Module 4

DATA PRIVACY AND DATA PROTECTION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

Published by Media Defence: www.mediadefence.org
This module was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in December 2020
Revised in November 2022

TABLE OF CONTENTS

INTRODUCTION 1
THE RIGHT TO PRIVACY 1
DATA PROTECTION 3
'THE RIGHT TO BE FORGOTTEN' 6
ENCRYPTION AND ANONYMITY ON THE INTERNET 9
GOVERNMENT-LED DIGITAL SURVEILLANCE 11
CONCLUSION 14

MODULE 4

DATA PRIVACY AND DATA PROTECTION

- **The right to privacy and data protection is a growing concern due to increasing data flows and the resulting need for the protection of personal information.**
- **In the African context, there are multiple instruments which govern data protection, notably the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention).**
- **Importantly, states should ensure that their domestic legislation provides for the lawful processing of personal information and that they keep step with data protection developments.**
- **Allied with data protection are the concepts of the 'right to be forgotten,' encryption, and government-led surveillance.**
- **Communications surveillance has special risks for freedom of expression in journalistic contexts due to the potential disclosure of confidential sources and the risk of a chilling effect on media freedom.**

INTRODUCTION

The right to privacy and the concomitant requirement to protect personal information has garnered significant attention in the information age. The spread of internet access and the digitisation of many parts of public and private life have led to sharp increases in online information-sharing and data collection, yet legislative developments have failed to keep pace and adequately protect personal information. However, African states and regional and continental bodies have begun to develop various data protection instruments and regulations in an attempt to remedy and vindicate the privacy rights of their citizens.

This module focuses on data protection in Africa and the related concepts of the 'right to be forgotten' and encryption, and emerging principles and safeguards relating to surveillance.

THE RIGHT TO PRIVACY

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

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

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

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

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

These, in addition to the African Charter's protections for freedom against discrimination, liberty and security, freedom of assembly, health, and others, have prompted the argument that the implicit right to privacy should be 'read into' the African Charter as an inalienable component of those other rights.[1] While this approach has not been tested in relation to the Charter, it would follow the approach of the Supreme Court of India in its 2017 ruling that the right to privacy is protected as an intrinsic part of the right to life and personal liberty, and as part of the fundamental freedoms guaranteed by Part III of the Constitution of India.[2] As such, although the Constitution of India does not expressly contain a right to privacy, the right can nevertheless be read when considered in the context of the other rights and freedoms that are constitutionally guaranteed.

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

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

The 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa, adopted by the African Commission on Human and Peoples' Rights (ACHPR), also explicitly acknowledges the right to privacy and calls on states to provide extensive protections

[1] Ayalew, ' Untrodden Paths Towards the Right to Privacy in the Digital Era under African Human Rights Law' *12 International Data Privacy Law 1*, (2022) (accessible at https://ssrn.com/abstract=3993942).

[2] *Justice K.S. Puttaswamy and Another v Union of India and Others*, Petition No. 494/2012, (2017) (accessible at: http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf).

for privacy and personal information.[3] Moreover, almost all African states guarantee this right under their domestic constitutions.[4]

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

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

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

DATA PROTECTION

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

Most comprehensive data protection laws make provision for the following principles:[6]

- Personal information must be processed fairly and lawfully and must not be processed unless the stipulated conditions are met.
- Personal information must be obtained for a specified purpose (or purposes) and must not be further processed in any manner incompatible with that purpose.
- Personal data must be adequate, relevant and not excessive in relation to the purpose (or purposes) for which it is processed.

---

[3] Principles 40-42.

[4] At the domestic level, more than 50 African constitutions, inclusive of amendments and recent reviews, include reference to the right to privacy. Singh and 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 at: http://www.pulp.up.ac.za/images/pulp/books/journals/AHRY_2019/Power%202019.pdf). See also www.dataprotection.africa for an updated list.

[5] *NM and Others v Smith and Others*, [2007] ZACC 6, (2007) at para 33 (accessible at: https://www.saflii.org/za/cases/ZACC/2007/6.html), citing with approval *Bernstein and Others v Bester NNO and Others*, [1996] ZACC 2, (1996) at para 77.

[6] Information Commissioner's Office, 'Data protection principles' (accessible at: https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/).

