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/

December 2020

TABLE OF CONTENTS

INTRODUCTION 1
THE RIGHT TO PRIVACY 1
DATA PROTECTION 3
'THE RIGHT TO BE FORGOTTEN' 5
ENCRYPTION AND ANONYMITY ON THE INTERNET 8
GOVERNMENT-LED DIGITAL SURVEILLANCE 9
CONCLUSION 12

MODULE 4

DATA PRIVACY AND DATA PROTECTION

- **The right to privacy is gaining prominence with increasing data flows and the concomitant need for the protection of personal information.**
- **In the African context, there are multiple instruments, including the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention), which govern data protection.**
- **Importantly, states should ensure that their domestic legislation details principles for the lawful processing of personal information and that they keep step with data protection developments.**
- **Allied to data protection are the concepts of the 'right to be forgotten', encryption and government-led surveillance.**
- **Notably, the disclosure of journalistic sources as a result of state surveillance has a negative impact on freedom of expression and journalistic freedom.**

INTRODUCTION

The right to privacy and the concomitant requirement to protect personal information has garnered significant attention with the dawn of the information age. While the internet and online information-sharing and data collection increase at an exponential rate, legislative developments have failed to keep pace and adequately protect personal information. However, with time, African states and regional and continental bodies have begun to adopt data protection-related 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', encryption and surveillance.

THE RIGHT TO PRIVACY

There is an increasing recognition that the right to privacy plays a vital role in and of itself and in facilitating the right to freedom of expression. For instance, reliance on the right to privacy allows individuals to share views anonymously in circumstances where they may fear being censured for those views, it allows whistle-blowers to make protected disclosures, and it enables members of the media 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 not contained in the African Charter on Human and Peoples' Rights (ACHPR), the right to privacy of children is contained in article 10 of the African Charter on the Rights and Welfare of the Child (ACRWC), which 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 right to privacy has also been recognised in other regional and sub-regional instruments in the context of data protection, which is discussed further below. Moreover, almost all African states guarantee this right under their domestic constitutions.[1]

Interestingly, in 2017, the Supreme Court of India declared 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. Although this has not been tested in the context of the ACHPR, there is arguably scope to read the right to privacy into other provisions of the African Charter.

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:[3]

> "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

[1] 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, http://www.pulp.up.ac.za/images/pulp/books/journals/AHRY_2019/Power%202019.pdf.

[2] *Justice K.S. Puttaswamy and Another v Union of India and Others*, Petition No. 494/2012, 24 August 2017 (accessible at: http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf).

[3] *NM and Others v Smith and Others*, [2007] ZACC 6, 4 April 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, 27 March 1996 at para 77.

> 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 that the internet has had 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). This refers to 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, refers to the person or entity responsible for processing the personal information about the data subject.

Data protection is one of the primary measures through which the right to privacy is given effect. There have already been a number of African states that have enacted data protection laws, and more that are in the process of doing so.[4] 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.

In relation to data protection of personal information, General Comment No. 16 on article 17 of the ICCPR (General Comment No. 16) provides as follows:[5]

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

[4] At present, there are 21 states in the African Union (AU) that have enacted comprehensive privacy laws: Angola, Benin, Burkina Faso, Cape Verde, Chad, Côte d'Ivoire, Equatorial Guinea, Egypt, Gabon, Ghana, Kenya, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Togolese Republic and Tunisia. There are a further four states that have shown indications of being close to adopting legislation: Niger, Tanzania, Uganda and Zimbabwe. See https://dataprotection.africa/ for more information.

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

Most comprehensive data protection laws typically 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.
- 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.

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

- **AU Convention on Cyber Security and Personal Data Protection 2014**[7] (AU Convention or "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, it may potentially in future be a binding legal instrument on data protection in Africa.
- **Draft EAC Legal Framework for Cyberlaws 2008**[8] (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 assist with informing 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**[9] (ECOWAS Supplementary Act): This instrument is designed to be directly transposed into a domestic context, and, in a similar vein to the AU Convention, provides in detail

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

[7] Accessible at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. At present, it has been ratified by one state, and signed by a further ten states.

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

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

for the conditions for lawful processing of personal information and the rights of data subjects.

