 'Legal standards on freedom of expression: Toolkit for the judiciary in Africa', (2018) at p 123 (accessible here).
[118] Id.

In this regard, General Comment No. 34 to the ICCPR provides that states parties "should recognise and respect that element of the right of freedom of expression that embraces the limited journalistic privilege not to disclose sources." Furthermore, the Africa Commission on Human and Peoples' Rights issued the Declaration of Principles on Freedom of Expression in Africa in 2019, which deals with the issue of protection of sources by providing as follows:

> "Journalists and other media practitioners shall not be required to reveal confidential sources of information or to disclose other material held for journalistic purposes except where disclosure has been ordered by a court after a full and fair public hearing."[119]

The Declaration emphasises that this should only take place where the identity of the source is necessary for the investigation or prosecution of a serious crime, where the information can't be obtained from elsewhere, and whether the public interest in disclosure outweighs the harm to freedom of expression.

It is important to note that the protection of sources has acquired new significance in the digital age in the context of the right to privacy of communications,[120] as surveillance technologies whose development is justified in terms of national security can be used to target journalists and their confidential sources.[121] The Secretary-General of the UN has noted that surveillance activities can have a chilling effect on media freedom and make it more difficult for journalists to communicate with sources and share and develop ideas, which may lead to self-censorship.[122] Similarly, a UN General Assembly resolution on the safety of journalists emphasised that journalists in the digital age are particularly vulnerable to becoming targets of unlawful or arbitrary surveillance, in violation of their rights to privacy and freedom of expression.[123] The resolution further noted that encryption and anonymity tools have become vital to journalists to secure their communications and protect the confidentiality of their sources.

Case notes: the right to source protection in South Africa

In *Bosasa Operations (Pty) Ltd v. Basson and Another*,(2012) the South Africa High Court established a general proposition that journalists are not required to reveal their sources, subject to certain exceptions. The court stated that:

> "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."[124]

[119] ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa,' 2019 at Principle 25, (accessible here).
[120] Id at p 124.
[121] Id at p 124.
[122] Report of the Secretary-General of the UN to the UNGA, 'Report on the safety of journalists and the issue of impunity', A/70/290, (2015) at paras 14-16, (accessible here).
[123] UNGA, 'Resolution on the safety of journalists',(2016) (accessible here).
[124] *Bosasa Operation v. Basson* [2012] ZAGPJHC 7 (accessible here) at para 38.

More recently, in 2023, reaffirming the Bosasa decision, the High Court in *Mazetti Management Services v. Amabhungane Centre for Investigative Journalism* (2023) stated that "resistance to disgorgement of information on the ground of protecting a source is functional and not optional to the work-process of investigative journalism."[125] The Court relied on a plethora of authorities from other jurisdictions and from international courts supportive of affording journalists the proper to protect sources.

Surveillance activities carried out against journalists run the risk of fundamentally undermining the source protection to which journalists are otherwise entitled. Principle 9 of the Global Principles on the Protection of Freedom of Expression and Privacy provides the following about the protection of sources:

> "9.1. The right to freedom of expression implies that everyone who obtains information from confidential sources with a view to exercising a journalistic activity has, subject to Principles 9.2 (a) and (b), a duty not to disclose the identity of their confidential sources and a right not to be required to do so.
> 9.2. States should provide for the protection of the confidentiality of sources in their legislation and ensure that:
> (a) Any restriction on the right to protection of sources complies with the three-part test under international human rights law…;
> (b) 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;
> (c) 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; and
> (d) Any court order under 9.2 (b) and (c) must only be granted after a fair hearing where sufficient notice has been given to the journalist in question, except in genuine emergencies."

Further to this, the United Nations Educational, Scientific and Cultural Organization (UNESCO) has set out that a robust and comprehensive source protection framework would encompass the need to:[126]

- Recognise the value to the public interest of source protection, with its legal foundation in the right to freedom of expression (including press freedom), and to privacy. These protections should also be embedded within a country's constitution and/or national law.
- Recognise that source protection should extend to all acts of journalism and across all platforms, services and mediums (of data storage and publication) and that it includes digital data and meta-data.