- Personal information must be accurate and, where necessary, kept up to date.
- Personal information must not be kept for longer than is necessary for the purpose of collection.
- Personal information must be processed in accordance with the rights of data subjects provided for under the data protection law.
- Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to another country that does not ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

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

The United Nations Special Rapporteur on the Right to Privacy in 2022 released a report providing an in-depth analysis of the principles of legality, lawfulness and legitimacy, consent, transparency, purpose, fairness, proportionality, minimisation, quality, responsibility, and security in the context of data protection legislation, which serves as a seminal guide for the development and harmonisation of data protection regulations around the world.[7]

Data protection is one of the primary measures through which the right to privacy is given effect. At least 33 African states have so far enacted data protection laws, and more are in the process of doing so.[8] In addition to giving effect to the right to privacy, data protection legislation also facilitates trade among states, as many data protection laws restrict cross-border data transfers in circumstances where the state receiving the information does not provide an adequate level of data protection – or framed more positively, data protection laws enable the regulated transfer of personal information across borders where both jurisdictions have put in place adequate data protection laws and procedures.

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

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

[7] Accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/594/48/PDF/N2259448.pdf?OpenElement.

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

[9] General Comment No. 16 at para 10.

individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."

There are a number of African regional instruments that deal with data protection:

- **AU Convention on Cyber Security and Personal Data Protection 2014**[10] (the Malabo Convention): This instrument, aimed at a continental level, includes provisions relating to data protection, e-transactions, cybercrimes and cybersecurity. The provisions relating to data protection are contained in Chapter II and contain the conditions for the lawful processing of personal information, as well as the rights afforded to data subjects. Although it has not entered into force as yet, once it is brought into operation it would be a binding legal instrument for data protection in Africa.[11]
- **Draft EAC Legal Framework for Cyberlaws 2008**[12] (EAC Legal Framework): This instrument covers topics relating to data protection, electronic commerce, data security and consumer protection. It is not intended to be a model law but instead provides guidance and recommendations to states to inform the development of their laws. Data protection is dealt with briefly at paragraph 2.5 of the EAC Legal Framework.
- **Supplementary Act on Personal Data Protection within ECOWAS 2010**[13] (ECOWAS Supplementary Act): This instrument is designed to be directly transposed into a domestic context among West African states, and provides in detail for the conditions for lawful processing of personal information and the rights of data subjects.
- **SADC Data Protection Model Law 2013**[14] (SADC Model Law): This instrument is a model law that can be adapted into domestic contexts among Southern African states. It seeks to ensure the harmonisation of information and communications technologies (ICT) policies and recognises that ICT developments impact the protection of personal data, including in government and commercial activities. It also deals with whistle-blowing, by providing that the data protection authority must establish rules to govern the whistleblowing system that preserve data protection principles, including the principles of fairness, lawfulness, purpose specification, proportionality, and openness.

In addition to giving effect to the right to privacy, data protection laws also typically facilitate a right of access to information, by providing for data subjects to request, and be given access to, the information being held about them by a controller. This mechanism can enable data

[10] Accessible at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

[11] At present, thirteen of the required fifteen states have ratified the Malabo Convention. (accessible at: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf).

[12] Accessible at: http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y.

[13] Accessible at: http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

[14] Accessible at: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf.

subjects to determine whether their personal information is being processed in line with applicable data protection laws and whether their rights are being upheld.

Mapping the state of data protection in Africa

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

'THE RIGHT TO BE FORGOTTEN'

The 'right to be forgotten'[15] – which is perhaps better described as 'the right to erasure' or 'the right to be de-listed' – entails a right to request that commercial search engines, or other websites that gather personal information for profit, remove links to private information when asked, subject to a balancing of public and individual interests. The right to be forgotten progresses from the right of data subjects contained in many data protection laws that personal information held about a person should be erased in circumstances where it is inadequate, irrelevant, or no longer relevant, or excessive in relation to purposes for which it was collected.

The right to be forgotten was established in a 2014 ruling of the Court of Justice of the European Union (CJEU) in the case of *Google Spain v Gonzalez*.[16] Mr Gonzalez, a Spanish national, lodged a complaint in 2010 with the Spanish information regulator. The cause of Mr Gonzalez's complaint was that any search for his name on Google's search engine prominently displayed old news articles about debt proceedings against him. Mr Gonzalez requested that the personal data relating to him, which was over a decade old, be removed or concealed because the proceedings had been fully resolved and the reference to him was now irrelevant.

