Training Manual on Digital Rights and Freedom of Expression Online

Litigating digital rights and online freedom of expression in East, West and Southern Africa

MLDI
Media Legal Defence Initiative

mediadefence.org

Published by Media Legal Defence Initiative
www.mediadefence.org

This work is licenced under the Creative Commons Attribution-NonCommercial 4.0 International License. This means that you are free to share and adapt this work so long as you give appropriate credit, provide a link to the license, and indicate if changes were made. Any such sharing or adaptation must be for non-commercial purposes, and must be made available under the same "share alike" terms. Full licence terms can be found at http://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.

CONTENTS

LIST OF ACRONYMS

ACDEG	African Charter on Democracy, Elections and Governance
ACHPR	African Commission on Human and Peoples' Rights
ACRWC	African Charter on the Rights and Welfare of the Child
AU	African Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CRC	United Nations Convention on the Rights of the Child
CRPD	United Nations Convention on the Rights of Persons with Disabilities
EAC	East African Community
ECOWAS	Economic Community of West African States
ECtHR	European Court of Human Rights
EU	European Union
GDPR	General Data Protection Regulation 2016/679 of the European Parliament and of the Council
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICTs	Information communication technologies
MLDI	Media Legal Defence Initiative
OAS	Organization of American States
OHCHR	United Nations Office of the High Commissioner for Human Rights
OSCE	Organization for Security and Co-operation in Europe
SADC	Southern African Development Community
SDGs	Sustainable Development Goals
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNGA	United Nations General Assembly
UNHRC	United Nations Human Rights Council
UNHRCtte	United Nations Human Rights Committee
UNSR	United Nations Special Rapporteur
URL	Uniform Resource Locator

CHAPTER 1: SETTING THE CONTEXT

The importance of the right to freedom of expression is well-established under domestic and international law. It is recognised as a fundamental right in and of itself, as well as being key to facilitating an array of other fundamental rights. Importantly, through the freedom to receive and impart information and ideas, the right to freedom of expression can play a crucial role in achieving openness, transparency and accountability. It further enables individuals to achieve self-fulfilment and to meaningfully participate in decision-making and political affairs.

The internet is one of the most powerful tools in facilitating the receiving and imparting of information and ideas. It allows for instant sharing of volumes of information, across borders and to wide audiences. It enables individuals to engage with diverse views and perspectives, and to access an array of resources to assist them to formulate their own views.

As described in a report published by the United Nations Educational, Scientific and Cultural Organization (**UNESCO**):[1]

> "Probably the single most important factor in understanding the impact of the internet on freedom of expression is the way in which it increases our ability to receive, seek and impart information. It enables the collaborative creation and sharing of content – it is a world where anyone can be an author and anyone can publish. The internet is helping develop spaces that can empower people, helping them communicate, collaborate and exchange views and information. This represents, in a real sense, the 'democratisation' of freedom of expression as it is no longer necessary to rely upon professional journalists or gatekeepers to act as public spokespeople for our views."

While the internet and other technologies offer enormous opportunities, they also present particular challenges. The digital rights landscape is constantly evolving as new technologies develop, and as we increasingly test the ambit of the right to freedom of expression and other rights online. This training manual highlights some of the key developments that have taken place or are currently being explored, both at an international and a national level. We hope that the manual will provide useful guidance for training purposes and in litigation, and can be a useful resource to anyone interested in media freedom, particularly in Africa.

I. What are digital rights?

It is now firmly entrenched by both the African Commission on Human and Peoples' Rights[2] (**ACHPR**) and the United Nations[3] (**UN**) that the same rights that people have offline must also be protected online, in particular the right to freedom of expression. As stipulated in

[1] A. Puddephatt, 'Freedom of expression and the internet', UNESCO, 2016 at p 19 (accessible at: http://unesdoc.unesco.org/images/0024/002466/246670e.pdf).

[2] ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', ACHPR/Res.362(LIX), 4 November 2016 (accessible at http://www.achpr.org/sessions/59th/resolutions/362/).

[3] UN Human Rights Council, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/32/L.20, 27 June 2016 at para 1 (accessible at: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf).

Article 19(2) of the International Covenant on Civil and Political Rights, the right to freedom of expression applies regardless of frontiers and through any media of one's choice.

In sum, digital rights are basically human rights in the digital era.[4] The advent of the internet and information technology has occasioned a change in the way we enjoy and exercise our fundamental rights, such as freedom of expression, access to information, assembly, education and political choice. The term 'digital rights' therefore comprises the rights that are implicated in our access to and use of these technologies. It also necessitates the consideration of what commensurate obligations there are on states and other actors to protect these rights.

However, the application of the long-established principles of freedom of expression to the online content is not always immediately apparent. A particular challenge that arises is in relation to the changing roles of journalists and publishers. These are challenges being grappled with by a number of courts and policy-makers around the world. That said, while some of the issues are indeed new, there are many that can be readily dealt with by applying a reasonable approach to the established principles of law.

It should be remembered that every state has an obligation to respect, protect and fulfil the right of all actors, including that of journalists and internet intermediaries, in accordance with the state's obligations under international human rights law. This obligation extends to ensuring that these role-players are able to fulfil their functions without fearing for their security.

II. Who constitutes a journalist?

Journalists are often the main protagonists in free speech cases. This is because media freedom is a core component of the right to freedom of expression, and members of the media often investigate and criticise state action as part of the exercise of their functions. As discussed in more detail below, the particular role that the media plays in achieving an open and democratic society, and the special protections that this deservedly engages have frequently been emphasised by the courts.[5] As such, with a growing body of civilian journalists, bloggers and other similar commentators, there is a need to consider who precisely constitutes a journalist entitled to this protection.

As expressed by the former United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom
of Opinion and Expression (**UNSR on Freedom of Expression**), Mr Frank la Rue, in his 2010 report to the UN General Assembly:[6]

> "Journalists are understood to be individuals who are dedicated to investigating, analysing and disseminating information, in a regular and specialized manner,

[4] World Economic Forum, 'What are your digital rights?', 13 November 2015 (accessible at: https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/).

[5] These can include can include the protection of their sources, the heightened leeway afforded to their freedom of expression, and the protections against penalisation for carrying out legitimate activities.

[6] Report of the UNSR on Freedom of Expression to the UN General Assembly (UNGA), 11 June 2010, A/65/284, 11 August 2010 at para 21 (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/482/85/PDF/N1048285.pdf?OpenElement).

> through any type of written media, broadcast media (television or radio) or electronic media. With the advent of new forms of communication, journalism has extended into new areas, including citizen journalism".

The report went on to note that while there is no universal definition of the term 'citizen journalist', it is usually understood as independent reporting, often by amateurs on the scene of an event, which is disseminated globally through modern media, such as the internet, through social media, blogs, and so on.[7] As stated, "[n]ew technologies have provided unprecedented access to means of global communication, and have therefore introduced new means of reporting on news and events around the world".[8] The report notes further that, although citizen journalists are not trained professional journalists, this is nevertheless an important form of journalism as it can contribute to a richer diversity of views and opinions, and can provide an immediate, insider's view of a conflict or catastrophe.[9]

This position is consistent with the United Nations Human Rights Committee's (**UNHRCtte**) General Comment No. 34 on Article 19 of the ICCPR (**General Comment No. 34**), published in 2011, which expressly provides that journalism is a function shared by a wide range of actors, from professional full-time reporters and analysts to bloggers and others who engage in forms of self-publication in print and on the internet.[10]

While the question of precisely who enjoys journalistic protections, and to what extent, will need to be decided on a case-by-case basis. The general point of departure should be to construe this broadly to apply to both professional and citizen journalists who are disseminating information in the public interest.

III. What is an internet intermediary?

An internet intermediary may be defined as an entity which provides services that enable people to use the internet, falling into two categories: (i) conduits, which are technical providers of internet access or transmission services; and (ii) hosts, which are providers of content services, such as online platforms (eg. websites), caching providers and storage services.[11] In sum, internet intermediaries are the pipes through which internet content is transmitted and the storage spaces in which it is stored, and are therefore essential to the functioning of the internet.[12] Examples of internet intermediaries include network operators,

---

[7] *Id.* at para 62.

[8] *Id.* at para 62.

[9] *Id.* at para 63.

[10] General Comment No. 34 at para 44.

[11] Association for Progressive Communications, 'Frequently asked questions on internet intermediary liability', May 2014 (accessible at: https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-internet-intermed). Examples of internet intermediaries are as follows:

- Network operators: MTN, Safaricom.
- Network infrastructure providers: Cisco, Huawei, Ericsson, Dark Fibre Africa.
- Internet access providers: Comcast, MWeb, AccessKenya.
- Internet service providers: Liquid Telecommunications South Africa, iBurst, Vox Telecom.
- Social networks: Facebook, Twitter, LinkedIn.

[12] Alex Comninos, 'The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain', Association for Progressive Communications, October 2012 at p 4 (accessible at:

network infrastructure providers, internet access providers, internet service providers (**ISPs**), hosting providers, social networks, and search engines.[13]

Internet intermediaries can function both independently and interdependently, depending on the services being offered. This can be illustrated as follows:[14]

> "[D]ifferent types of intermediaries perform different functions. They also have different technical architectures. For example, [ISPs] connect a user's device, whether it is a laptop, a mobile phone or something else, to the network of networks known as the internet. Once a user is connected to the internet, web hosting providers and domain registrars and registries, in turn, make it possible for websites to be published and to be accessed online. Search engines make a portion of the World Wide Web accessible by allowing individuals to search their database. Search engines are often an essential go-between between websites and internet users. Social networks connect individual internet users by allowing them to exchange text, photos, videos, as well as by allowing them to post content to their network of contacts, or to the public at large."

IV. The borderless enjoyment of freedom of expression

The particular opportunity that freedom of expression online presents is that the right is able to be enjoyed regardless of physical borders. People are able to speak, share ideas, coordinate and mobilise across the globe on a significant scale. This can lead, for instance, to international pressure being put on states for rights violations, global campaigns being developed and supported, and a rigorous marketplace of ideas being fostered.

However, the internet also gives rise to particular challenges that need to be addressed. Through the internet, the ability to publish immediately and reach an expansive audience can create difficulties from a legal perspective. For example, the borderless nature of the internet can make establishing the true identity of an online speaker more challenging, founding jurisdiction for a claim more complex, or achieving accountability for wrongdoing that has been perpetrated online more difficult.

Moreover, the adage of "closing the stable door after the horse has bolted" often rings true when dealing with online publication, as there are instances where injured parties may find themselves on the backfoot with little meaningful recourse available to contain the impact of the publication once it has been posted online. While steps are being taken in an effort to find solutions to address these challenges, it is essential that these solutions strike the appropriate balance between the competing rights and interests, and do not erode the enjoyment of digital rights and freedom of expression online.

---

https://www.apc.org/sites/default/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL_0.pdf).

[13] *Id.* at p 5.

[14] Rebecca MacKinnon et al, 'Fostering freedom online: The role of internet intermediaries', UNESCO, 2013 at p 22 (accessible at: http://unesdoc.unesco.org/images/0023/002311/231162e.pdf).

CHAPTER 2: FREEDOM OF EXPRESSION ONLINE

I. Key principles of international law

Human rights are inherent to all persons. They are enshrined in both national and international law, and all persons are entitled to enjoy such rights without distinction. When fully realised, human rights reflect the minimum standards to enable persons to live with dignity, freedom, equality, justice and peace.

The cornerstones of human rights are that they are inalienable and therefore cannot be taken away; interconnected and therefore dependant on one another; and indivisible, meaning that they cannot be treated in isolation. Not all rights are absolute, and some rights may be subject to certain limitations and restrictions in order to balance competing rights and interests.

Human rights under international law are generally considered to be rooted in the Universal Declaration of Human Rights (**UDHR**), which was agreed to at the United Nations in 1948 following the end of World War II. The UDHR is not a binding treaty in itself, but countries can be bound by those UDHR principles that have acquired the status of customary international law. The UDHR has further been the catalyst to creating other binding legal instruments, most notably the ICCPR and the International Covenant on Economic, Social and Cultural Rights (**ICESCR**).

- The ICCPR enshrines civil and political rights, sometimes referred to as first-generation rights, and includes the rights to life, liberty, freedom of expression, access to information, privacy, and assembly.

- The ICESCR enshrines economic, social and cultural rights, sometimes referred to as second-generation rights, and includes the rights to health, education, work, and to participate in cultural life. In recognition of the limited resources of many states, it is generally accepted that these rights are to be progressively realised over time.

Treaties are an important binding source of international law on those states that have ratified them. However, treaties are not the only sources of international law. Article 38 of the Statute of the International Court of Justice identifies the following sources: (i) international conventions; (ii) international custom, as evidence of a general practice accepted as law; (iii) general principles of law recognised by nations; and (iv) judicial decisions and teachings of the most highly qualified publicists, as subsidiary means for the determination of the rules of law. For the ACHPR, articles 60 and 61 of the African Charter on Human and Peoples' Rights (**African Charter**) set out the binding and subsidiary sources of law, respectively, for the ACHPR to consider.[15]

[15] Articles 60 and 61 of the African Charter state as follows:

> "**Article 60**
>
> The Commission shall draw inspiration from international law on human and peoples' rights, particularly from the provisions of various African instruments on human and peoples' rights, the Charter of the United Nations, the Charter of the Organization of African Unity, the Universal Declaration of Human Rights, other instruments adopted by the United Nations and by African countries in the field of human and peoples' rights as well as from the provisions of various instruments adopted within the Specialized Agencies of the United Nations of which the parties to the present Charter are members."

States are the primary duty-bearers for the realisation of human rights, which encompasses both negative and positive duties. With negative duties, states must avoid violating the rights of individuals and communities within their territories and protect them against violations by others. On the other hand, the obligation to fulfil human rights requires states to take positive steps to enable the full enjoyment of these rights. By ratifying treaties, states commit to put in place domestic measures, such as legislation, to give effect to their treaty obligations.

II. The right to freedom of expression under international law

The rights contained under Article 19 of the ICCPR comprise three core tenets:

- The right to hold opinions without interference (freedom of opinion);
- The right to seek and receive information (access to information);
- The right to impart information (freedom of expression).