[125] *Mazetti Management Services v. Amabhungane Centre for Investigative Journalism NPC* [2023] ZAGPJHC 771 (accessible here) at para 25.
[126] UNESCO, 'Protecting journalism sources in the digital age', (2017) at pp 132-133, (accessible here).

- Recognise that source protection does not entail registration or licensing of practitioners of journalism.
- Recognise the potential detrimental impact on public interest journalism, and on society, of source-related information being caught up in bulk data recording, tracking, storage and collection.
- Affirm that state and corporate actors (including third-party intermediaries), who capture journalistic digital data must treat it confidentially (also acknowledging the desirability of the storage and use of such data being consistent with the general right to privacy).
- Shield acts of journalism from targeted surveillance, data retention and handover of material connected to confidential sources.
- Define exceptions to all the above very narrowly, so as to preserve the principle of source protection as the effective norm and standard.
- Define exceptions as needing to conform to a provision of "necessity" and "proportionality" – in other words, when no alternative to disclosure is possible, when there is a greater public interest in disclosure than in protection, and when the terms and extent of disclosure still preserve confidentiality as much as possible.
- Define a transparent and independent judicial process with appeal potential for authorised exceptions and ensure that law-enforcement agents and judicial actors are educated about the principles involved.
- Criminalise arbitrary, unauthorised and wilful violations of confidentiality of sources by third-party actors.
- Recognise that source protection laws can be strengthened by complementary whistleblower legislation.

UNESCO has further noted that there is a particular gender dimension that arises with respect to source protection in the digital age. Women journalists face additional risks in the course of their work, both on- and offline: in the physical realm, these risks include sexual harassment, physical assault and rape, which may limit their physical mobility; and in the digital sphere, acts of harassment and threats of violence are rampant.[127] Similarly, female sources face increased risks when acting as whistleblowers or confidential informants.[128] As such, women journalists need to be able to rely on secure, non-physical forms of communication with their sources, in particular secure digital communications, to be able to engage with their sources.[129]

Digital safety and security are paramount for both female journalists and sources

In 2017, UNESCO highlighted the heightened risks faced by women journalists due to the interception and analysis of journalistic communications.[130] This practice not only endangers the physical safety of women journalists and their sources but also undermines the confidentiality necessary for effective reporting. Encrypted communications and other defensive measures were noted as crucial to safeguard movements and protect the anonymity of sources. UNESCO further recorded that the risks are even greater for female

[127] Id at p 134.
[128] Id.
[129] Id.
[130] UNESCO, 'Protecting journalism sources in the digital age' (2017) (accessible here).

whistleblowers, who rely on secure digital communication methods to minimize detection and ensure their stories reach the public and called for robust legal protections, applied with gender sensitivity, are essential to safeguard confidentiality, particularly in cases where judicial orders compel disclosure.

In 2022, the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression highlighted the disproportionate targeting of women journalists in some countries through digital surveillance, amounting to a form of gender-based violence.[131] Surveillance practices not only compromise the personal information of women journalists but also deter confidential sources from communicating, chilling whistle-blowing and investigative journalism. The extraterritorial reach of digital surveillance expands state control over expression globally, potentially stifling investigative reporting at an international level. The report recommends incorporating adequate safeguards in national laws, including judicial oversight, to ensure that digital surveillance activities uphold international standards on the protection of journalists and their sources. Additionally, it calls for holding surveillance companies accountable for the foreseeable misuse of their technology and amending sovereign immunity laws to enable civil action against states engaged in cross-border digital attacks on journalists.

8. ONLINE HARASSMENT

Harassment, threats, and online violence severely restrict the enjoyment that persons have of their rights online, particularly vulnerable, and marginalised groups, including women and members of sexual minorities. For more online violence, see Media Defence Modules on Online Violence against Journalists in Sub-Saharan Africa.

Social media platforms are especially fertile ground for online harassment, but these behaviours occur in a wide range of online venues.[132] For those who experience online harassment directly, these encounters can have profound real-world consequences, ranging from mental or emotional stress to reputational damage or even fear for one's personal safety.[133] Furthermore, whether one is affected directly or indirectly by it, it can lead to significant self-censorship to avoid incurring such harassment.