The CJEU upheld the claim, relying on the EU data protection law in effect at the time. The CJEU noted that the very display of personal information on a search results page constitutes processing of such information,[17] and there was no reason why a search engine should not be subject to the obligations and guarantees laid out under the law.[18] Further, it was noted that the processing of personal information carried out by a search engine can significantly affect the fundamental rights to privacy and to the protection of personal data when a search is carried out of a person's name, as it enables any internet user to establish a profile of the

[15] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

[16] *Google Spain SL and Another v Agencia Española de Protección de Datos (AEPD) and Another*, Case No. C-131/12, (2014) (accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131).

[17] *Id* at para 57.

[18] *Id* at para 58.

person.[19] According to the CJEU, the effect of the interference "is heightened taking into account the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous."[20]

With regard to de-listing, the CJEU held that the removal of links from the list of results could, depending on the information at issue, have effects on the legitimate interests of internet users seeking access to that information.[21] This would require a fair balance to be struck between those interests and the data subject's fundamental rights, taking into account the nature of the information, its sensitivity for the data subject's private life, and the interest of the public in having that information, which may vary according to the role played by the data subject in public life.[22]

The CJEU went on to hold that a data subject is permitted to request that information about them be removed from search results where, having regard to all the circumstances, the information appears to be inadequate, irrelevant or no longer relevant, or excessive in relation to purposes of the processing carried out by the operator of the search engine.[23] In such circumstances, the information and links concerned in the list of results must be erased.[24]

The right to be forgotten has also been recognised in domestic contexts. For instance, in a de-listing dispute between a publisher and a local restaurant owner, Italy's Supreme Court of Cassation held that the public interest in retaining access to a news article about a fight at the restaurant diminished over time, and that sensitive and private information should not be available to the public indefinitely.[25] The European Court of Human Rights (**ECtHR**) subsequently upheld the decision.[26] In the case of *Hurbain v Belgium*, the ECtHR upheld an order requiring the anonymisation of a person involved in a road accident and was not a breach of the publisher's freedom of expression.[27] The Belgian Court of Cassation has also recognised the right to be forgotten,[28] as has the State Court of Appeals of São Paulo, Brazil.[29]

---

[19] *Id* at para 80.

[20] *Id.*

[21] *Id* at para 81.

[22] *Id*.

[23] *Id*. at para 94.

[24] *Id*. at para 94.

[25] *Plaintiff X v PrimaDaNoi*, Case No. 13161, (2015) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/plaintiff-x-v-primadanoi/).

[26] European Court of Human Rights, Application no. 77419/16 (2022) (accessible at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-213827%22]}).

[27] *Hurbain v Belgium*, Application no. 57292/16, (2021) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/hurbain-v-belgium/).

[28] *P.H. v O.G.*, Case No. 15/0052/F, (2016) (accessible at: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/06/download_blob.pdf). For a discussion of the case, see Hunton & Williams, 'Belgian Court of Cassation rules on right to be forgotten', 1 June 2016 (accessible at: https://www.huntonprivacyblog.com/2016/06/01/belgian-court-of-cassation-rules-on-right-to-be-forgotten/).

For more on the right to be forgotten, see *NT1 & NT2 v Google LLC* in the UK (2018) (accessible at: https://www.judiciary.uk/wp-content/uploads/2018/04/nt1-nt2-v-google-press-summary-180413.pdf).

[29] De Queiroz v. Google Brasil Internet Ltda. Case No. 0004144-77.2015.8.26.0297 (2016) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/de-queiroz-v-google-brasil-internet-ltda/).

The Supreme Court of Chile, in 2019, made an order requiring several digital media outlets to update information they had published about a person involved in a criminal case in order to achieve a balance between the right to information that was in the public interest and the right to honour.[30]

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

There are, however, limits to the ambit of the right to be forgotten. In 2017, the CJEU was seized with a request for a preliminary ruling in the case of *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*.[31] Mr Manni, relying on the *Gonzalez* decision, sought an order requiring the Chamber of Commerce to erase, anonymise or block any data linking him to the liquidation of his company contained in the companies register. The CJEU declined to uphold Mr Manni's request and held that in light of the range of possible legitimate uses for data in company registers and the different limitation periods applicable to such records, it was impossible to identify a suitable maximum retention period. Accordingly, the CJEU declined to find that there is a general right to be forgotten from public company registers.