The right is contained in a number of legal instruments that have been developed by the United Nations and by regional human rights mechanisms, such as the ACHPR. Certain instruments provide a holistic guarantee of the right, whilst others focus on particular aspects thereof. The right to freedom of expression is not absolute and may be limited in accordance with prescribed conditions.

A. United Nations

The first recordal of the right to freedom of expression under international law can be found in Article 19 of the UDHR,[16] which was later encapsulated in Article 19 of the ICCPR as follows:

> "(1) Everyone shall have the right to hold opinions without interference.
> (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

General Comment No. 34 notes that the right to freedom of expression includes, for example, political discourse, commentary on one's own affairs and on public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching, and religious discourse.[17] It also embraces expression that may be regarded by some as deeply

---

"**Article 61**

The Commission shall also take into consideration, as subsidiary measures to determine the principles of law, other general or special international conventions, laying down rules expressly recognized by member states of the Organization of African Unity, African practices consistent with international norms on human and people's rights, customs generally accepted as law, general principles of law recognized by African states as well as legal precedents and doctrine."

[16] Article 19 of the UDHR provides as follows:

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

[17] General Comment No. 34 at para 11.

offensive.[18] The right covers communications that are both verbal and non-verbal, and all modes of expression, including audio-visual, electronic and internet-based modes of communication.[19]

In terms of article 19(3) of the ICCPR, the right to freedom of expression contained in article 19(2) may be subject to certain restrictions:

> "The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
> (a) For respect of the rights or reputations of others;
> (b) For the protection of national security or of public order (*ordre public*), or of public health or morals."

Notably, the limitations clause contained in article 19(3) only applies to the right to freedom of expression contained in article 19(2). It does not apply to the right to hold opinions without interference in terms of article 19(1). As such, it is apparent from the framework of article 19(1) that the right to hold opinions without interference may not be restricted or limited in any manner.

With respect to a limitation on the right to freedom of expression under article 19(2), a three-part test is used to assess whether such a limitation is justified: (i) the limitation must be provided for in law; (ii) it must pursue a legitimate aim; and (iii) it must be necessary for a legitimate purpose.[20] This test applies similarly to limitations of the right to freedom of expression under other legal instruments, including the African Charter.

Restrictions on the right to freedom of expression may not put the right itself in jeopardy.[21] This is in accordance with article 5(1) of the ICCPR, which provides that "nothing in the present Covenant may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms recognized herein or at their limitation to a greater extent than is provided for in the present Covenant".

The proportionality analysis contained in the third step of the three-part test is worth highlighting. This requires that the restriction must be the least restrictive measure and proportionate to the aim pursued. In the 2002 decision of *Attorney-General v 'Mopa,*[22] the Lesotho Court of Appeal (per Gauntlett JA) stated that:

---

[18] General Comment No. 34 at para 11. For further discussion on this, see Nani Jansen Reventlow, 'The right to 'offend, shock or disturb', or the importance of protecting unpleasant speech' in *Perspectives on harmful speech online: A collection of essays*, Berkman Klein Center for Internet & Society, 2016 at pp 7-9 (accessible at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746096).

[19] General Comment No. 34 at para 12.

[20] For a fuller discussion on how freedom of expression may be legitimately limited, see the training manual published by MLDI on the principles of freedom of expression under international law: Richard Carver, 'Training manual on international and comparative media and freedom of expression law', MLDI at pp 14-16 (accessible at: https://www.mediadefence.org/sites/default/files/resources/files/MLDI.FoEManual.Version1.1.pdf).

[21] General Comment No. 34 at para 21.

[22] [2003] 1 LRC 224 at para 33, quoting with approval the decision of the Canadian Supreme Court in *R v Oakes [1987] LRC (Const) 477 at 499-500* (accessible at: http://www.chr.up.ac.za/index.php/browse-by-subject/341-lesotho-attorney-general-v-mopa-2002-ahrlr-91-leca-2002.html).

> "There are, in my view, three important components of a proportionality test. First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective. Secondly, the means, even if rationally connected to the objective in this first sense, should impair as little as possible' the right or freedom in question … Thirdly there must be a proportionality between the effects of the measures which are responsible for limiting the Charter right or freedom, and the objective which has been identified as of sufficient importance."

The principles relating to proportionality have been distilled in General Comment No. 34 to include the following:

- Restrictive measures must be appropriate to achieve their protective function;[23]
- They must be proportionate to the interest to be protected;[24]
- The principle of proportionality must be respected both in law and by the authorities applying the law;[25]
- The principle of proportionality must take into account the form of expression and the means of dissemination, for instance if it pertains to a public debate concerning figures in the public and political domain.[26]

In *Zimbabwe Lawyers for Human Rights & Associated Newspapers of Zimbabwe v Zimbabwe*, the ACHPR identified the following guiding questions that must be asked when determining whether a measure is proportionate under Article 19(2) of the ICCPR and Article 9 of the African Charter:[27] Were there sufficient reasons to justify the action? Was there a less restrictive alternative? Was the decision-making process procedurally fair? Were there any safeguards against abuse? Does the action destroy the essence of the rights guaranteed by the treaty provision?[28]

In addition to Article 19(3) of the ICCPR, which provides for restrictions on the right to freedom of expression, Article 20 of the ICCPR goes further to identify those categories of speech that must be prohibited by law. Article 20 states as follows:

> "(1) Any propaganda for war shall be prohibited by law.
> (2) Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."

General Comment No. 34 states that Articles 19 and 20 of the ICCPR are compatible and complementary.[29] The key distinction between the two provisions is that Article 20 provides a specific response to the identified speech: the requirement that it be prohibited by law. Given

[23] General Comment No. 34 at para 34.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Zimbabwe Lawyers for Human Rights & Associated Newspapers of Zimbabwe v. Zimbabwe*, Communication No. 284/03, 3 April 2009 (accessible at: http://www.achpr.org/communications/decision/284.03/).

[28] *Id.* at para 176.

[29] General Comment No. 34 at para 50.

the drastic nature of this measure, careful consideration should be given to the implementation of Article 20, in particular whether the speech in question is indeed that which is contemplated by the provision.[30] Article 20, specifically in the context of hate speech, is dealt with in more detail below.

The ICCPR is not the only treaty within the United Nations framework to address the right to freedom of expression. For instance:

- Article 15(3) of the ICESCR specifically refers to the freedom required for scientific research and creative activity, providing that:

  > "The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity."

- Articles 12 and 13 of the UN Convention on the Rights of the Child (**CRC**) contain extensive protections relating to the right to freedom of expression enjoyed by children, providing that:

  > "**Article 12**
  > (1) States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.
  > (2) For this purpose, the child shall in particular be provided the opportunity to be heard in any judicial and administrative proceedings affecting the child, either directly, or through a representative or an appropriate body, in a manner consistent with the procedural rules of national law."

  > "**Article 13**
  > (1) The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.
  > (2) The exercise of this right may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; or (b) For the protection of national security or of public order (ordre public), or of public health or morals."

- Article 21 of the United Nations Convention on the Rights of Persons with Disabilities (**CRPD**) contains extensive protections relating to freedom of expression and access to information of persons with disabilities, providing as follows:

  > "States Parties shall take all appropriate measures to ensure that persons with disabilities can exercise the right to freedom of expression and opinion, including the freedom to seek, receive and impart information and ideas on an

[30] The interplay between articles 19 and 20 of the ICCPR is considered further in the discussion on hate speech in Chapter 5 below.

> equal basis with others and through all forms of communication of their choice, as defined in article 2 of the present Convention, including by:
> (a) Providing information intended for the general public to persons with disabilities in accessible formats and technologies appropriate to different kinds of disabilities in a timely manner and without additional cost;
> (b) Accepting and facilitating the use of sign languages, Braille, augmentative and alternative communication, and all other accessible means, modes and formats of communication of their choice by persons with disabilities in official interactions;
> (c) Urging private entities that provide services to the general public, including through the Internet, to provide information and services in accessible and usable formats for persons with disabilities;
> (d) Encouraging the mass media, including providers of information through the Internet, to make their services accessible to persons with disabilities;
> (e) Recognizing and promoting the use of sign languages."

It is therefore clear that the right to freedom of expression is firmly entrenched within the United Nations system, both as an important right on its own, as well as a crucial enabling right. For example, as stated in the UNHRCtte General Comment No. 25 (**General Comment No. 25**), in the context of the right to participate in public affairs, voting rights and the right of equal access to public service, it was noted that: "Citizens can also take part in the conduct of public affairs by exerting influence through public debate and dialogue with their representatives or through their capacity to organize themselves. This participation is supported by ensuring freedom of expression, assembly and association".[31]

B. African regional instruments

Similarly, the right to freedom of expression is also well entrenched in the African regional system, and contained in a number of regional treaties and soft law instruments. As a starting point, Article 9 of the African Charter is key in this regard and provides for the right to freedom of expression as follows:

> "(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."

The reference to "within the law" should not be seen as permitting states to enact laws that violate the right to freedom of expression. The ACHPR has made clear that this position is not acceptable. In its decision in *Constitutional Rights Project / Nigeria*,[32] specifically in relation to Article 9 of the African Charter and reference to its earlier decision in *Civil Liberties*

[31] General Comment No. 25 at para 8.

[32] *Constitutional Rights Project / Nigeria*, Communication No. 102/93, 31 October 1998 at paras 57-58 (accessible at: http://www.achpr.org/files/sessions/24th/comunications/102.93/achpr24_102_93_eng.pdf).

Organisation (in respect of the Nigerian Bar Association) / Nigeria,[33] the ACHPR stated as follows:

> "The government justifies its actions with regard to the journalists and proscription of publications by reference to the 'chaotic' situation that transpired after the elections were annulled. The Commission decided, in its decision on communication 101/93, with respect to freedom of association, that 'competent authorities should not enact provisions which limit the exercise of this freedom. The competent authorities should not override constitutional provisions or undermine fundamental rights guaranteed by the constitution and international human rights standards.'
>
> With these words the Commission states a general principle that applies to all rights, not only freedom of association. Government[s] should avoid restricting rights, and take special care with regard to those rights protected by constitutional or international human rights law. No situation justifies the wholesale violation of human rights. In fact, general restrictions on rights diminish public confidence in the rule of law and are often counter-productive."

It is therefore clear that national law must be consistent with the state's obligations under the African Charter and cannot be relied upon to justify non-compliance. As stated by the Zimbabwean Constitutional Court in *Chimakure v. Attorney-General of Zimbabwe*, the principle of legality requires that states specify "clearly and concretely in the law the actual limitations to the exercise of freedom of expression" in order to enable the public to know in advance what is permissible and what the consequences are of disobedience.[34]

In addition to the internal limitation contained in Article 9(2), Article 27 of the African Charter also contains a general limitations clause:

> "(1) Every individual shall have duties towards his family and society, the State and other legally recognised communities and the international community.
> (2) The rights and freedoms of each individual shall be exercised with due regard to the rights of others, collective security, morality and common interest."

Limitations on the right to freedom of expression under the African Charter – as with limitations under the ICCPR – are required to comply with the three-part test (as discussed above) before they can be deemed justifiable under the African Charter.

The guarantee of the right to freedom of expression is underscored in the Declaration of Principles on Freedom of Expression in Africa,[35] adopted by resolution of the ACHPR in October 2002. In its preamble, it notes "the fundamental importance of freedom of expression as an individual human right, as a cornerstone of democracy and as a means of ensuring

---

[33] *Civil Liberties Organisation (in respect of the Nigerian Bar Association) / Nigeria*, Communication No. 101/93, 22 March 1995 (accessible at: http://www.achpr.org/files/sessions/17th/comunications/101.93/achpr17_101_93_eng.pdf).

[34] *Chimakure v Attorney-General of Zimbabwe*, Application No. CCZ 247/09, Judgment No. CCZ 6/2014, 22 July 2014 at paras 24 and 26 (accessible at: https://globalfreedomofexpression.columbia.edu/cases/chimakure-ors-v-the-attorney-general/).

[35] ACHPR, 'Resolution on the adoption of the 'Declaration of Principles on Freedom of Expression in Africa", ACHPR/Res.62(XXXII)02, 2002 (accessible at: http://www.achpr.org/sessions/32nd/resolutions/62/).

respect for all human rights and freedoms" and "the important contribution that can be made to the realisation of the right to freedom of expression by new information and communication technologies". Principle I(2) reaffirms that: "Everyone shall have an equal opportunity to exercise the right to freedom of expression and access to information without discrimination". Moreover, Principle XVI calls on state parties to the African Charter to make every effort to give practical effect to the principles contained in the Declaration of Principles on Freedom of Expression in Africa.

The ACHPR Guidelines on Freedom of Association and Assembly in Africa[36] also give useful guidance on the right to freedom of expression. In particular, it notes that the right to freedom of association protects, amongst other things, expression and criticism of state conduct.[37] It further calls on states to fully respect, both in law and in practice, the right to freedom of expression through assembly, and provides that "[t]he expression aimed at, in and through assemblies is protected by the right to freedom of expression, and includes expression that may give offence or be provocative".[38]

Other treaties within the African regional system that address the right to freedom of expression include the following:

- The African Charter on the Rights and Welfare of the Child (**ACRWC**) specifically provides for the right to freedom of expression for every child capable of communication, as well as for freedom of thought and conscience. In this regard, it provides as follows:

  > "**Article 7: Freedom of expression**
  > Every child who is capable of communicating his or her own views shall be assured the rights to express his opinions freely in all matters and to disseminate his opinions subject to such restrictions as are prescribed by laws."
  >
  > "**Article 9: Freedom of thought, conscience and religion**
  > (1) Every child shall have the right to freedom of thought conscience and religion.
  > (2) Parents, and where applicable, legal guardians shall have the duty to provide guidance and direction in the exercise of these rights having regard to the evolving capacities, and best interests of the child.
  > (3) State Parties shall respect the duty of parents and where applicable, legal guardians, to provide guidance and direction in the enjoyment of these rights subject to the national laws and policies."

- Article 27(8) of the African Charter on Democracy, Elections and Governance (**ACDEG**) provides that, in order to advance political, economic and social governance, state parties must commit themselves to, among other things,

[36] ACHPR, Guidelines on Freedom of Association and Assembly in Africa (accessible at http://www.achpr.org/files/instruments/freedom-association-assembly/guidelines_on_freedom_of_association_and_assembly_in_africa_eng.pdf).

[37] *Id.* at para 28.