While the internet provides a forum for people to seek information about their identities and sexual orientation, and to express themselves on these topics, many people suffer a wide range of attacks in doing so, including attacks on sexuality, exposing personal information, and the manipulation of images that are then used for blackmail and destroying credibility. Furthermore, a common trend amongst children using the internet involves so-called 'cyberbullying'. Research has shown that online harassment is often focused on personal or physical characteristics, with political views, gender, physical appearance, and race being

[131] UNHRC, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression - Reinforcing media freedom and the safety of journalists in the digital age' (2022) (accessible here).
[132] Id.
[133] Id.

among the most common.[134] Furthermore, women encounter sexualised forms of online harassment at much higher rates than men.[135]

A particular form of online harassment, typically towards women, is that of the non-consensual publication of a person's intimate or sexually explicit photographs or videos. This constitutes a gross violation of a person's privacy, often for the purposes of extortion, blackmail, and/or humiliation. Several recently enacted cybercrime laws in Southern Africa criminalise the non-consensual distribution of private sexual photographs and films – most notably in Botswana and South Africa.[136]

Ongoing harassment and attacks on members of the media have become a particularly worrying trend. As stated in the preamble to the 2011 African Commission Resolution on the Safety of Journalists and Media Practitioners in Africa, freedom of expression, press freedom and access to information can only be enjoyed when journalists and media practitioners are free from intimidation, pressure, and coercion.

Types of online harassment

PEN America has provided a useful glossary of terms relating to various forms of online harassment:[137]

- **Cyberbullying**: An umbrella term (like "online harassment") meant to encompass a number of harassing online behaviours. Like physical bullying, "cyberbullying" is generally aimed at young people and may involve threats, embarrassment, or humiliation in an online setting.

- **Cyber mob attacks**: Cyber-mob attack occurs when a large group gathers online to try to collectively shame, harass, threaten, or discredit a target. Targets overwhelmingly belong to traditionally marginalized groups. "Outrage mobs" or "shaming mobs" are a distinct kind of cyber mob made up of internet users who collectively troll individuals in the hopes of silencing or publicly punishing them. Targets of outrage mobs are often attacked for expressing opinions on politically charged topics or ideas the outrage mob disagrees with and/or has taken out of context in order to promote a particular agenda. Outrage mobbing can sometimes have severe consequences offline and has even resulted in targets losing their jobs.

- **Cyberstalking**: In a legal context, "cyberstalking" is the prolonged use (a "course of conduct") of online harassment intended to kill, injure, harass, intimidate, or place under surveillance a target. Cyberstalking can comprise a number of harassing behaviours committed repeatedly or with regularity that usually cause a target to suffer fear, anxiety, humiliation, and extreme emotional distress.

[134] Id.
[135] Id.
[136] MISA Zimbabwe, 'Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights,' (2021) (accessible here).
[137] PEN America, 'Defining online harassment: A glossary of terms', (accessible here).

- **Denial of service (DoS) or Distributed Denial-of-Service (DDoS) attacks**: A DoS attack is a cyberattack that temporarily or indefinitely disrupts internet service by overwhelming a system with data, resulting in the web server crashing or becoming inoperable. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (such as banking), or other services that rely on the affected computer. In a DDoS attack, an attacker takes control of one user's computer in order to attack a different user's computer. This can force the hijacked computer to send large amounts of data to a particular website or send spam to targeted email addresses.

- **Doxing (or doxxing)**: Doxing involves publishing someone's sensitive personal information online in an attempt to harass, intimidate, extort, stalk, or steal the identity of a target. "Sensitive information" can include social security numbers, phone numbers, home addresses, personal photos, employment information, email addresses, and family members' personal information.

- **Hateful speech and online threats**: By far the most common form of online harassment, hateful speech or threats, both explicit and implicit, can be issued by an ill-intentioned internet user pretty much anywhere on the web. Hateful speech is a form of expression attacking a specific aspect of a person's identity, such as one's race, ethnicity, gender identity, religion, sexual orientation, or disability. Hateful speech online often takes the form of ad hominem attacks, which invoke prejudicial feelings over intellectual arguments in order to avoid discussion of the topic at hand by attacking a person's character or attributes. Threats issued online can be just as frightening as they are offline and are frequently meant to be physically or sexually intimidating.