Furthermore, other jurisdictions have refused to uphold a right to be forgotten against search engines. In Brazil, for example, it was held that search engines cannot be compelled to remove search results relating to a specific term or expression;[32] similarly, the Supreme Court of Japan declined to enforce the right to be forgotten against Google, finding that deletion "can be allowed only when the value of privacy protection significantly outweighs that of information disclosure".[33]

According to the Global Principles of Freedom of Expression and Privacy (Global Principles),[34] the right – to the extent that it is recognised in a particular jurisdiction – should be limited to the right of individuals under data protection law to request search engines to delist inaccurate or out-of-date search results produced on the basis of a search for their name[35] and should be limited in scope to the domain name corresponding to the country where the right is recognised and the individual has established substantial damage.[36] It states further that de-

[30] Surgeon v. Court of Appeals of Santiago, Case No. Rol No. 1279-2019 (2019) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/surgeon-v-court-of-appeals-of-santiago/).

[31] Case No. C-385-15, (2017) (accessible at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=446798).

[32] *Ministra Nancy Andrighi v Google Brasil Internet Ltd and Others*, 2011/0307909-6, (2012) (accessible at: https://www.internetlab.org.br/wp-content/uploads/2017/02/STJ-REsp-1316921.pdf).

[33] The Japan Times, 'Top court rejects 'right to be forgotten' demand', (2017) (accessible at: https://www.japantimes.co.jp/news/2017/02/01/national/crime-legal/top-court-rejects-right-forgotten-demand/#.WqZQXehubIV).

[34] The Global Principles (accessible at: https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf) were developed by civil society, led by ARTICLE19, in cooperation with high-level experts from around the world.

[35] Principle 18(1) of the Global Principles.

[36] *Id* at principle 18(4).

listing requests should be subject to ultimate adjudication by a court or independent adjudicatory body with relevant expertise in freedom of expression and data protection law.[37]

ENCRYPTION AND ANONYMITY ON THE INTERNET[38]

Encryption refers to a mathematical process of converting messages, information or data into a form unreadable by anyone except the intended recipient, and in doing so protecting the confidentiality and integrity of content against third-party access or manipulation.[39] 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.[40] It is also possible to encrypt data at rest that is stored on one's device, such as a laptop or hard drive.[41]

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.[42] 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.[43]

Encryption and anonymity are necessary tools for the full enjoyment of digital rights and deserve protection by virtue of the critical role that they play in securing the rights to freedom of expression and privacy. As described by the United Nations Special Rapporteur (**UNSR**) on freedom of expression:[44]

> "Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent

[37] *Id* at principle 18(2).

[38] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

[39] Report of the UNSR on Freedom of Expression, 'Report on anonymity, encryption and the human rights framework', A/HRC/29/32, (2015) (UNSR Report on Anonymity and Encryption) at para 7 (accessible at: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx). For further discussion and resources, see UCI Law International Justice Clinic, 'Selected references: Unofficial companion report to Report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and freedom of expression' (accessible at: http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/Selected_References_SR_Report.pdf).

[40] *Id*.

[41] *Id*.

[42] Electronic Frontier Foundation, *Anonymity and encryption*, (2015) at p 3 (accessible at: https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf).

[43] *Id*.

[44] UNSR Report on Anonymity and Encryption above n 30 at para 12.

> 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 society that does not tolerate unconventional opinions or expression."

Encryption and anonymity are especially useful for the development and sharing of opinions online, particularly in circumstances where a person fears that their communications may be subject to interference or attack by state or non-state actors. These are therefore specific technologies through which individuals may exercise their rights. 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 have the potential to frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public safety justifications to support any restrictions or to identify situations where the restriction has been necessary to achieve a legitimate goal.[45] Outright prohibitions on the individual use of encryption technology disproportionately restrict the right to freedom of expression as they deprive all online users in a particular jurisdiction of the right to carve out a space for opinion and expression, without any particular claim of the use of encryption being for unlawful ends.[46] 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.[47]

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.[48]

The 2019 ACHPR Declaration of Principles on Freedom of Expression and Access to Information likewise provides that states should not adopt laws or other measures prohibiting or weakening encryption, including backdoors or key escrows unless such measures are justifiable and compatible with international human rights law and standards.[49]

---

[45] *Id*. at para 36.