[38] *Id.* at paras 77-78. Para 78 goes on to state that "[h]ate speech and the incitement of violence are not protected and shall be prohibited".

"[p]romoting freedom of expression, in particular freedom of the press and fostering a professional media".

There are a further number of sub-regional instruments that engage the right to freedom of expression:

- Article 6 of the Treaty Establishing the East African Community (**EAC**) includes among its fundamental principles the principle of good governance, and goes on to state that this includes the principles of democracy, rule of law, accountability, transparency, and the rights contained in the African Charter.[39]

- Article 66 of the Revised Treaty of the Economic Community of West African States (**ECOWAS**) provides that members agree (i) to maintain within their borders, and between one another, freedom of access for professionals of the communication industry and for information sources; (ii) to facilitate exchange of information between their press organs; to promote and foster effective dissemination of information within the Economic Community of West African states; (iii) to ensure respect for the rights of journalists; (iv) to take measures to encourage investment capital, both public and private, in the communication industries in member states.[40]

- In terms of the Protocol on Culture, Information and Sport of the Southern African Development Community (**SADC**), Article 19(1) provides that state parties will cooperate on improving the free flow of information within the region; and Article 20 provides that state parties will take the necessary measures to ensure the development of media that are editorially independent and conscious of their obligations to the public and greater society.

It is thus apparent that the right to freedom of expression is an indispensable part of the regional and international human rights framework. Nonetheless, how does the right to freedom of expression apply online?

III. The right to freedom of expression online

Article 19(2) of the ICCPR was drafted in a technologically-neutral manner. In other words, through its statement that the right to freedom of expression applies "regardless of frontiers", it makes clear that the medium through which the speech is communicated does not affect the ambit of the protection that the right conveys. General Comment No. 34 further explains that Article 19(2) includes internet-based modes of communication.[41] General Comment No. 34 goes further to call on states to take all necessary steps to foster the independence of new forms

[39] See, for instance, *Burundi Journalists' Union v The Attorney General of the Republic of Burundi*, Reference No. 7 of 2013 (2015) (accessible at: http://eacj.org/?cases=burundi-journalists-union-vs-the-attorney-general-of-the-republic-of-burundi).

[40] See, for instance, *Hydara Jr v the Gambia* ECW/CCJ/APP/30/11 (2014) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/hydara-v-gambia/); *Federation of African Journalists and Others v the Gambia* Application No. ECW/CCJ/APP/36/15 (2018) (accessible at: https://www.mediadefence.org/sites/default/files/blog/files/FAJ%20and%20Others%20v%20The%20Gambia%20Judgment.pdf).

[41] General Comment No. 34 at para 12.

of media that have arisen through information and communication technologies (**ICTs**),[42] and to take into account both the differences and points of convergence in print and broadcast media on the one hand, and the internet on the other.[43]

In a 2016 resolution, the UNHRC affirmed that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights".[44] The UNHRC further recognised the global and open nature of the internet as a driving force in accelerating progress in various forms, including in achieving the Sustainable Development Goals (**SDGs**).[45]

This has similarly been recognised by the ACHPR. In a 2016 resolution, the ACHPR recalled that the UNHRC's affirmation that the same rights that people have offline must also be protected online, and called on states to promote and facilitate access to the internet and international cooperation aimed at the development of media and information and communications facilities in all countries.[46] The ACPHR further called on states to respect and to take legislative and other measures to guarantee, respect and protect citizens' rights to freedom of information and expression through access to internet services.[47] The ACHPR also included a call to African citizens to exercise their right to freedom of expression on the internet responsibly.

Historically, different forms of media were regulated differently. For instance, print media was typically self-regulated, whilst broadcast media often had more involvement from the state. The significance of this distinction, however, has diminished considerably over time.[48] There is ever-increasing convergence between the traditional and digital media sectors, including in respect of infrastructure that is increasingly becoming interdependent. The recognition by the UNHRC and by the ACHPR that the right to freedom of expression must be equally protected both offline and online is therefore appropriate, and pays due regard to the convergence of different mediums and platforms through which the right to freedom of expression is exercised.

---

[42] General Comment No. 34 at para 15.

[43] General Comment No. 34 at para 39.

[44] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/32/L.20, 27 June 2016 (2016 UN Resolution on the Internet) at para 1 (accessible at: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf).

[45] *Id.* at para 2.

[46] ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', ACHPR/Res.362(LIX), 4 November 2016 (2016 ACHPR Resolution on the Internet) (accessible at http://www.achpr.org/sessions/59th/resolutions/362/).

[47] *Id.* at para 1.

[48] For further discussion, see for instance Eve Salmon, 'Independent regulation of broadcasting: A review of international policies and experiences', UNESCO (2016) (accessible at: http://unesdoc.unesco.org/images/0024/002460/246055E.pdf); Lara Fielden, 'Press regulation: Taking account of media convergence', Foundation for Law, Justice and Society, University of Oxford (2012) (accessible at: http://www.fljs.org/sites/www.fljs.org/files/publications/Fielden.pdf).

CHAPTER 3: ACCESS TO THE INTERNET

I. Is there a right to the internet under international law?

An express right to the internet has not, as yet, been recognised in any international treaty or similar instrument. This has been the source of much debate, and the arguments for and against whether the internet should be considered a human right have been summarised as follows:[49]

Arguments in favour of access to the internet as a human right	Arguments against access to the internet as a human right
• *Necessity*. There is a certain consensus on not only the usefulness of the internet but its crucial role as an "indispensable tool" for human rights and development in the current century. • *Implied existence under current international human rights law*. The full exercise of freedom of expression, participation in cultural life and enjoyment of scientific benefits requires access to the internet. Current standards of living include participation in the broader community in different ways, e.g. through the connection to the internet. • *Inevitability*. A number of countries including Greece, Estonia, Finland, Spain, Costa Rica and France have asserted or recognised some right of access in their constitutions, legal codes, or judicial rulings. These are most easily accessed online. • *Inseparability*. Technological progress changes how people enjoy their rights and governments should address the link between those rights and their current methods of enjoyment. • *Progression*. The notion of rights themselves has the ability to change, as social contexts change. The growing importance of the internet in changing social contexts makes it necessary to ensure access to it. • *Public support*. Worldwide surveys show a single predominant attitude	• *No international treaty directly creates a right of access to the internet*. In simple terms, it is not a human right if the international community has not recognised it as such in a binding instrument, and there is no discussion of a new treaty to do so in any forum. • *Analogy to other forms of media*. There is no right to the telephone, the television, the printed press (either for publishing or receiving it) or any other similar medium that has imposed a duty on states to provide it to its citizens and cover its costs. • *Universality*. Access to the internet is not an economic right that can be construed from Article 11 of the ICESCR or Article 25 of the UDHR, for they are representative of standards of living that cannot be considered on the same scale for countries in much different stages of development. • *Nature as a right*. Even if there is a legal recognition of access, it is established not as much as an individual right but as an obligation for states, in an economic key, to provide populations with opportunities for development. • *Means to an end*. Access to the internet consists of technology, which is a tool, not a right itself. • *Access to the internet is not absolutely necessary for participation in a political community*. A big part of the world's population is without internet access, but there is little outcry if states

[49] Juan Carlos Lara, 'Internet access and economic, social and cultural rights', Association for Progressive Communications, September 2015 at pp 10-11 (accessible at: https://www.apc.org/sites/default/files/APC_ESCR_Access_Juan%20Carlos%20Lara_September2015%20%281%29_0.pdf).

towards access to the internet: that it should be recognised as a right.	are unable to provide access. It is only when such participation already exists and is taken away that it deserves attention. • *Inflation*. Claiming that an interest is a basic, fundamental or human right, without considering the conditions under which it can really be realised, inflates the number of rights, diminishing the forcefulness of core traditional human rights. • *Flexibility of existing human rights*. It is not necessary to "create" new rights aside from those already recognised, but to ensure their exercise and enjoyment in changing technological contexts. • *Side effects*. Digital inclusion policies carry concerns regarding the true beneficiary. On one hand, access policies will benefit those users with devices with the ability to access the internet, therefore exacerbating inequalities. On the other hand, lack of control by governments would lead to the need for investment in private telecommunications companies, therefore granting them economic benefit before citizens.

Regardless of which side of the debate one falls, the current position is that there is no express right to the internet under international law. Nevertheless, there is an increasing recognition of access to the internet being indispensable to the enjoyment of an array of fundamental rights. The corollary is that those without access to the internet are deprived of the full enjoyment of those rights, which, in many instances, can exacerbate already existing socio-economic divisions. For instance, a lack of access to the internet can impede an individual's ability to obtain key information, facilitate trade, search for jobs, or consume goods and services.

Access entails two distinct but interrelated dimensions: (i) access to and dissemination of content online; and (ii) access to the physical infrastructure to enable access to and dissemination of such online content. In 2003, UNESCO was among the first international bodies to call on states to take steps to realise a right of access to the internet. In this regard, it stated that:[50]

> "Member States and international organizations should promote access to the Internet as a service of public interest through the adoption of appropriate policies in order to

[50] UNESCO, 'Recommendation concerning the promotion and use of multilingualism and universal access to cyberspace' at paras 7 and 15 (accessible at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Eng%20-%20Recommendation%20concerning%20the%20Promotion%20and%20Use%20of%20Multilingualism%20and%20Universal%20Access%20to%20Cyberspace.pdf).

> enhance the process of empowering citizenship and civil society, and by encouraging proper implementation of, and support to, such policies in developing countries, with due consideration of the needs of rural communities.
>
> ...
>
> Member States should recognize and enact the right of universal online access to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or economic situation."

In 2012, the UNHRC passed an important resolution that "[called] upon all States to facilitate access to the Internet and international cooperation aimed at the development of media and information communications facilities in all countries".[51]

This has been expanded upon in the SDGs, which recognise that "[t]he spread of information and communications technology and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies".[52] The SDGs further call on states to enhance the use of ICTs and other enabling technologies to promote the empowerment of women,[53] and to strive to provide universal and affordable access to the internet in least developed countries by 2020.[54]

The 2016 UN Resolution on the Internet recognises that the internet can accelerate progress towards development, including in achieving the SDGs, and affirms the importance of applying a rights-based approach in providing and expanding access to the internet.[55] Notably, it affirms the importance of applying a comprehensive rights-based approach in providing and in expanding access to the internet,[56] and calls on states to consider formulating and adopting national internet-related public policies with the objective of universal access and the enjoyment of human rights at their core.[57]

Two categories of persons are recognised in the 2016 UN Resolution on the Internet as being deserving of special attention:

---

[51] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/20/L.13, 29 June 2012 at para 2 (accessible at: ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc). This was expanded upon further the following year in UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/Res/26/13, 14 July 2014 (accessible at: http://hrlibrary.umn.edu/hrcouncil_res26-13.pdf).

[52] UNGA, 'Transforming our world: The 2030 agenda for sustainable development', A/Res/70/1, 21 October 2015 at para 15 (accessible at http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E).

[53] *Id.* at goal 5(b) at p 18.

[54] *Id.* at goal 9(c) at p21.

[55] 2016 UN Resolution on the Internet at para 2.

[56] *Id.* at para 5.

[57] *Id.* at para 12.

- The first category relates to women and girls. The resolution echoes the call contained in the SDGs for states to bridge the gender digital divide and enhance the use of enabling technologies, in particular ICTs, to promote the empowerment of all women and girls.[58]

- The second category relates to persons with disabilities. In this regard, the resolution calls on states to take appropriate measures to promote the design, development production and distribution of ICTs and systems that are accessible to persons with disabilities.[59]

The UN Commission on Science and Technology for Development has also expanded upon some of the economic, social and political benefits that can accrue from providing citizens with access to the internet.[60] This includes creating possibilities for economic development by the creation of online services, businesses and applications which concurrently create jobs; enhancing education as the internet provides a platform for exchanging information and learning from others; benefiting healthcare by giving people, especially in rural areas, fast and direct access to consult about basic health questions; contributing to cultural and social development; and enhancing political engagement.

Notwithstanding whether the internet is seen as a self-standing right or an enabling tool to facilitate the realisation of other rights, the groundwork has firmly been laid for the need to realise universal access to the internet. States are concomitantly required to take steps to achieve universal access. However, in reality, universal access to the internet is far from being realised. This is due to a confluence of factors, including a lack of financial resources to be able to access the internet, inadequate locally-relevant content, insufficient levels of digital literacy, and a lack of political will to make this a priority.

In the Joint Declaration on Freedom of Expression and the Internet, the freedom of expression mandate-holders stipulate that, as states are under a positive obligation to promote universal access to the internet, they should at a minimum put in place the following measures to fulfil this obligation:[61]

- Regulatory mechanisms – which could include pricing regimes, universal service requirements and licensing agreements – that foster greater access to the internet, including for the poor and in rural areas.[62]

---

[58] *Id.* at para 6.

[59] *Id.* at para 7.

[60] UN Commission on Science and Technology for Development, 'Internet broadband for an inclusive digital society', UN Doc. E/CN.16/2013 (2013).

[61] International Mechanisms for Promoting Freedom of Expression, 'Joint declaration on freedom of expression and the internet', 1 June 2011 (**2011 Joint Declaration**) (accessible at: https://www.osce.org/fom/78309?download=true). The 2011 Joint Declaration is signed by the UNSR on Freedom of Expression, the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, the Organization for Security and Co-operation in Europe (**OSCE**) Representative on Freedom of the Media, and the Organization of American States (**OAS**) Special Rapporteur on Freedom of Expression.

[62] *Id.* at para 6(e)(i).

- Direct support to facilitate access, including by establishing community-based ICT centres and other public access points.[63]

- Promotion of adequate awareness about both how to use the internet and the benefits it can bring, especially among the poor, children and the elderly, and isolated rural populations.[64]

- Special measures to ensure equitable access to the internet for the disabled and for disadvantaged persons.[65]

In order to implement this, the mandate-holders stipulate that states should adopt detailed multi-year action plans for increasing access to the internet, which should include clear and specific targets, standards of transparency, and public reporting and monitoring systems.[66]

In *Kalda v. Estonia*, the European Court of Human Rights (**ECtHR**) held that the right of the applicant – a prisoner – to freedom of expression had been violated through the refusal to grant him access to the internet in order to visit websites containing legal information, as this had breached his right to receive information.[67] The ECtHR noted that if a state is willing to allow prisoners access to the internet, as with the case in question, it had to give sufficient reasons for refusing access to specific sites.[68]

II. Interferences with access to the internet

Some of the ways in which access to the internet is interfered with is through internet shutdowns, the disruption of online networks and social media sites, and the blocking and filtering of content. Such interferences can pose severe restrictions on the enjoyment of the right to freedom of expression, as well as the enjoyment of a range of other rights and services (including mobile banking, online trade, and the ability to access government services via the internet).