- **Message bombing**: "Message bombing" is the intentional flooding of a person's or institution's phone or email accounts with messages meant to limit or block a user's access to a device's operating system or platform. Because large numbers of messages sent in a short period of time can typically render a person's account unusable, this is an effective way for a harasser to prevent you from using your devices or accessing your online accounts. Message bombing typically occurs over texting apps, chat apps, or email accounts.

- **Non-consensual, intimate images and videos (such as "revenge porn")**: The dissemination of non-consensual intimate images **(NCII)** – often called "revenge porn" – is the distribution of private, sexual or intimate images or videos of a person without their consent. This can also fall under the category of "sextortion," i.e. the threat of distributing a nude or sexually explicit image or video in an effort to blackmail an individual.

- **Online impersonation**: "Online impersonation" is a strategy whereby harassers create hoax social media accounts, usually in order to post offensive or inflammatory statements in your name. In most cases, the harasser's intention is to defame or discredit you, often by convincing others to believe the fake quotes attributed to you, which might then incite others to commit additional acts of harassment. Impersonation

trolling can also happen when a harasser impersonates someone you know in order to offend or hurt you.

- **Online sexual harassment**: Online sexual harassment – which is targeted at women at a far higher rate than men – encompasses a wide range of sexual misconduct on digital platforms and includes some of the more specific forms of online harassment, such as "revenge porn". It often manifests as hateful speech or online threats. There are four distinct types of online sexual harassment: non-consensual sharing of intimate images and videos; exploitation, coercion and threats; sexualised bullying; and unwanted sexualisation.

- **Trolling**: "Trolling" is one of those terms that's evolved so much over time as to have no single agreed-upon meaning. The term "trolling" is defined here as the repetitive posting of inflammatory or hateful comments online by an individual whose intent is to seek attention, intentionally harm a target, cause trouble and/or controversy, and/or join up with a group of trolls who have already commenced a trolling campaign. There are three subcategories of trolling to be aware of: concern trolling, where harassers pose as fans or supporters of your work with the intention of making harmful or demeaning comments masked as constructive feedback; dogpiling, where a group of trolls works together to overwhelm a target through a barrage of disingenuous questions, threats, slurs, insults, and other tactics meant to shame, silence, discredit, or drive a target offline; and botnet or sock-puppet trolling, which are used for a variety of reasons, from promoting propaganda to amplifying hate or defamation against targeted individuals.

A recent research report on online gender-based violence (OGBV) in Southern Africa has uncovered alarming trends regarding the escalation of online harm in the region.[138] The report examines patterns and policy frameworks related to OGBV across eight SADC countries: **Angola**, **Botswana**, **Malawi**, **Mozambique**, **Namibia**, **South Africa**, **Zambia**, and **Zimbabwe**. Additionally, it offers specific recommendations tailored to each country and underscores that the region is not immune to the growing threat of OGBV. Particularly concerning are the identified issues of inadequate legal safeguards and insufficient governmental responses.

Research on 48 African countries reveals a stark reality: 36 lack specific cyber-harassment laws, while an additional 9 have legislation that overlooks sexual harassment, leaving only 3 countries (6%) with laws addressing sexual harassment in cyber contexts.[139] For example, **South Africa's** Cybercrimes Act of 2019 criminalizes cyber-bullying and cyber-extortion, while the Electronic Communications and Transactions Act of 2002 covers various forms of electronic harassment. Nigeria's Cybercrimes Act of 2015 offers a comprehensive definition of cyber-harassment and outlines specifically related offences.

[138] Centre for Human Rights et al, 'Understanding Online Gender-based violence in Southern Africa', 2022 (accessible here).
[139] World Bank, 'Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws,' (2023) (accessible here).