[46] *Id.* at para 40.

[47] *Id.* at para 41.

[48] *Id*. at paras 59-60.

[49] Principle 40 (accessible at: https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf).

GOVERNMENT-LED DIGITAL SURVEILLANCE[50]

Communications surveillance encompasses the monitoring, intercepting, collecting, analysing, retention, or similar actions, of a person's communications in the past, present, or future.[51] This relates to both the content of communications and communication *metadata* – which is information *about* a communication, such as the identities of the parties, the time or duration or location of the communication, and technical services used. It has been noted that even communication metadata can give detailed insights into an individual's behaviour, social relationships, private preferences and identity. Taken as a whole, it may allow very precise conclusions to be drawn concerning the private life of the person.

In recent years, the use of sophisticated surveillance technology on mobile phones has gained increasing prominence amidst concerns about its extensive abuse to monitor political opponents and activists. In 2021, news broke that at least 180 journalists had been targeted for surveillance by the Pegasus spyware, a system that can be remotely installed on a smartphone enabling complete control over the device.[52] The news attracted widespread condemnation, including, for example, through an order of the Supreme Court of India in 2021 that ordered an independent inquiry into allegations that the government deployed the Pegasus spyware against various journalists, politicians, and dissidents because of the deeply chilling effects its use could have on freedom of expression.[53]

General Comment No. 16 provides that "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited".[54] Surveillance – both bulk (or mass) collection of data[55] or targeted collection of data – interferes directly with the privacy and security necessary for freedom of opinion and expression, and must be considered against the three-part test to assess the permissibility of the restriction.[56] In the digital age, ICTs have enhanced the capacity of governments, corporations, and individuals to conduct surveillance, interception and data collection, and have meant that the effectiveness of conducting such

---

[50] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

[51] Necessary and proportionate: International principles on the application of human rights to communications surveillance, (2014) (Necessary and Proportionate Principles) at p 4 (accessible at: https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf).

[52] Forbidden Stories, 'Journalists Under Surveillance,' (2021) (accessible at: https://forbiddenstories.org/pegasus-journalists-under-surveillance/).

[53] *Sharma v Union of India and Others*, Writ Petition (CRL.) No. 314 (2021) (accessible at: https://main.sci.gov.in/supremecourt/2021/16884/16884_2021_1_1501_30827_Judgement_27-Oct-2021.pdf).

[54] General Comment No. 16 at para 8.

[55] Revelations be whistle-blowers, such as Edward Snowden, have revealed that the National Security Agency in the USA and the General Communications Headquarters in the United Kingdom had developed technologies allowing access to much global internet traffic, calling records in the United States, individuals' electronic address books and huge volumes of other digital communications content. These technologies are deployed through a transnational network comprising strategic intelligence relationships between governments and other role-players. This is referred to as bulk or mass surveillance. See 2016 Report of the OHCHR at para 4.

[56] 2016 Report of the UNSR on Freedom of Expression at para 20.

surveillance is no longer limited by scale or duration.[57] In Africa, some countries have even passed legislation enabling digital surveillance of targeted groups; for example the United Nations Special Rapporteur on Privacy has noted with concern the Anti-Cybercrime Law enacted in Egypt in 2018 which reportedly enables surveillance of the LGBTQI community.[58]

In a resolution adopted by the UN General Assembly (UNGA) on the right to privacy in the digital age, the UNGA emphasised that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, are highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression, and may contradict the tenets of a democratic society, including when undertaken on a mass scale.[59] It noted further that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory.[60]

In order to meet the condition of legality, many states have taken steps to reform their surveillance laws to allow for the powers required to conduct surveillance activities. According to the Necessary and Proportionate Principles, a civil society initiative to document the principles that apply to any limitation on freedom of expression, communications surveillance should be regarded as a highly intrusive act, and in order to meet the threshold of proportionality, the state should be required at a minimum to establish the following information to a competent judicial authority prior to conducting any communications surveillance:[61]

- 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.

---

[57] Report of the OHCHR at para 2.

[58] Report of the UN Special Rapporteur on Privacy (2019) at p. 14 (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/307/40/PDF/G1930740.pdf?OpenElement).