The act of disrupting or blocking access to internet services and websites amounts to a form of prior restraint as it restricts internet users from expressing themselves through these services and websites before the expression actually occurs. Due to the profound chilling effect prior restraints can have on the exercise of the right to freedom of expression, the ICCPR has been interpreted as providing for an absolute prohibition on such measures.[69]

---

[63] *Id.* at para 6(e)(ii).

[64] *Id.* at para 6(e)(iii).

[65] *Id.* at para 6(e)(iv).

[66] 2011 Joint Declaration at para 6(f).

[67] Application No. 17429, 19 January 2016 (accessible at: http://hudoc.echr.coe.int/eng?i=001-160270).

[68] *Id.* at para 53. In the subsequent decision of *Jankovskis v Lithuania*, Application No. 21575/08, 17 January 2017 (accessible at: http://hudoc.echr.coe.int/eng?i=001-170354), also in relation to a prisoner who had been refused access to a website containing education-related information, the ECtHR again upheld the applicant's claim of a violation of the right to freedom of expression.

[69] This has been inferred from the *travaux préparatoires* of the ICCPR that prior restraints are absolutely prohibited under Article 19 of the ICCPR. See Marc J. Bossuyt, 'Guide to the "Travaux Preparatoires" of the International Covenant on Civil and Political Rights', Martinus Nijhoff (1987) at p 398.

A. What is an internet shutdown?

An internet shutdown may be defined as an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.[70] In other words, this arises when someone, be it the government or a private sector actor, intentionally disrupts the internet, a telecommunications network or a n internet service, arguably to control or curb what people say or do.[71] This is sometimes also referred to as a 'kill switch'.

In some instances, this may entail there being a total network outage, whereby access to the internet is shutdown in its entirety. In other circumstances, this may also arise when access to mobile communications, websites or social media and messaging applications is blocked, throttled or rendered effectively unusable.[72] Shutdowns may affect towns or regions within a country, an entire country, or even multiple countries, and have been seen to range from several hours to several months.[73]

It should be noted that governments typically conduct shutdowns with the assistance of private actors that operate networks or facilitate network traffic.[74] As noted by the UNSR on Freedom of Expression, large-scale attacks on network infrastructure committed by private parties, such as distributed denial-of-service (known as 'DDoS') attacks, may also have the same effect as an internet shutdown.

B. What is the blocking and filtering of content?

Although a less drastic measure than a complete internet shutdown, the blocking and filtering of content online can also hinder the full enjoyment of the right to freedom of expression. Blocking/filtering has been defined as follows:

> "[T]he difference between "filtering" and "blocking" is a matter of scale and perspective.
> - Filtering is commonly associated with the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords, or on the basis of their perceived connection to content deemed inappropriate or unlawful;
> - Blocking, by contrast, usually refers to preventing access to specific websites, domains, IP addresses, protocols or services included on a blacklist."[75]

[70] Access Now, 'What is an internet shutdown?' (accessible at: https://www.accessnow.org/keepiton/?ignorelocale).

[71] *Id.*

[72] Report of the UNSR on Freedom of Expression to the UNGA, A/HRC/35/22, 30 March 2017 (2017 Report of the UNSR on Freedom of Expression) at para 8 (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement).

[73] *Id.*

[74] *Id.*

[75] ARTICLE 19, 'Freedom of expression unfiltered: How blocking and filtering affect free speech, October 2016 (**ARTICLE19 Report on Blocking and Filtering**) at p 7 (accessible at: https://www.article19.oort rg/data/files/medialibrary/38588/Blocking_and_filtering_final.pdf).

C. What is network neutrality?

Network neutrality refers to the principle that all internet data should be treated equally without undue interference, and promotes the widest possible access to information on the internet.[76] In other words, ISPs should treat all data that travels over their networks fairly, without improper discrimination in favour of a particular application, website or service.[77] Discrimination of information can involve the halting, slowing or otherwise tampering of the transfer of data for a purpose other than a legitimate network management purpose (such as easing congestion or blocking spam).[78]

As noted by the UNSR on Freedom of Expression, in the digital age the freedom to choose among information sources is meaningful only when internet content and applications of all kinds are transmitted without undue discrimination or interference by non-state actors, including providers.[79] In this regard, the state's positive duty to promote freedom of expression strongly favours network neutrality in order to promote the widest possible non-discriminatory access to information.[80]

The 2017 Report of the UNSR on Freedom of Expression describes two key ways in which net neutrality may be affected:[81]

- Paid prioritisation schemes, in terms of which providers give preferential treatment to certain types of internet traffic over others for payment or other commercial benefit.

- Zero rating, which is the practice of not charging for the use of internet data associated with a particular application or service; other services or applications, meanwhile, are subject to metered cost.

In various countries around Africa, there has been significant debate about access to zero-rated content, as particularly social networking sites offer some measure of free access to users. On the one hand, the argument in favour is that zero-rating provides access to persons who might not otherwise have been able to access the internet, and can serve as a gateway to users to understand the opportunities that the internet can offer. On the other hand, the argument against is that zero-rating can lead to unfair competition, and can distort users' perceptions by only allowing access to particular sites.[82]

---

[76] 2017 Report of the UNSR on Freedom of Expression at para 23.

[77] Electronic Frontier Foundation, 'Net neutrality' (accessible at: https://www.eff.org/issues/net-neutrality).

[78] American Civil Liberties Union, 'What is net neutrality?' (accessible at: https://www.aclu.org/issues/free-speech/internet-speech/what-net-neutrality).

[79] 2017 Report of the UNSR on Freedom of Expression at para 23.

[80] *Id.*

[81] *Id.* at paras 24-28.

[82] For a discussion on zero-rating in Africa, see Research ICT Africa, 'Much ado about nothing? Zero-rating in the African context', 12 September 2016 (accessible at: https://www.researchictafrica.net/publications/Other_publications/2016_RIA_Zero-Rating_Policy_Paper_-_Much_ado_about_nothing.pdf).

D. Limitation of the right to freedom of expression

In 2016, the UNSR on Freedom of Expression noted that "[t]he blocking of Internet platforms and the shutting down of telecommunications infrastructure are persistent threats, for even if they are premised on national security or public order, they tend to block the communications of often millions of individuals".[83] This poses an obvious limitation on the right to freedom of expression, and may further limit a range of other rights.

The 2011 Joint Declaration on Freedom of Expression and the Internet highlights the egregious nature that these limitations can cause:[84]

> "(a) Mandatory blocking of entire websites, [internet protocol (**IP**)] addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.
> (b) Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression.
> (c) Products designed to facilitate end-user filtering should be required to be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering."

Internet and telecommunications shutdowns that involve measures to intentionally prevent or disrupt access to or dissemination of information online is a violation of human rights law.[85] In the 2016 UN Resolution on the Internet, the UNHRC stated that it "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and calls upon all States to refrain from and cease such measures".[86]

As set out in General Comment No. 34:[87]

> "Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with [Article 19(3) of the ICCPR]. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with [Article 19(3) of the ICCPR]. It is also inconsistent with [Article 19(3) of the ICCPR] to prohibit a site or an information dissemination system from publishing material solely on the basis that it

[83] Report of the UNSR on Freedom of Expression to the UNGA, A/71/373, 6 September 2016 (2016 Report of the UNSR on Freedom of Expression) at para 22 (accessible at: http://www.un.org/ga/search/view_doc.asp?symbol=A/71/373).

[84] International Mechanisms for Promoting Freedom of Expression, 'Joint declaration on freedom of expression and the internet', 1 June 2011 (2011 Joint Declaration)

[85] 2017 Report of the UNSR on Freedom of Expression at para 8.

[86] 2016 UN Resolution on the Internet at para 10.

[87] General Comment No. 34 at para 43.

> may be critical of the government or the political social system espoused by the government."

In applying the three-part test to ascertain the permissibility of the limitation to the right to freedom of expression that is caused by an internet shutdown, the UNSR on Freedom of Expression has noted that internet shutdowns are often ordered covertly and without a legal basis, and violate the requirement that the restrictions must be provided for in law.[88] Similarly, shutdowns ordered pursuant to vaguely formulated laws and regulations, or in terms of laws and regulations that are adopted and implemented in secret, also fail to satisfy the legality requirement.[89] In some countries, this has led to the government enacting new laws to expressly allow for shutdowns to take place.[90]

The UNSR on Freedom of Expression has further noted that network shutdowns invariably fail to meet the standard of necessity,[91] and are generally disproportionate.[92] States frequently seek to justify this on the ground of national security, which is discussed further below.

In relation to the blocking and filtering of content, there may indeed be circumstances where such measures are justifiable, for example in relation to websites distributing child pornography. Such measures still constitute a limitation of rights, and are therefore required to meet the three-part test for a justifiable limitation. This will need to be assessed on a case-by-case basis, with regard being had to the fact that such measures can often be ineffective at achieving a targeted outcome, and lack transparency with little to no judicial oversight exercised. In this regard, the following measures have been proposed when dealing with the blocking and filtering of content:[93]

- Blanket filtering must be prohibited by law, and should be user-controlled and transparent.

- Any requirement to block unlawful content must be provided for in law.

- Blocking should only be ordered by an independent and impartial court or adjudicatory body, and such blocking orders must be strictly proportionate to the aim pursued.

---

[88] 2017 Report of the UNSR on Freedom of Expression at para 9.

[89] *Id.* at para 10.

[90] In India, for example, following the internet reportedly having been shut down more than 40 times during the course of 2017, the Department of Telecommunications issued new rules - the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules - in August 2017 allowing the government to shut down telephone and internet services during a public emergency or for public safety. The government had previously relied on section 144 of the Criminal Code that was aimed at preventing "obstruction, annoyance or injury" to impose internet restrictions. This legal development has been met with mixed responses. On the one hand, the new rules would potentially mean that, if the government were to persist with internet shutdowns, this could arguably be done in a more organised manner. On the other hand, however, concerns have been raised about the lack of definitions for the terms "public emergency" or "public safety", and the potential that these new rules may have to facilitate censorship online. See: for instance, http://www.hindustantimes.com/india-news/govt-issues-first-ever-rules-to-carry-out-internet-shutdowns-in-india/story-Drn0MnxJAp58RoZoFI7u4L.html.

[91] 2017 Report of the UNSR on Freedom of Expression at para 14.

[92] *Id.* at para 15.

[93] ARTICLE19 Report on Blocking and Filtering, *ibid.* at pp 19-23.

Similarly, limitations to network neutrality may also be permissible in certain circumstances, for example for legitimate network management purposes. However, as a general principle, there should be no discrimination in the treatment of internet data and traffic, regardless of the device, content, author, origin and/or destination of the content, service or application.[94] Further, internet intermediaries should be required to be transparent about any traffic or information management practices they employ, and relevant information on such practices should be made available in a form that is accessible to all stakeholders.[95]

E. National security as "legitimate aim"

National security is frequently relied upon as reason for justifying an interference with access to the internet, as well as other interferences with the right to freedom of expression.[96] While this may, in appropriate circumstances, be a legitimate aim, it also has the potential to be relied upon to quell dissent and cover up state abuses. The covert nature of many national security laws, policies and practices, as well as the refusal by states to disclose complete information about the national security threat, tends to exacerbate this concern. Furthermore, courts and other institutions have often been deferent to the state in determining what constitutes national security. As has been previously noted:[97]

> "The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability."

Principle XIII(2) of the Declaration of Principles on Freedom of Expression in Africa provides that the right to freedom of expression should not be restricted on public order or national security grounds "unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression".

As set out under Principle 2 of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (**the Johannesburg Principles**):[98]

> "(a) A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the

---

[94] 2011 Joint Declaration at para 5(a).

[95] *Id.* at para 5(b).

[96] For a fuller discussion on national security more broadly, see Richard Carver, *ibid.* at pp 77-88.

[97] Report of the UNSR on Freedom of Expression to the UNGA, A/HRC/23/40, 17 April 2013 at para 60 (accessible at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf).

[98] Principle 2 of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, November 1996 (accessible at https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf). The Johannesburg Principles were developed by a group of experts in international law, national security and human rights, convened by ARTICLE 19. It was endorsed by the then UNSR on Freedom of Expression.

> use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.
> (b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest."

Principle 7 goes further to state that the peaceful exercise of the right to freedom of expression shall not be considered a threat to national security or subjected to any restrictions or penalties.

Another important principle contained in the Johannesburg Principles is Principle 23, which provides that: "Expression shall not be subject to prior censorship in the interest of protecting national security, except in time of public emergency which threatens the life of the country". As a general proposition, prior restraint of expression is impermissible. The measures described above can often give rise to a prior restraint on content, and consequently have a chilling effect on the enjoyment of the right to freedom of expression.

In a recent judgment delivered by the Islamabad High Court in Pakistan,[99] the court ruled that the Federal Government and the Pakistan Telecommunication Authority had impermissibly suspended or caused the suspension of mobile cellular services or operations in Pakistan. The petitioners had argued that the Telecommunication Authority compelled licensees to suspend telecommunications services from time to time, on the basis of mere apprehensions of national security risks. According to the court, the only instance permitted under domestic law whereby mobile services or operations could be suspended was if the President proclaimed a state of emergency. In the present circumstances, in the absence of any such proclamations – and notwithstanding the concerns that the state may have in relation to national security – any actions, orders or directives issued by the Federal Government or the Telecommunication Authority was declared to be illegal, *ultra vires,* and without lawful authority and jurisdiction. The court noted further that causing the suspension of services or operations outside of instances permitted under the law may expose the Federal Government and the Telecommunication Authority to claims of compensation or damages by the licensees or the users of mobile services.