- **SADC Data Protection Model Law 2013**[10] (SADC Model Law): This instrument is a model law that can be utilised in a national context by member states. It seeks to ensure the harmonisations of information and communications technologies (ICT) policies, and recognises that ICT developments impact the rights and protection of personal data, including in government and commercial activities. In addition to setting out the conditions for lawful processing of personal information and the rights of data subjects, it also deals with whistle-blowing, providing that the data protection authority must establish rules giving authorisation for and governing the whistleblowing system which preserve the 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. In this regard, 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 ascertain whether their personal information is being processed in accordance with the applicable data protection laws, and whether their rights are indeed being upheld.

'THE RIGHT TO BE FORGOTTEN'[11]

The so-called 'right to be forgotten' — 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, such as Google, should remove links to private information when asked. 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.

In 2014, the Court of Justice of the European Union (CJEU) handed down an important ruling in the case of *Google Spain v Gonzalez*.[12] Mr Gonzalez, a Spanish national, lodged a complaint in 2010 with the Spanish information regulator. The cause of Mr Gonzalez's complaint was that, when an internet user entered his name into Google's search engine, the user would obtain links to pages of the Spanish newspaper from 1998 referring to attachment proceedings against him for the recovery of certain debts. Mr Gonzalez requested that the personal data relating to him be removed or concealed because the proceedings against him had been fully resolved and the reference to him was therefore now entirely irrelevant.

---

[10] 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.

[11] 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).

[12] *Google Spain SL and Another v Agencia Española de Protección de Datos (AEPD) and Another*, Case No. C-131/12, 13 May 2014 (accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131).

Before the CJEU, relying to the EU data protection law in effect at the time, the claim was upheld. The CJEU noted that the very display of personal information on a search results page constitutes processing of such information,[13] and there was no reason why a search engine should not be subject to the obligations and guarantees laid out under the law.[14] 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 obtain a structured overview of information relating to that individual and establish a profile of the person.[15] 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."[16]

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 legitimate internet users potentially interested in having access to that information.[17] This would require a fair balance to be struck between that interest 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.[18]

The CJEU went on to hold that a data subject is permitted to request that information about him or her no longer be made available to the general public by its inclusion in a list of 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.[19] In such circumstances, the information and links concerned in the list of results must be erased.[20]

The right to be forgotten has also been recognised in domestic contexts. For instance, Italy's Supreme Court of Cassation has held that the public interest in an article diminished after two and a half years, and that sensitive and private information should not be available to the public indefinitely.[21] The case is currently being litigated before the European Court of Human Rights.[22] The Belgian Court of Cassation has also recognised the right to be forgotten.[23]

---

[13] *Id* at para 57.

[14] *Id* at para 58.

[15] *Id* at para 80.

[16] *Id.*

[17] *Id* at para 81.

[18] *Id*.

[19] *Id*. at para 94.

[20] *Id*. at para 94.

[21] *Plaintiff X v PrimaDaNoi*, Case No. 13161, 22 November 2015 (accessible at: https://globalfreedomofexpression.columbia.edu/cases/plaintiff-x-v-primadanoi/).

[22] European Court of Human Rights, Application no. 77419/16 (2020) (accessible at: https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-201483%22%5D%7D).

[23] *P.H. v O.G.*, Case No. 15/0052/F, 29 April 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

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*.[24] 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 companies 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;[25] 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".[26]

According to the Global Principles of Freedom of Expression and Privacy (Global Principles),[27] 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,[28] 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.[29] It states further that de-listing requests should be subject to ultimate adjudication by a court or independent adjudicatory body with relevant expertise in freedom of expression and data protection law.[30]

---

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).

[24] Case No. C-385-15, 9 March 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).

[25] *Ministra Nancy Andrighi v Google Brasil Internet Ltd and Others*, 2011/0307909-6, 26 June 2012 (accessible at: https://www.internetlab.org.br/wp-content/uploads/2017/02/STJ-REsp-1316921.pdf).

[26] The Japan Times, 'Top court rejects 'right to be forgotten' demand', 1 February 2017 (accessible at: https://www.japantimes.co.jp/news/2017/02/01/national/crime-legal/top-court-rejects-right-forgotten-demand/#.WqZQXehubIV).