[59] UNGA, 'Resolution on the right to privacy in the digital age', A/C.3/71/L.39/Rev.1, (2016) (2016 UN Resolution on Privacy) (accessible at: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1).

[60] *Id*.

[61] Above at n 43, Principle 5.

Surveillance constitutes an obvious interference with the right to privacy. Further, it also constitutes an interference with the right to hold opinions without interference and the right to freedom of expression. With particular reference to the right to hold opinions without interference, surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes.[62]

The interference with the right to freedom of expression is particularly apparent in the context of journalists who may be placed under surveillance as a result of their journalistic activities. The disclosure or surveillance of journalistic sources can have negative consequences for the right to freedom of expression due to a breach of an individual's confidentiality in their communications.[63] This is the same for cases concerning the disclosure of anonymous user data. Once confidentiality is undermined, it cannot be restored. It is therefore of utmost importance that measures that undermine confidentiality are not taken arbitrarily.

The importance of source protection has been well-established. For example, in *Bosasa Operation (Pty) Ltd v Basson and Another*, the South Africa High Court held that journalists are not required to reveal their sources, subject to certain exceptions.[64] The court stated in this regard 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."[65]

Surveillance activities carried out against journalists have the risk of fundamentally undermining the source protection to which journalists are otherwise entitled.[66]

---

[62] UNSR Report on Anonymity and Encryption at para 21.

[63] For more, see *Big Brother Watch v United Kingdom* in the ECtHR (2018) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/) and *amaBhungane Centre for Investigative Journalism v Minister of Justice* in South Africa (2019) (accessible at: http://www.saflii.org/za/cases/ZAGPPHC/2019/384.html).

[64] [2012] ZAGPJHC 71, (2012) (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2012/71.html).

[65] *Id*. at para 38.

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

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

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

- In South Africa, the Constitutional Court in 2021 declared various provisions of the domestic surveillance law to be unconstitutional as a result of a complaint brought by an investigative journalist whose communications had been monitored by intelligence officials; the Court ordered a range of amendments to improve transparency, safeguards, and oversight mechanisms state surveillance operations.[67]
- 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, found that the free press's democratic function was at stake, and that "such chilling effect on the freedom of speech is an assault on the vital public watchdog role of the press, which may undermine the ability of the press to provide accurate and reliable information."[68]
- The European Court of Human Rights found some aspects of the United Kingdom's mass surveillance regime to be in violation of the right to privacy and the right to freedom of expression under the European Convention on Human Rights, holding that although bulk interception regimes are not in themselves incompatible with those rights, the lack of independent oversight and the fact that the regime's use was not limited to combatting "serious crime" and did not sufficiently protect journalists' confidential communication resulted in it constituting a violation.[69]
- In a similar thread, in 2022, Media Defence filed a series of complaints at the European Court of Human Rights concerning the Azerbaijan government's apparent use of the Pegasus software to target Azeri journalists.[70]

CONCLUSION

As more of the world moves online, data protection is becoming increasingly necessary. In an African context, some headway has been made: as of 2022, a majority of African states (33) had enacted data protection laws.[71] However, with the growth and increasing sophistication of technologies and practices related to data harvesting and profiling, legislators are some way

- Any court order must only be granted after a fair hearing where sufficient notice has been given to the journalist in question, except in genuine emergencies.

[67] *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* ZACC 3 (2021) (accessible at: http://www.saflii.org/za/cases/ZACC/2021/3.html).
[68] Writ Petition (Crl.) No. 314 of 2021, (2021) (accessible at: https://main.sci.gov.in/supremecourt/2021/16884/16884_2021_1_1501_30827_Judgement_27-Oct-2021.pdf).
[69] Big Brother Watch v. The United Kingdom (Big Brother I) App nos. 58170/13, 62322/14 and 24960/15 (2018) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/).
[70] Media Defence, 'Media Defence files four cases at the ECtHR concerning use of Pegasus spyware by the Azerbaijan government', (2022) (accessible here: https://www.mediadefence.org/news/pegasus-spyware-azerbaijan/)
[71] See https://dataprotection.africa/ for more information.

behind in fully protecting and promoting data privacy and data protection. As we move forward, digital rights activists have a significant role to play in ensuring that states keep step with data protection developments and enact legislative frameworks that fully protect and promote people's rights to privacy.