Similarly, counter-terrorism as a purported justification for network shutdowns or other interferences with access to the internet should also be treated with caution. As noted in General Comment No. 34, the media plays an important role in informing the public about acts of terrorism, and it should be able to perform its legitimate functions and duties without hindrance.[100] While governments may argue that internet shutdowns are necessary to ban the spread of news about terrorist attacks to prevent panic or copycat attacks, it has instead been

[99] *CM Pak Limited v Pakistan Telecommunication Authority*, FAO No. 42 of 2016, 26 February 2016 (accessible at http://www.livelaw.in/pak-court-holds-suspension-mobile-services-federal-govt-ground-national-security-illegal-read-judgment/).

[100] General Comment No. 34 at para 46.

found that maintaining connectivity may mitigate public safety concerns and help restore public order.[101]

At a minimum, if there is to be a limitation of access to the internet, there should be transparency regarding the laws, policies and practices relied upon, clear definitions of terms such as 'national security' and 'terrorism', and independent and impartial oversight being exercised.

III. Intermediary liability

Intermediary liability occurs where technological intermediaries, such as ISPs and websites, are held liable for unlawful or harmful content created by users of those services.[102] This can occur in various circumstances, including copyright infringements, digital piracy, trademark disputes, network management, spamming and phishing, "cybercrime", defamation, hate speech, child pornography, "illegal content", offensive but legal content, censorship, broadcasting and telecommunications laws and regulations, and privacy protection.[103]

A report published by UNESCO identifies the following challenges facing intermediaries:[104]

- Limiting the liability of intermediaries for content published or transmitted by third parties is essential to the flourishing of internet services that facilitate expression.

- Laws, policies, and regulations requiring intermediaries to carry out content restriction, blocking, and filtering in many jurisdictions are not sufficiently compatible with international human rights standards for freedom of expression.

- Laws, policies, and practices related to government surveillance and data collection from intermediaries, when insufficiently compatible with human rights norms, impede intermediaries' ability to adequately protect users' privacy.

- Whereas due process generally requires that legal enforcement and decision-making are transparent and publicly accessible, governments are frequently opaque about requests to companies for content restriction, the handover of user data, and other surveillance requirements.

The right to freedom of expression online can only be sufficiently protected if intermediaries are adequately insulated from liability for content generated by others. Such insulation can be achieved in a number of ways, such as through a system of absolute immunity from liability, or a regime that only fixes intermediaries with liability following their refusal to obey an order from a court or other competent body to remove the impugned content.

[101] 2017 Report of the UNSR on Freedom of Expression at para 14.

[102] Alex Comninos, *ibid.* at p 6.

[103] *Id.*

[104] Rebecca MacKinnon et al, *ibid.* at pp 179-180.

Certain countries have legislated limitations to intermediary liability.[105] However, where intermediaries face the possibility of civil or criminal liability for content on their networks, they are more incentivised to control or police this content.[106] In such cases, intermediaries may err on the side of removing content without properly analysing whether the content is indeed unlawful. This impacts the right to freedom of expression, and may result in access to online content being denied in circumstances where this should not be the case. As explained by the UNSR on Freedom of Expression, "such intermediary liability creates a strong incentive to censor: providers may find it safest not to challenge such regulation but to over-regulate content such that legitimate and lawful expression also ends up restricted. The pressure to assist in State censorship and surveillance also escalates when authorities harass, threaten or arrest employees, or attempt to tamper with the company's networks or equipment".[107]

Practically, the consequent effect of intermediary liability is that it gives intermediaries quasi-judicial authority to decide about the legality of content, in circumstances where they are ill-equipped to do so and are not required to follow due process procedures, make their decisions transparent or offer independent appeals mechanisms.[108]

As stated in the 2011 Joint Declaration on intermediary liability:[109]

> "(a) No one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so ('mere conduit principle').
> (b) Consideration should be given to insulating fully other intermediaries, including those mentioned in the preamble, from liability for content generated by others under the same conditions as in paragraph 2(a). At a minimum, intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the 'notice and takedown' rules currently being applied)."

The ECtHR has considered intermediary liability in several cases:

- In 2013, in the case of *Delfi AS v Estonia*, the ECtHR considered the liability of an internet news portal for offensive comments that were posted by readers below one of its online news articles.[110] The portal complained that being held liable for the comments of its readers breached its right to freedom of expression. The ECtHR dismissed the case, holding that the finding of liability by the domestic courts was a justified and proportionate

[105] *Id.* See, for example, the South African Electronic Communications and Transactions Act 25 of 2002 and the Ugandan Electronic Transactions Act 8 of 2011.

[106] *Id.* at p 9.

[107] 2017 Report of the UNSR on Freedom of Expression at para 49.

[108] ARTICLE 19, 'Freedom of expression and ICTs: Overview of international standards', 2013 (**ARTICLE19 Report on ICTs**) at p 19 (accessible at: https://www.article19.org/data/files/medialibrary/37380/FoE-and-ICTs.pdf).

[109] 2011 Joint Declaration at para 2. See, also, 'Manila principles on intermediary Liability (accessible at: https://www.manilaprinciples.org/principles).

[110] Application No. 64569/09, 10 October 2013 (accessible at: http://hudoc.echr.coe.int/eng?i=001-155105).

restriction of freedom of expression because the comments were highly offensive (i.e. hate speech) and clearly unlawful; the portal failed to remove them a reasonable time after publication; there were impediments to bringing proceedings against the original authors of the comments; and the fine imposed by the Estonian courts was not excessive.

- In 2016, in the case of *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*, the ECtHR considered the liability of a self-regulatory body of internet content providers and an internet news portal for vulgar and offensive online comments posted on their websites.[111] The ECtHR reiterated that, although they were not the authors of the comments, the website operates still had to assume duties and responsibilities. In the present case, the ECtHR distinguished the facts from those in *Delfi* and found that by imposing liability on the two website operators the Hungarian courts' had violated the right to freedom of expression under Article 10 of the European Convention on Human Rights. The ECtHR noted that a notice-and-take-down procedure will usually be adequate to ensure a balance is struck between the right to freedom of expression and the right to reputation in cases concerning intermediaries.

- In 2017, in the case of *Tamiz v United Kingdom*, the ECtHR had another opportunity to consider the ambit of intermediary liability.[112] The applicant, a former politician in the United Kingdom, had claimed before the domestic courts that a number of third-party comments posted by anonymous users on Google's Blogger.com platform were defamatory. Before the ECtHR, the applicant argued that his right to respect for his private life had been violated because the domestic courts had refused to grant him a remedy against the intermediary. His claim was ultimately dismissed by the ECtHR on the basis that the resulting damage to his reputation would have been trivial. The ECtHR highlighted the important role that ISPs perform in facilitating access to information and debate on a wide range of political, social and cultural rights, and seemed to endorse the line of argument that ISPs should not be obliged to monitor content or proactively investigate potential defamatory activity on their sites.

---

[111] Application No 22947/13, 2 February 2016 (accessible at: http://hudoc.echr.coe.int/eng?i=001-160314).

[112] *Tamiz v United Kingdom*, Application No. 3877/14, 19 September 2017 (accessible at: http://hudoc.echr.coe.int/eng?i=001-178106). MLDI, together with a coalition of organisations, made submissions to the ECtHR on proposed principles for intermediary based on best practices in national legislation, the views of the Committee of Ministers of the Council of Europe (CoE) and special mandate holders.

In the above case before the, MLDI together with a coalition of other organisations. The proposed principles are as follows:

- Intermediaries should not be the arbiters of the lawfulness of content posted, stored or transferred by the users of their services.
- Assuming that they have not contributed to or manipulated content, intermediaries should not be liable for content posted, stored or transferred using their services unless and until they have failed to comply with an order of a court or other competent body to remove or block specific content.
- Notwithstanding the above, intermediaries should in no circumstances be liable for content unless it has been brought to their attention in such a way that the intermediary can be deemed to have actual knowledge of the illegality of that content.
- A requirement to monitor content on an ongoing basis is incompatible with the right to freedom of expression contained in article 10 of the European Convention on Human Rights.

The submissions are accessible here: https://www.mediadefence.org/sites/default/files/blog/files/20160407%20Tamiz%20v%20UK%20Intervention%20Filing.pdf.

Other courts have taken more definitive positions in respect of intermediary liability. For example, the Supreme Court of India has interpreted the domestic law to only provide for intermediary liability where an intermediary has received actual knowledge from a court order, or where an intermediary has been notified by the government that one of the unlawful acts prescribed under the law are going to be committed, and the intermediary has subsequently failed to remove or disable access to such information.[113] Furthermore, the Supreme Court of Argentina has held that search engines are under no duty to monitor the legality of third-party content to which they link, noting that only in exceptional cases involving "gross and manifest harm" could intermediaries be required to disable access.[114]

In light of the vital role played by intermediaries in promoting and protecting the right to freedom of expression online, it is imperative that they are safeguarded against unwarranted interference - by state and private actors - that could have a deleterious effect on the right. For example, as an individual's ability to exercise their right to freedom of expression online is dependent on the passive nature of online intermediaries, any legal regime that causes an intermediary to apply undue restraint or censorship toward content communicated through their services will ultimately have an adverse effect on the right to freedom of expression online. The UNSR has noted that intermediaries can serve as an important bulwark against government and private overreach, as they are usually, for instance, best-placed to push back on a government's proposed measure.[115] However, this can only truly be realised in circumstances where intermediaries are able to do so without fear of sanction or penalties.

[113] *Shreya Singhal v Union of India*, Application No. 167/2012 at paras 112-118 (accessible at: http://www.livelaw.in/summary-of-the-judgment-in-shreya-singhal-vs-union-of-india-read-the-judgment/).

[114] *María Belén Rodriguez v Google*, Fallo R.522.XLIX (accessible at: http://www.csjn.gov.ar/docus/documentos/verdoc.jsp). The decision has been described in the 2016 Report of the UNSR on Freedom of Expression at para 52.

[115] 2017 Report of the UNSR on Freedom of Expression at para 50.

CHAPTER 4: DIGITAL PRIVACY AND DATA PROTECTION

I. The right to privacy

The right to privacy is sometimes seen to be the flipside of the right to freedom of expression: whilst freedom of expression is typically about facilitating access to and disseminating information, privacy is often about choosing what information one does not want to be shared. However, there is an increasing recognition that the right to privacy also plays a role in facilitating 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 right to privacy is contained in article 17 of the ICCPR, which provides as follows:

> "(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."

The ACHPR does not expressly recognise a right to privacy. Notably, 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, 1949.[116] 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.

Although not contained in the African Charter, the right to privacy of children is contained in article 10 of the 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, a number of African states guarantee right to privacy under their domestic constitutions.

[116] *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).

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:[117]

> "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 that the internet has had on the enjoyment of this right.

II. 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 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.[118] 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, the UNHRCtte's General Comment No. 16 on Article 17 of the ICCPR (**General Comment No. 16**) provides as follows:[119]

> "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

[117] *NM and Others v Smith and Others*, [2007] ZACC 6, 4 April 2007 at para 33 (accessible at: http://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.

[118] At present, there are 18 states in the African Union (**AU**) that have enacted comprehensive privacy laws: Angola, Benin, Burkina Faso, Cape Verde, Chad, Côte d'Ivoire, Equatorial Guinea, Gabon, Ghana, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa and Tunisia. There are a further five states that have shown indications of being close to adopting legislation: Kenya, Niger, Tanzania, Uganda and Zimbabwe.

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

> 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."

Most comprehensive data protection laws typically make provision for the following principles:[120]

- 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.

In relation to the last-mentioned principle, this is one of the key drivers in data protection legislation being enacted, in order to facilitate cross-border transfers of personal information for trade and other purposes. The Court of Justice of the European Union (**CJEU**) has taken a firm stance on this, and in 2015 declared the data-sharing arrangement between the European Union (**EU**) and the United States of America (**USA**) to be invalid on the basis that the USA failed to meet the adequacy threshold for data protection as contemplated under EU

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

law. In *Maximillian Schrems v Data Protection Commissioner*,[121] 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 USA, 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 in the EU Directive.

The CJEU upheld the claim, noting that the protective rules laid out in the data sharing arrangement between the 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 was of the view that legislation that does not provide for an individual to pursue legal remedies to access one's personal information, or to have such information rectified or erased, compromises the essence of the right to effective judicial protection.

Accordingly, the CJEU declared the Safe Harbour Agreement 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".[122]

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

- AU Convention on Cyber Security and Personal Data Protection 2014[123] (**AU 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[124] (**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.

[121] Case No. C-362/14, 6 October 2015 (accessible at: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN).

[122] *Id.* at paras 73-74 and 96.

[123] 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.

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

- Supplementary Act on Personal Data Protection within ECOWAS 2010[125] (**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 for the conditions for lawful processing of personal information and the rights of data subjects.

- SADC Data Protection Model Law 2013[126] (**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 ICT policies, and recognises that ICT technology developments impacts 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.

III. 'The right to be forgotten'

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 CJEU handed down an important ruling in the case of *Google Spain v Gonzalez*.[127] 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.

---

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

[126] 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.

[127] *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: http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre=).

Before the CJEU, relying on 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,[128] and there was no reason why a search engine should not be subject to the obligations and guarantees laid out under the law.[129] 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.[130] 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."[131]

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.[132] 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.[133]

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.[134] In such circumstances, the information and links concerned in the list of results must be erased.[135] In sum, the CJEU held that:

> "A the data subject may, in the light of his fundamental rights … request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held … that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question".[136]

---

[128] *Id.* at para 57.
[129] *Id.* at para 58.
[130] *Id.* at para 80.
[131] *Id.*
[132] *Id.* at para 81.
[133] *Id.*
[134] *Id.* at para 94.
[135] *Id.* at para 94.
[136] *Id.* at para 97. As per the CJEU's order at para 100(4):

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.[137] In this case, PrimaDaNoi.it – an online news publication – reported a story regarding a fight that had taken place outside a restaurant that involved the restaurant owner. The court held that providing direct and easy access to the old article, and its continued spread on the internet was unlawful as of the date that PrimaDaNoit.it had been requested to delete the publication, and that the continued publication and spread on the internet of the news item could not be classed as lawful processing or collecting of journalistic data for historical or editorial purposes. Although the court accepted the importance of the right to report, it held that sensitive and private information should not be available to the public indefinitely (unless the publisher receives consent to do so from the concerned person).