[27] 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.

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

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

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

ENCRYPTION AND ANONYMITY ON THE INTERNET[31]

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.[32] With a "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.[33] It is also possible to encrypt data at rest that is stored on one's device, such as a laptop or hard drive.[34]

Anonymity can be defined either as acting or communicating without using or presenting one's name or identity, or 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.[35] Anonymity may be distinguished from pseudo-anonymity: the former refers to taking no name at all, whilst the latter refers to taking an assumed name.[36]

Encryption and anonymity are necessary tools for the full enjoyment of digital rights, and enjoy 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:[37]

> "Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's

[31] 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).

[32] 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 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).

[33] *Id*.

[34] *Id*.

[35] Electronic Frontier Foundation, *Anonymity and encryption*, 10 February 2015 at p 3 (accessible at: https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf).

[36] *Id*.

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

> 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 persons may be concerned 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 frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public justification to support the restriction or to identify situations where the restriction has been necessary to achieve a legitimate goal.[38] Outright prohibitions on the individual use of encryption technology disproportionately restricts the right to freedom of expression as it deprives 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.[39] 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.[40]

The UNSR on freedom of expression has called on states to promote strong encryption and anonymity, and noted that decryption orders should only be permissible when it results 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 of individuals.[41]

GOVERNMENT-LED DIGITAL SURVEILLANCE[42]

Communications surveillance encompasses the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future.[43] This relates to both the content of communications and metadata. In respect of the latter, it has been noted that the aggregation of information —

[38] *Id*. at para 36.

[39] *Id.* at para 40.

[40] *Id.* at para 41.

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

[42] 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).

[43] 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).

commonly referred to as 'metadata' — may give an insight 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.

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".[44] Surveillance — both bulk (or mass) collection of data[45] 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.[46] 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 in conducting such surveillance is no longer limited by scale or duration.[47]

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.[48] 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.[49]

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 the surveillance activities. According to the Necessity and Proportionate Principles, 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:[50]

- 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.

---

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

[45] 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.

[46] 2016 Report of the UNSR on Freedom of Expression at para 20.

[47] Report of the OHCHR at para 2.

[48] UNGA, 'Resolution on the right to privacy in the digital age', A/C.3/71/L.39/Rev.1, 16 November 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).

[49] *Id*.

[50] Above at n 43, Principle 5.

- 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.

Surveillance constitutes an obvious interference with the right to privacy. Further, it also constitutes an interference 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, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes.[51]

The interference with the right to freedom of expression is particularly apparent in the context of journalists and members of the media who may be placed under surveillance as a result of their journalistic activities. As noted by the Secretary-General of the UN, this can have a chilling effect on the enjoyment of media freedom, and renders it more difficult to communicate with sources and share and develop ideas, which may lead to self-censorship.[52] The use of encryption and other similar tools have become essential to the work of journalists to ensure that they are able to conduct their work without interference.

The disclosure of journalistic sources and surveillance can have negative consequences for the right to freedom of expression due to a breach of an individual's confidentiality in their communications.[53] 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

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

[52] Report of the Secretary-General on the UN to the UNGA, 'Report on the safety of journalists and the issue of impunity', A/70/290, 6 August 2015 (2015 Report of the UN Secretary-General) at paras 14-16 (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/247/06/PDF/N1524706.pdf?OpenElement).

[53] 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).

are not required to reveal their sources, subject to certain exceptions.[54] 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."[55]

Surveillance activities carried out against journalists have the risk of fundamentally undermining the source protection to which journalists are otherwise entitled.[56]

CONCLUSION

As more of the world moves online, data protection is becoming increasingly necessary. In an African context, some headway has been made with 21 African states having privacy laws in place. However, with the rapid growth in data harvesting, legislators are some way behind in fully protecting and promoting data privacy and data protection. As we move forward, digital rights activists have a significant role to play in ensuring that states keep step with data protection developments and enact legislative frameworks that fully protect and promote peoples' rights to privacy.

---

[54] [2012] ZAGPJHC 71, 26 April 2012 (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2012/71.html).

[55] *Id*. at para 38.

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

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