Arguably, one of the key challenges is in getting lawmakers and law enforcement officials to recognise the severity of such harassment and threats, and to treat it with the appropriate levels of concern, recognising that the real and persistent harm suffered applies whether the harassment and threats take place online or offline. Two further challenges that arise that are exacerbated in the online sphere relate to the volume of threats that can be received, given the relative ease with which this can be done via social media platforms, for instance; and the concurrent difficulties in identifying perpetrators who are sometimes able to mask their online identities.

This ties in with the issue of anonymity online. This is because one of the particular challenges with online harassment is that perpetrators may mask their identities, making it difficult for law enforcement officials to apprehend them. This, however, should not be seen as a sufficient basis to allow for a blanket ban on anonymity or encryption online. The UNSR on Freedom of Expression has responded to this concern and has stated that:[140]

> "The "dark" side of encryption and anonymity is a reflection of the fact that wrongdoing offline takes place online as well. Law enforcement and counter-terrorism officials express concern that terrorists and ordinary criminals use encryption and anonymity to hide their activities, making it difficult for Governments to prevent and conduct investigations into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives. Harassment and cyberbullying may rely on anonymity as a cowardly mask for discrimination, particularly against members of vulnerable groups. At the same time, however, law enforcement often uses the same tools to ensure their own operational security in undercover operations, while members of vulnerable groups may use the tools to ensure their privacy in the face of harassment. Moreover, Governments have at their disposal a broad set of alternative tools, such as wiretapping, geo-location and tracking, data-mining, traditional physical surveillance and many others, which strengthen contemporary law enforcement and counter-terrorism."

Where journalists allege imminent threats to their safety, courts are empowered to grant interdictory relief in appropriate circumstances and subject to the relevant legal requirements. For instance, in the matter of *South African National Editors Forum and Others v Black Land First and Others*,[141] the South African high court granted an interdict in favour of the media broadly, in terms of which the respondents were interdicted from "engaging in any of the following acts directed towards the applicants: Intimidation; Harassment; Assaults; Threats; Coming to their homes; or acting in any manner that would constitute an infringement of their personal liberty", and from "making any threatening or intimidating gestures on social media … that references any violence, harm and threat".[142]

Protection orders – South Africa

South Africa's Protection From Harassment Act (Harassment Act) safeguards victims' rights against harassment and enables the issuance of protection orders that can be invoked against online conduct aimed at causing harm.[143] The Act defines sexual harassment broadly,

[140] UNSR Report on Anonymity and Encryption at para 13.
[141] *South African National Editors Forum and Others v Black Land First and* Others (accessible here).
[142] Id. at para 29.
[143] See Power & Associates, 'Online Sexual Harassment Toolkit' (2021) (accessible here)

encompassing unwelcome sexual attention, explicit or implicit sexual behaviour, promises or threats for sexual compliance, and provides provisions for applying for protection orders, which mandate the cessation of harassing behaviour. Notably, the Act empowers courts to compel electronic service providers to furnish information pertaining to online harassment incidents, aiding in identifying perpetrators utilizing electronic communication methods such as email, text, or phone. This provision, known as a direction, allows courts to gather necessary details for addressing online harassment complaints effectively.

When a court issues a direction to an electronic service provider (ESP) where the identity of the respondent is unknown the court will ask the ESP for the following information:

- Details (the electronic communications identity number) about where the harassing electronic communications or electronic mail originated.
- The name, surname, identity number and address of the respondent to whom the electronic communications identity number has been assigned.
- Date and time on which electronic communications were received by the complainant. o Duration of communication received by the complainant.
- Any other information that is available to an electronic communications service provider may be of assistance to the court to identify the respondent

As stated in the 2016 UN Resolution on the Safety of Journalists, impunity for attacks against journalists constitutes one of the greatest challenges to the safety of journalists and ensuring accountability for crimes committed against journalists is a key element in preventing future attacks. More recently the UNHRC, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression explained

> "Online attacks against women journalists are one of the most serious contemporary threats to their safety, gender equality and media freedom. Vicious, coordinated, highly sexualized and malicious, the attacks often target women from religious and ethnic minorities or gender non-conforming people."[144]