The Belgian Court of Cassation has also recognised the right to be forgotten.[138] The case was initiated by a Belgian national against a newspaper for not complying with a request to remove from its online archives an article dating back to 1994 regarding a car accident in which he was involved that caused the deaths of two people. The Court of Cassation held that the publication of articles in a newspaper's online archives could be considered a new disclosure of facts of a person's judicial past, which could potentially infringe the individual's right to be forgotten. Furthermore, in seeking to strike a balance between the right to freedom of expression and the right to privacy, the Court of Cassation held that the online publication of the non-anonymised article was likely to cause damages to the applicant, which were disproportionate to the interests of the newspaper's freedom of expression, and therefore ordered the newspaper to remove all references to the individual from the article in the online archive.

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*.[139] 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.

> "As the data subject may, in the light of his fundamental rights … request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question."

Following the *Gonzalez* decision, Google has published information in its Transparency Report about de-listing requests that it has received in Europe. As at the end of February 2018, Google had received approximately 650 000 requests to de-list and approximately 2.4 million requests to remove URLs. See: https://transparencyreport.google.com/eu-privacy/overview.

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

[138] *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 forgotten', 1 June 2016 (accessible at: https://www.huntonprivacyblog.com/2016/06/01/belgian-court-of-cassation-rules-on-right-to-be-forgotten/).

[139] Case No. C-385-15, 9 March 2017 (accessible at http://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=446798).

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;[140] 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".[141]

In Europe, the EU has since codified the right to be forgotten under article 17 of the EU General Data Protection Regulation 2016/679 (**GDPR**), which provides for a data subject to have a controller erase personal information about him or her without unduly delay where one of the stipulated grounds is applicable.[142] Specifically in relation to the right to be forgotten, article 17(2) of the GDPR states as follows:

> "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."

However, article 17(3) of the GDPR goes on to state that the provisions do not apply to the extent that processing is necessary for one of the stipulated grounds, which includes for exercising the right of freedom of expression and information; for the performance of a task carried out in the public interest; for archiving purposes in the public interest; for scientific, historical research or statistical purposes, in circumstances where the erasure of the personal information is likely to render the achievement of the processing completely impossible or seriously impaired; or for the establishment, exercise or defence of legal claims.

According to the Global Principles of Freedom of Expression and Privacy (**Global Principles**),[143] 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,[144] and should be limited in scope to the domain name corresponding to the country

---

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

[141] 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).

[142] Article 17(1) of the GDPR.

[143] 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.

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

where the right is recognised and the individual has established substantial damage.[145] 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.[146]

IV. Encryption and anonymity on the internet

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 protects the confidentiality and integrity of content against third party access or manipulation.[147] 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.[148] It is also possible to encrypt data at rest that is stored on one's device, such as a laptop or hard drive.[149]

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.[150] Anonymity may be distinguished from

---

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

[146] *Id.* at principle 18(2). It states further, at principle 18(3), that the following factors should be taken into account when deciding whether or not to grant a de-listing request:

- Whether the information is personal information.
- Whether the claimant or plaintiff had a reasonable expectation of privacy with respect to the information, having regard to his or her prior conduct, whether consent had been given, and the prior existence of the information in the public domain.
- Whether the information is in the public interest.
- Whether the information at issue pertains to a public figure.
- Whether the information is part of the public record, in particular whether the material at issue has been published or recorded for journalistic, artistic, literary, or academic purposes or has been published by the government in discharge of a legal obligation to make personal data publicly available.
- In cases where the information at issue is of a public nature or has been made public with the consent of the claimant or plaintiff, whether the claimant or plaintiff has demonstrated substantial harm as a result of the availability of search results linked to their name.
- How recent the information is and whether it retains public interest value, having regard to the fact that the more recent the information, the more likely it is to be of public interest value, and that certain types of information may retain public interest value indefinitely.
- Whether alternative remedies, such as seeking voluntary deletion of the content from any third party publisher, a right to reply or a defamation claim would be more appropriate; and whether such remedies should have been exhausted first or instead.
- Whether granting a request to be de-listed is a proportionate restriction on the right to freedom of expression, having regard to all the circumstances of the case.

[147] 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).

[148] *Id.*

[149] *Id.*

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

pseudo-anonymity: the former refers to taking no name at all, whilst the latter refers to taking an assumed name.[151]

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 UNSR on Freedom of Expression:[152]

> "Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also 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.[153] 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.[154] 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.[155]

---

[151] *Id.*

[152] UNSR Report on Anonymity and Encryption at para 12.

[153] *Id.* at para 36.

[154] *Id.* at para 40.

[155] *Id.* at para 41.

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 a legal 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.[156] Creating an intentional mechanism to allow state access would inevitably undermine the security of all users online.[157]

Encryption is a tool that can be used to contribute to one's anonymity online. Anonymity has been recognised for the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation and debate. A number of courts have protected anonymity, both of individual users and of journalistic sources.[158] However, there are also a number of states that prohibit or interfere with anonymity online, for example by requiring real-name registration for online activity or through mandatory SIM card registration.[159] Attempts to ban anonymous speech have particularly been seen during times of protest as a measure aimed at protestors and activists.[160]

Intermediary liability is again of concern in relation to anonymous users, as some states have moved towards imposing responsibilities on ISPs and media platforms to regulate online comments by anonymous users. For instance, in *Delfi v Estonia*, discussed above, the ECtHR upheld an Estonian law that imposes liability on a media platform for anonymous defamatory statements posted on its site.[161]

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.[162]

As has previously been argued by MLDI, a court should only order an ISP to disclose user data where:[163]

- 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;

---

[156] *Id.* at para 42.

[157] *Id.*

[158] *Id.* at paras 47-48.

[159] *Id* at paras 49-52. With regard to mandatory SIM card registration, there are at present approximately 50 countries in Africa that require or are in the process of requiring the registration of personally identifiable data when activating a SIM card.

[160] *Id.* at para 53.

[161] Application No. 64569/09. 16 June 2015 (accessible at: http://hudoc.echr.coe.int/eng?i=001-155105).

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

[163] See MLDI's third party intervener submissions in *Standard Verlagsgesellschaft MbH*, Application No. 39378 (accessible at: http://www.mediadefence.org/sites/default/files/blog/files/20170925%20Standard%20Verlags%20v%20Austria%20Written%20Comments.pdf).

- 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.

V. Government-led digital surveillance

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.[164] This relates to both the content of communications and metadata. In respect of the latter, it has been noted that the aggregation of information – 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".[165] Surveillance – both bulk (or mass) collection of data[166] 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.[167] 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.[168]

In a resolution adopted by the 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.[169] 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.[170]

---

[164] 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).

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

[166] 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.

[167] 2016 Report of the UNSR on Freedom of Expression at para 20.

[168] Report of the OHCHR at para 2.

[169] 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).

[170] *Id.*

The 2016 UN Resolution on Privacy calls on states to, amongst other things:[171]

- Review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.

- Establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.

- Provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations.

- Develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention or use of personal data by individuals, governments, business enterprises and private organisations.

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 Necessary 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 establishing the following information to a competent judicial authority prior to conducting any communications surveillance:[172]

- 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.

[171] 2016 UN Resolution on the Safety of Journalists at para 5.

[172] Principle 5.

- 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.[173]

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.[174] 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.

This is the position adopted in the resolution adopted by the UNHRC on the safety of journalists, wherein it was emphasised that journalists in the digital age are particularly vulnerable to becoming targets of unlawful or arbitrary surveillance and/or interception of communications in violation of their rights to privacy and freedom of expression.[175] In this regard, it goes on to note that encryption and anonymity tools have become vital to journalists to secure their communications and protect the confidentiality of their sources.

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. 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

---

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

[174] 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).

[175] UNGA, 'Resolution on the safety of journalists', A/HRC/33/L.6, 26 September 2016 (**2016 UN Resolution on the Safety of Journalists**) (accessible at: https://www.article19.org/data/files/SoJ_res_Draft.pdf).

are not required to reveal their sources, subject to certain exceptions.[176] 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."[177] Surveillance activities carried out against journalists have the risk of fundamentally undermining the source protection to which journalists are otherwise entitled.[178]

[176] [2012] ZAGPJHC 71, 26 April 2012 (accessible at: http://www.saflii.*org*/za/cases/ZAGPJHC/2012/71.html).

[177] *Id.* at para 38.

[178] 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.

CHAPTER 5: SPECIFIC TYPES OF SPEECH-RELATED OFFENCES ONLINE

It has already been mentioned that, while the internet provides a range of opportunities, it also presents particular challenges. This has resulted in scenarios whereby old principles are being applied in an improper manner to the new digital landscape, or where laws are being created in an effort to quell speech online. Set out below, we consider some of the common speech-related offences that occur online, and consider the interplay between these offences and the rights that they limit.

I. Defamation and reputation

The impact of the internet, and particularly social media networks, has meant that it is easier than ever to publish content to a wide audience. Article 17 of the ICCPR provides for protection against unlawful attacks on a person's honour and reputation, and article 19(3) of the ICCPR also makes reference to the rights and reputation of others as a legitimate ground for limitation of the right to freedom of expression. Reputation is the underlying basis in any claim of defamation or libel.[179] Many countries have domestic laws regarding civil claims for defamation in instances where a person feels aggrieved about the harm that a statement or publication has caused to that person's reputation. In instances where a person is successfully able to prove a civil claim for defamation, and the person responsible for the statement or publication is not able to successfully raise a defence, the person who has suffered reputational harm is typically entitled to monetary compensation in the form of civil damages.

As stated in the Principles on Freedom of Expression in Africa, "[n]o one shall be found liable for true statements". Truth is therefore a key defence to many defence claims. In some jurisdictions, truth alone is not sufficient to establish a defence against a defamation claim: it is further required that the public interest in the publication be established as well.

In respect of the media, the South African Supreme Court of Appeal has held that strict liability in defamation cases is not compatible with the constitutional protection of the right to freedom of expression. In this regard, in *National Media Ltd and Others v Bogoshi*, the court developed the defence of reasonable publication, finding that: "[T]he publication in the press of false defamatory allegations of fact will not be regarded as unlawful if, upon a consideration of all the circumstances of the case, it is found to have been reasonable to publish the particular facts in the particular way and at the particular time."[180]

In considering the reasonableness of the publication, the court stated further that:[181]

> "[A]ccount must obviously be taken of the nature, extent and tone of the allegations. We know, for instance, that greater latitude is usually allowed in respect of political discussion, and that the tone in which a newspaper article is written, or the way in which it is presented, sometimes provides additional, and perhaps unnecessary, sting. What will also figure prominently, is the nature of the information on which the allegations were based and the reliability of their source, as well as the steps taken to

[179] For a fuller discussion on the law of defamation, see Carver, *ibid.* at pp 48-64.

[180] [1998] ZASCA 94, 29 September 1998 at 30-31.

[181] *Id.* at 31-32.

> verify the information. Ultimately there can be no justification for the publication of untruths, and members of the press should not be left with the impression that they have a licence to lower the standards of care which must be observed before defamatory matter is published in a newspaper … I have mentioned some of the relevant matters; others, such as the opportunity given to the person concerned to respond, and the need to publish before establishing the truth in a positive manner, also come to mind. The list is not intended to be exhaustive or definitive."

In *Isparta v Richter*, the South African High Court awarded damages in the amount of ZAR 40 000 for a Facebook post that the court held to be scandalous and suggesting that the plaintiff encouraged and tolerated sexual deviation and paedophilia.[182] In this case, the court not only ordered damages against the author of the posts, but also held her husband equally liable as he was tagged in the posts and failed to take steps to distance himself from them.[183]

A further aspect to consider is defamation liability for hyperlinking. The following principles should be noted:[184]

- Given the ubiquitous operation of hyperlinking on the Internet, it is an impermissible interference with the right to freedom of expression for the use of hyperlinks to be capable of giving rise to liability in defamation;
- Given the dynamic nature of the content on the internet to which hyperlinks may provide access (but over which the poster of the hyperlink is unlikely to have control), attaching liability in defamation to the provision of hyperlinks risks a particularly pronounced chilling effect on freedom of expression; and
- Defences that are available in law to the traditional media should also be made available to bloggers and online news sites – the formal designation of persons should be immaterial for the purposes of the right to freedom of expression in this context.

Some countries also still have the criminal law offence of criminal defamation on their statute books. Both the United Nations and the ACHPR have urged states to reconsider this. For instance, General Comment No. 34 provides that: "States Parties should consider the decriminalization of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty".[185] Moreover, Principle XIII(1) of the Principles on Freedom of Expression in Africa calls on states to review all criminal restrictions on content to ensure that they serve a legitimate interest in a democratic society.

In a landmark decision handed down by the African Court on Human and Peoples' Rights (**African Court**) in 2013, in the matter of *Konate v Burkina Faso*,[186] it was held that

---

[182] Case No. 22452/12, 4 September 2013 (accessible at: http://www.saflii.org/za/cases/ZAGPPHC/2013/243.html).

[183] *Id.*

[184] See the third party intervener submissions filed by MLDI and others to the ECtHR (accessible at: https://www.mediadefence.org/sites/default/files/blog/files/20170418%20Navalnyy%20v%20Russia%20Intervention%20Final.pdf).

[185] General Comment No. 34 at para 47.

[186] Application No. 004/2013 (accessible at: http://www.chr.up.ac.za/images/files/news/news_2014/Konate%20Decision%20English%20UNSIGNED%20Version%20from%20Registry%2020141217.pdf).

imprisonment for defamation violates the right to freedom of expression, and that criminal defamation laws should only be used in restricted circumstances. In that case, the editor of a weekly publication in Burkina Faso was sentenced to 12 months in prison and a fine of 4 000 000 CFA francs for defaming a state prosecutor, after he published two articles alleging an abuse of power in the prosecutor's office. In its analysis, the African Court found that the offence of criminal defamation was prescribed in the domestic law of Burkina Faso, and that its objective – namely, to protect the honour and reputation of magistrates, jurors and assessors in the performance of their duties – was legitimate. However, turning then to the third leg of the test, the African Court posed three questions: (i) are there sufficient reasons to justify the action; (ii) is there a less restrictive solution; and (iii) does the action destroy the essence of the rights guaranteed by the African Charter? The African Court also had regard to the fact that the prosecutor is a public figure, noting that "freedom of expression in a democratic society must be the subject of a lesser degree of interference when it occurs in the context of public debate relating to public figures".

In concluding that the applicable criminal defamation laws were incompatible with article 9 of the African Charter, the African Court stated as follows:[187]

> "Apart from serious and very exceptional circumstances for example, incitement to international crimes, public incitement to hatred, discrimination or violence or threats against a person or a group of people, because of specific criteria such as race, colour, religion or nationality, the Court is of the view that the violations of laws on freedom of speech and the press cannot be sanctioned by custodial sentences, without going contrary to the above provisions.
>
> The Court further notes that other criminal sanctions, be they (fines), civil or administrative, are subject to the criteria of necessity and proportionality; which therefore implies that if such sanctions are disproportionate, or excessive, they are incompatible with the Charter and other relevant human rights instruments."

Since the African Court's decision, there have been important developments in domestic courts on the continent. For instance, in 2016, *Misa-Zimbabwe et al v Minister of Justice et al,*[188] the Constitutional Court of Zimbabwe declared the offence of criminal defamation unconstitutional and inconsistent with the right to freedom of expression as protected under the Zimbabwean constitution. The following year, in 2017, in *Okuta v Attorney-General*,[189] the High Court of Kenya similarly declared the offence of criminal defamation under the Penal Code unconstitutional, finding it to be disproportionate and excessive for the purpose of protecting personal reputation, and that there existed an alternative civil remedy for defamation.

A particular aspect to consider is the application of the law of defamation to public officials. Public officials frequently rely on the law of defamation – ostensibly in an effort to safeguard their reputation – to try and curtail freedom of expression and criticism. However, there is

[187] *Id.* at paras 165-166.

[188] Case no. CCZ/07/15 (accessible at: https://globalfreedomofexpression.columbia.edu/cases/misa-zimbabwe-et-al-v-minister-justice-et-al/).

[189] [2017] eKLR (Petition no. 397 of 2016) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/okuta-v-attorney-general/).

often manifest public interest in publishing information about public officials, which may extend to their private life if it relates to, or affects, their public role. Public officials have a lower expectation of privacy as they knowingly place themselves in the public spotlight.

In the context of defamation, this has led to certain courts imposing a higher threshold on a public official or figure to establish such a claim, requiring there to be "actual malice". In *New York Times v Sullivan*, the US Supreme Court held that:[190]

> "The constitutional guarantees require, we think, a federal rule that prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with "actual malice" -- that is, with knowledge that it was false or with reckless disregard of whether it was false or not."

In a later decision, the US Supreme Court extended this to apply to all public figures, on the basis that public figures have access to the media to counteract false statements.[191]

This accords with the African Court's decision in *Konate*, wherein it stated that:

> "[F]reedom of expression in a democratic society must be the subject of a lesser degree of interference when it occurs in the context of public debate relating to public figures. Consequently, as stated by the [African] Commission [on Human and Peoples' Rights], 'people who assume highly visible public roles must necessarily face a higher degree of criticism than private citizens; otherwise public debate may be stifled altogether'."[192]

II. Breach of privacy

There will be occasions where members of the media will need to balance the right to freedom of expression with the right to privacy when determining whether or not to publish. This will be so, for instance, where the intended publication contains private facts or information about another person, or where the information has been obtained by covert means. In *Tshabalala-Msimang and Another v Makhanya and Others* – a case involving the publication of health records of the then-Minister of Health of South Africa – the court stated that "[j]ournalists should be cautious when using information that is tainted with criminal activity. It is an integral part of the professional standards of journalists to respect the right to privacy and human dignity of the individual."[193]

The right to privacy exists on a spectrum. Considerations of public interest and the public status of individuals are key determinants in whether information should be published. This was affirmed, for instance, in the case *Radio Twist v Slovakia*,[194] where the ECtHR had cause

[190] *New York Times v Sullivan* 376 US 254 (1964) at paras 279-80.

[191] *Gertz v. Robert Welch Inc* 418 US 323 (1974).

[192] *Konate v Burkina Faso*, *ibid.* at para 155. See, also, *Media Rights Agenda and Others v Nigeria* (accessible at: http://www.chr.up.ac.za/index.php/browse-by-subject/407-nigeria-media-rights-agenda-and-others-v-nigeria-2000-ahrlr-200-achpr-1998.html).

[193] [2007] ZAGPHC 161, 30 August 2007 at para 51 (accessible at http://www.saflii.org/za/cases/ZAGPHC/2007/161.html).

[194] Application No. 62202/00, 8 November 2005 (accessible at http://hudoc.echr.coe.int/eng?i=001-71431).

to consider the unlawful recording of a telephone conversation that had been broadcast on the radio. The recording was of a conversation amongst several senior members of government discussing issues around the privatisation of an insurance company. The broadcasting had not been made by the radio station, but had been dropped in its mailbox. The ECtHR had particular regard to the context and content of the conversation being clearly political in nature, and the subject-matter of the conversation being on a matter of general interest.[195] 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 being deprived of its right to freedom of expression.[196] The ECtHR therefore held that the radio station had not violated the rights of the persons who were recorded.

Principle 12(a) of the Global Principles lists the following factors to take into consideration in balancing the rights to freedom of expression and privacy, relevant in determining whether to publish: the extent to which the publication at issue 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.[197]

Furthermore, when dealing with photographs, video footage or sound recordings, regard should also be had to whether this was taken voluntarily and with consent. It has been suggested that 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 efforts have been made to address the privacy concerns to minimise the interference.[198]

III. Harassment

Harassment, threats and online violence severely restricts the enjoyment that persons have of their rights online, particularly vulnerable and marginalised groups, including women and members of sexual minorities. 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'.

---

[195] *Id.* at para 58.

[196] *Id.* at para 62. See, also, *Axel Springer AG v Germany*, Case No. 48311/10 (accessible at: https://globalfreedomofexpression.columbia.edu/cases/axel-springer-ag-v-germany-no-2/), the ECtHR unanimously found a vilation of the applicant's right to freedom of expression. The applicant newspaper has published a passage voicing suspicions that a former politician had vacated his post solely to accept a lucrative position with a German-Russian oil conglomerate. Contrary to the decisions of the German courts, the ECtHR held that Axel Springer AG had not exceeded the limits of its journalistic freedom in publishing the passage.

[197] ARTICLE 19, 'Global principles on freedom of expression and privacy: A policy brief', 2017 (accessible at: https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf).

[198] Principle 12(c) of the Global Principles of Freedom of Expression and Privacy.

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 relates 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.

A particular form of harassment, typically towards women, is that of 'revenge porn' online. This relates to a gross violation of a person's privacy where private and sexually explicit video and photographic images are published, without permission and consent, onto various websites for the purposes of extortion, blackmail and/or humiliation. In South Africa, a proposed legislative amendment seeks to criminalise the distribution of private sexual photographs and films.[199]

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[200] (**2011 ACHPR Resolution**), 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.

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,[201] 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".[202]

The 2011 ACHPR Resolution noted that killings, attacks and kidnapping of journalists, which are contrary to international humanitarian and human rights law, are often committed in an environment of impunity. As stated in the 2016 UN Resolution on the Safety of Journalists, such impunity 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.

Principle XI of the Declaration of Principles on Freedom of Expression in Africa provides as follows:

---

[199] Section 18F of the Films and Publications Amendment Bill (accessible at: https://www.ellipsis.co.za/wp-content/uploads/2017/11/B37B-2015.pdf).

[200] Accessible at: http://www.achpr.org/sessions/49th/resolutions/185/.

[201] [2017] ZAGPJHC 179 (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2017/179.html).

[202] *Id.* at para 29.

> "**Attacks on media practitioners**
> (1) Attacks such as the murder, kidnapping, intimidation of and threats to media practitioners and others exercising their right to freedom of expression, as well as the material destruction of communications facilities, undermines independent journalism, freedom of expression and the free flow of information to the public.
> (2) States are under an obligation to take effective measures to prevent such attacks and, when they do occur, to investigate them, to punish perpetrators and to ensure that victims have access to effective remedies.
> (3) In times of conflict, States shall respect the status of media practitioners as non-combatants."

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.[203] 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.[204]

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. However, 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:[205]

> "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."

[203] General Comment No. 34 at para 23.

[204] General Comment No. 34 at para 23.

[205] UNSR Report on Anonymity and Encryption at para 13.

IV. Hate speech

Not all speech is protected under international law, and some forms of speech are required to be prohibited by states. Article 20 of the ICCPR is important in this regard. It provides that:

> "(1) Any propaganda for war shall be prohibited by law.
> (2) Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."

General Comment No. 34 states that articles 19 and 20 of the ICCPR are compatible and complement each other.[206] Accordingly, the prohibited grounds listed in article 20 of the ICCPR are also subject to restriction in accordance with article 19(3), and must also be capable of justification in terms of the three-part test.[207] The key distinction, therefore, is that article 20 provides for a specific response to such speech: it must be prohibited by law.[208]

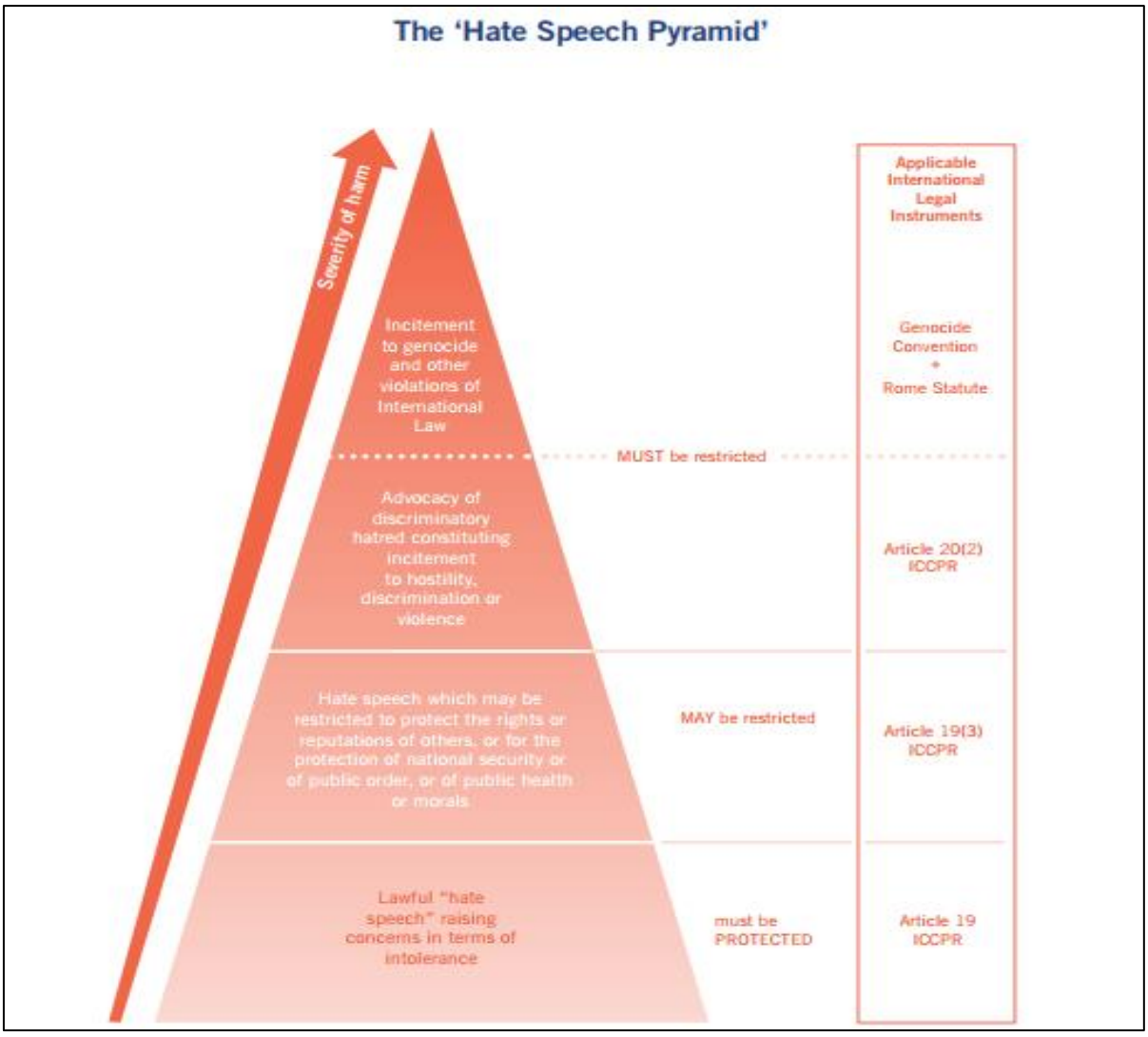
Also of relevance, article 4(a) of the International Convention on the Elimination of All Forms of Racial Discrimination requires that the dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, must be declared an offence that is punishable by law.

Hate speech provisions under international law distinguish between three categories: that which must be respected, that which may be restricted; and that which is lawful and subject to protection. This is depicted as follows:

[206] General Comment No. 34 at para 50.

[207] General Comment No. 34 at para 50.

[208] General Comment No. 34 at para 50.



Source: https://www.article19.org/data/files/medialibrary/38231/'Hate-Speech'-Explained---A-Toolkit-%282015-Edition%29.pdf

While the provisions above refer to hatred, they do not use the term 'hate speech'. This, however, has become a popular term used in domestic contexts, although it has proven difficult to define. There is a plethora of legislation that seeks to regulate hate speech, both offline and online, together with similarly vague terms, such as 'violent extremism', without providing for clear and narrowly circumscribed definitions of what is meant by these terms, or objective criteria that can be applied. Care should be exercised by states to avoid over-regulating hate speech online, and in doing so, violating the right to freedom of expression. It has been suggested that key considerations in this regard include that views on what is considered offensive or acceptable speech will inevitably change according to who is judging the speech; that allowing offensive ideas to be expressed verbally serves as an important safety valve against the expression of such ideas by means of physical violence; and that we cannot get closer to a functioning 'marketplace of ideas' if the only ideas allowed into that marketplace consist of speech that everyone agrees with or feels neutral towards.[209]

[209] Nani Jansen Reventlow, *ibid.* at p 8.

Importantly, hate speech should not be conflated with offensive speech, as the right to freedom of expression includes speech that is robust, critical, or that causes shock or offence.