UNESCO has found that online violence targeting women journalists[145] aims to belittle and intimidate them, fostering a climate of fear and withdrawal.[146] It further seeks to tarnish their professional credibility, undermining trust in the media. This "amounts to an attack on democratic deliberation and media freedom, encompassing the public's right to access information, and it cannot afford to be normalised or tolerated as an inevitable aspect of online discourse, nor contemporary audience-engaged journalism."[147] The right to be free from discrimination, threats, and violence applies both off- and online. Countering online violence

[144] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on reinforcing media freedom and the safety of journalists in the digital age' (2022) (accessible here) at para 36 (UNSR on FreeEx Report).
[145] For conciseness, we refer hereafter to "women+" to include all those who identify as women and those with marginalised or at-risk identities including members of the LGBTQI+ community, except where specific instruments or documents referenced refer explicitly to "women" or some other grouping.
[146] UNESCO 'The Chilling: Global trends in online violence against women journalists' (2021) (accessible here) at 6 (The Chilling).
[147] Id.

that targets women journalists is critical to the promotion of, among others, the rights to freedom of expression, media freedom, and privacy.

Principle 20 of the Declaration of Principles on Freedom of Expression in Africa provides that states must guarantee the safety of journalists and take measures to prevent attacks on them, as well as take effective legal steps to investigate and prosecute attacks against journalists. It further calls on states to take specific measures to ensure the safety of female journalists by addressing gender-specific safety concerns, including sexual and gender-based violence, intimidation, and harassment.[148]

General Comment No. 34 provides that an attack on any person because of the exercise of his or her right to freedom of expression, including forms of attack such as arbitrary arrest, torture, threats to life and killing, cannot be justified under article 19 of the ICCPR.[149] It states further that journalists, as well as other persons involved in gathering and analysing information about human rights situations such as lawyers and judges, are frequently subjected to threats, intimidation and attacks because of their activities.[150]

Although it is clear that what is required in the face of online attacks is swift and firm justice, the reality is that many perpetrators commit such with impunity.[151] Impunity perpetuates a cycle of violence: it raises serious concern that such attacks going unpunished send a public signal that the state and public authorities do not take such attacks seriously.[152]

There is therefore clear guidance under international law that states must take measures to protect persons, including members of the media, against such harassment and attacks. This is so whether the harassment takes place offline or online.

Tips for digital safety to protect against online harassment and trolling

- Create long and strong passwords for your accounts. (Password managers are useful tools to be able to remember the different passwords used for different accounts.)
- Turn on two-factor authentication.
- Review your privacy settings for each account and make sure any personal data, such as phone numbers and date of birth, is removed.
- Look through your accounts and remove any photos or images that could be manipulated and used as a way to discredit you.
- Consider getting your account verified by the social media company.
- Monitor your accounts for signs of increased trolling activity or for indications that a digital threat could become a physical threat.[153]
- Speak with family and friends about online harassment

[148] Africa Declaration above n 121.
[149] General Comment No. 34 at para 23.
[150] General Comment No. 34 at para 23.
[151] South African National Editors' Forum, 'South Africa 2019 elections: Handbook for journalists', (2019) (accessible here).
[152] Id.
[153] See Committee for the Protection of Journalists, 'South Africa elections 2019: Journalist safety toolkit' (2019) (accessible at here).

9. CONCLUSION

The right to privacy has encountered many new challenges in the digital era. The rapid and widespread adoption of data processing has raised concerns for the protection of personal information, leading to a raft of new data protection laws being passed across the world, and efforts to engender accountability for government and private-sector-led surveillance based on invasive new technologies including facial recognition.

It has also resulted in a need to find the appropriate balance between protecting freedom of expression by enabling anonymity and encryption online while ensuring accountability for crimes committed in the digital sphere. Generally, wholesale prohibitions on anonymity and encryption are seen as disproportionate infringements on the right to freedom of expression, and in recent years international law guidance for states and private actors on these issues has become robust.

These digital rights challenges have particular resonance for journalists who operate online and often bear the brunt of efforts to surveil or intrude in their private communications, including facing high levels of online abuse and harassment. Women journalists are particularly targeted in this regard. It is vital that states take steps to protect journalists in the online sphere and to align their legislative frameworks with the international guidance that exists in order to ensure the protection of freedom of expression in the modern era.