While the law does not necessarily distinguish between hate speech offline and online, the following factors may give rise to a distinction:[210]

- There is the danger of conflating a rant tweeted without thinking of the possible consequences, with an actual threat that is part of a systematic campaign of hatred.
- Hate speech can stay online for a long time in different formats across multiple platforms, which can be linked repeatedly.
- Hate speech online can be itinerant, and even when content is removed, it may find expression elsewhere, possibly on the same platform under a different name or on different online spaces.
- Anonymity can also present a challenge to dealing with hate speech online.
- The internet has transnational reach, which raises issues of cross-jurisdictional cooperation in regard to legal mechanisms for combatting hate speech.

Central to the question of whether hate speech rises to the threshold of being criminal relates to the severity of the speech in question. The Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence,[211] compiled by a meeting of experts coordinated by the OHCHR, proposes the following six-part threshold test to establish whether expression is criminally prohibited:

- Context: Context is of great importance when assessing whether particular statements are likely to incite to discrimination, hostility or violence against the target group and it may have a bearing directly on both intent and/or causation. Analysis of the context should place the speech act within the social and political context prevalent at the time the speech was made and disseminated.
- Speaker: The position or status of the speaker in the society should be considered, specifically the individual's or organisation's standing in the context of the audience to whom the speech is directed.
- Intent: Article 20 of the ICCPR requires intent. Negligence and recklessness are not sufficient for an article 20 situation which requires "advocacy" and "incitement" rather than mere distribution or circulation. In this regard, it requires the activation of a triangular relationship between the object and subject of the speech as well as the audience.

[210] Iginio Gagliardone et al, 'Countering online hate speech', UNESCO at pp 13-15 (accessible at: http://unesdoc.unesco.org/images/0023/002332/233231e.pdf).

[211] Accessible at: http://www.un.org/en/preventgenocide/adviser/pdf/Rabat_draft_outcome.pdf.

- Content or form: The content of the speech constitutes one of the key foci of the court's deliberations and is a critical element of incitement. Content analysis may include the degree to which the speech was provocative and direct, as well as a focus on the form, style, nature of the arguments deployed in the speech at issue or in the balance struck between arguments deployed, etc.

- Extent of the speech: This includes elements such as the reach of the speech, its public nature, magnitude and the size of its audience. Further elements are whether the speech is public, what the means of dissemination are, considering whether the speech was disseminated through one single leaflet or through broadcasting in the mainstream media or internet, what was the frequency, the amount and the extent of the communications, whether the audience had the means to act on the incitement, whether the statement (or work of art) was circulated in a restricted environment or widely accessible to the general public.

- Likelihood, including imminence of violence: Incitement, by definition, is an inchoate crime. The action advocated through incitement speech does not have to be committed for that speech to amount to a crime. Nevertheless some degree of risk of resulting harm must be identified. It means the courts will have to determine that there was a reasonable probability that the speech would succeed in inciting actual action against the target group, recognising that such causation should be rather direct.

When assessing recourse for allegations of hate speech, it should be noted as a general principle that no one should be penalised for statements that are true. Furthermore, the right of journalists to communicate information and ideas to the public should be respected, particularly when they are reporting on racism and intolerance, and no one should be subject to prior censorship. Any imposition by a court of sanctions on the basis of hate speech should be in strict conformity with the principle of proportionality.

Outside of strictly legal measures, an important response to hate speech can be a counter-narrative. As suggested by UNESCO:[212]

> "Initiatives promoting greater media and information literacy have begun to emerge as a more structural response to hate speech online. Given young people's increasing exposure to social media, information about how to identify and react to hate speech may become increasingly important. While some schools have expressed interest in progressively incorporating media and information literacy in their curriculum, these initiatives, however, are still patchy and have often not reached the most vulnerable who need the most to be alerted about the risk of hate speech online and offline. It is particularly important that anti-hate speech modules are incorporated in those countries where the actual risk of widespread violence is highest. There is also a need to include in such programmes, modules that reflect on identity, so that young people can recognise attempts to manipulate their emotions in favour of hatred, and be empowered to advance their individual right to be their own masters of who they are and wish to become. Pre-emptive and preventative initiatives like these should also be accompanied by measures to evaluate the impact upon students' actual behaviour

[212] Iginio Gagliardone et al, *ibid*. at p 58.

online and offline, and on their ability to identify and respond to hate speech messages."

V. 'False news', ' false news', misinformation and propaganda

'Fake news' refers to news items that are intentionally and verifiably false, and seek to mislead readers. In March 2017, the Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda (**2017 Joint Declaration**) was issued by the relevant freedom of expression mandate-holders of the UN, ACHPR, OSCE and OAS.[213] The 2017 Joint Declaration noted the growing prevalence of disinformation and propaganda, both online and offline, and the various harms to which they may contribute or be a primary cause. The quandary remains that the internet both facilitates the circulation of disinformation and propaganda, and also provides a useful tool to enable responses to this.

Importantly, the 2017 Joint Declaration stressed that general prohibitions on the dissemination of information based on vague and ambiguous ideas, such as "false news", are incompatible with international standards for restrictions on freedom of expression. However, it went further to state that this did not justify the dissemination of knowingly or recklessly false statements by official or state actors. In this regard, the Joint Declaration called on state actors to take care to ensure that they disseminate reliable and trustworthy information, and not to make, sponsor, encourage or further disseminate statements that they know (or reasonably should know) to be false or which demonstrate a reckless disregard for verifiable information.

The 2017 Joint Declaration identified the following standards on disinformation and propaganda:

> "**Standards on disinformation and propaganda**
> (a) General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a), and should be abolished.
> (b) Criminal defamation laws are unduly restrictive and should be abolished. Civil law rules on liability for false and defamatory statements are legitimate only if defendants are given a full opportunity and fail to prove the truth of those statements and also benefit from other defences, such as fair comment.
> (c) State actors should not make, sponsor, encourage or further disseminate statements which they know or reasonably should know to be false (disinformation) or which demonstrate a reckless disregard for verifiable information (propaganda).
> (d) State actors should, in accordance with their domestic and international legal obligations and their public duties, take care to ensure that they disseminate reliable and trustworthy information, including about matters of public interest, such as the economy, public health, security and the environment."

False news provisions are laws which prohibit and punish the dissemination of false or inaccurate statements. This has been decriminalised in various countries. For example, in the

[213] Accessible at: http://www.osce.org/fom/302796?download=true

matter of *Chavunduka and Another v Minister of Home Affairs and Another*,[214] the Zimbabwe Supreme Court dealt with the constitutionality of the criminal offence of publishing false news under Zimbabwean law. In 1999, following the publication of an article in *The Standard* titled "Senior army officers arrested", the editor and a senior journalist were charged with contravening section 50(2)(a) of the Law and Order Maintenance Act, on the basis that they had published a false statement that was likely to cause fear, alarm or despondency among the public or a section of the public. The editor and journalist challenged the constitutionality of this provision as being an unjustifiable limitation of the right to freedom of expression and the right to a fair trial.

Of particular relevance, in finding that the section was indeed unconstitutional, the Supreme Court stated that:

> "Because s 50(2)(a) is concerned with likelihood rather than reality and since the passage of time between the dates of publication and trial is irrelevant, it is, to my mind, vague, being susceptible of too wide an interpretation. It places persons in doubt as to what can lawfully be done and what cannot. As a result, it exerts an unacceptable "chilling effect" on freedom of expression, since people will tend to steer clear of the potential zone of application to avoid censure, and liability to serve a maximum period of seven years" imprisonment.
>
> The expression "fear, alarm or despondency" is over-broad. Almost anything that is newsworthy is likely to cause, to some degree at least, in a section of the public or in a single person, one or other of these subjective emotions. A report of a bus accident which mistakenly informs that fifty instead of forty-nine passengers were killed, might be considered to fall foul of s 50(2)(a).
>
> The use of the word "false" is wide enough to embrace a statement, rumour or report which is merely incorrect or inaccurate, as well as a blatant lie; and actual knowledge of such condition is not an element of liability; negligence is criminalised. Failure by the person accused to show, on a balance of probabilities, that any or reasonable measures to verify the accuracy of the publication were taken, suffices to incur liability even if the statement, rumour or report that was published was simply inaccurate."

Accordingly, the Supreme Court held that the criminalisation of false news, as contained in section 50(2)(a), was unconstitutional and a violation of the right to freedom of expression.

More recently, the ECOWAS Court of Justice delivered a landmark judgment in the case of *Federation of African Journalists and Others v The Gambia*,[215] where it found that the rights of four Gambian journalists had been violated by the state authorities. It was submitted that security agents of The Gambia arbitrarily arrested, harassed and detained the journalists under inhumane conditions, and forced them into exile as a consequence of their work as journalists.

[214] 2000 (1) ZLR 552 (S). Accessible at: http://crm.misa.org/upload/web/CHAVUNDUKA.pdf.

[215] Application No. ECW/CCJ/APP/36/15, *ibid.*

The Court upheld the claim, finding that The Gambia had violated the journalists' rights to freedom of expression, liberty and freedom of movement, as well as violated the prohibition against torture. As such, it awarded six million Dalasi in compensation to the journalists. Importantly, The Gambia was ordered to immediately repeal or amend its laws on, amongst others, false news in line with its obligations under international law.

VI. Cybercrimes

There is no precise, universal definition of the term 'cybercrime'. In general terms, it refers to a crime that is committed using a computer network or the internet.[216] This can cover a wide range of activities, including terrorist activities and espionage conducted with the help of the internet and illegal hacking into computer systems, theft and manipulation of data, and cyber-stalking.[217]

The AU Convention deals with combatting cybercrimes in Chapter III. Article 25 of the AU Convention calls on states to adopt legislation and/or regulatory measures to prosecute cybercrimes. Importantly, in doing so, it requires states to take into consideration the choice of language that is used in international best practice. Furthermore, it provides for the rights of citizens in article 25(3), stating that:

> "In adopting legal measures in the area of cybersecurity and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions,, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others."

The AU Convention further calls on states to foster civil society involvement in the development of laws and policies, and to provide capacity-building and training on matters of cybersecurity.

There is a plethora of laws currently being enacted that seek to regulate cybercrimes, and whilst there may be a legitimate aim in doing so, there is serious concern that many of the laws are vague and overbroad, lacking clear definitions, and susceptible to being used to regulate online content and restrict freedom of expression.

As set out in *Andare v Attorney General of Kenya*,[218] the High Court of Kenya emphasised that the state has a duty to demonstrate that such laws are permissible in a free and democratic society, to establish the relationship between the limitation and its purpose, and to show that there were no less restrictive means to achieve the purpose intended.[219] In order to meet the

[216] ARTICLE19 Report on ICTs, *ibid.* at p 25.

[217] *Id.*

[218] Petition No. 149 of 2015 (19 April 2016) at para 96 (accessible at: http://kenyalaw.org/caselaw/cases/view/121033/)

[219] See, also, *Shreyal Singh v India*, Writ 167 of 2012.

test for proportionality, it has been proposed that any cybercrime law should met the following criteria:[220]

- Any legislation should provide for narrowly defined, clear and adequate definitions of key legal and technical terms covered by the offence.
- Legislation should require proof about the likelihood of harm arising from the criminal activity, including in relation to offences involving the obtaining or dissemination of classified information.
- Legislation should require the nature of the threat to national security resulting from any criminal activity to be identified.
- Legislation should provide for a public interest defence in relation to the obtaining and dissemination of information classified as secret.
- Legislation should refrain from imposing prison sentences for expression-related offences, except for those permitted by international legal standards and with adequate safeguards against abuse.

[220] *Id.* at p 26.

CHAPTER 6: THE FUTURE OF DIGITAL RIGHTS IN AFRICA

The number of internet users in Africa has grown exponentially over the last decade. Particularly with increased access to mobile services and mobile devices, people across the continent – even in rural or remote areas – have had the opportunity to enjoy their digital rights, and in particular exercise their right to freedom of expression online. Indeed, access to the internet in Africa does remain disparate with a marked digital divide, but increasing steps by states, private actors and civil society organisations have begun to lay foundations for this to be ameliorated over time.

However, the increase in access to the internet and ICTs has also led to increased violations of users' rights. This has been seen to take place through, for instance, intentional network disruptions, the enactment of laws that impermissibly limit the right to freedom of expression, surveillance and harassment online. In many instances, these measures are used to stifle criticism or dissent. These infringements not only impede the enjoyment of the right to freedom of expression, but also have ramifications for the enjoyment of other rights and services.

It is encouraging to note the positive developments that have occurred in respect of the right to freedom of expression in both the regional and domestic courts around the continent, as well as by regional bodies such as the ACHPR. These legal developments have a significant impact on the enjoyment of the right to freedom of expression, both online and offline. It is essential that the internet remains a free and open instrument that can be enjoyed by all. It is therefore essential that efforts are maintained to ensure that states and other actors do not erode digital rights in Africa.

We hope that this manual will provide a useful resource for work being undertaken in the field of freedom of expression online and digital rights. This remains a dynamic and evolving area of the law with many opportunities to foster growth and development across the continent.

GLOSSARY OF KEY TERMS

Anonymity	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. Anonymity refers to taking no name at all, whilst pseudo-anonymity refers to taking an assumed name.
Blocking of content	Preventing access to specific websites, domains, IP addresses, protocols or services included on a blacklist.
Communications surveillance	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.
Cybercrimes	A crime that is committed using a computer network or the internet.
Encryption	A mathematical process of converting messages, information or data into a form unreadable by anyone except the intended recipient, and in doing so protects the confidentiality and integrity of content against third party access or manipulation.
Filtering of content	Making use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords, or on the basis of their perceived connection to content deemed inappropriate or unlawful.
Intermediary (or internet intermediary)	An entity which provides services that enable people to use the internet, falling into two categories: (i) conduits, which are technical providers of internet access or transmission services; and (ii) hosts, which are providers of content services, such as online platforms and storage services.
Intermediary liability	Liability incurred by an intermediary where governments or private litigants can hold technological intermediaries, such as ISPs and websites, liable for unlawful or harmful content created by users of those services.
Internet shutdown	An intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.
Metadata	Data that provides information about other data, and supports the discovery, understanding and management of that data.

Network neutrality	The principle that all internet data should be treated equally without undue interference, and promotes the widest possible access to information.
Personal information (or personal data)	Any information relating to an identified or identifiable natural person (ie. the data subject), whereby 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 physical, physiological, mental, economic, cultural or social identity.