Surveillance Law in Africa: a review of six countries

Sudan country report

Mohamed Farahat

DOI: 10.19088/IDS.2021.059

Introduction

Many human rights can be affected by surveillance, including the right to freedom of expression, the right to assembly, the right to information and communication, and the right to privacy.
According to one definition, '"Communications surveillance" in the modern environment 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' (Electronic Frontier Foundation (EFF) 2013). According to the United Nations (UN) Draft Legal Instrument on Government-led Surveillance and Privacy (UN 2018),[1] surveillance is defined as 'any monitoring, collecting, observing or listening by a state or on its behalf or at its order to persons, their movements, their conversations or their other activities or communications including metadata and/or the recording of the monitoring, observation and listening activities'. Both sources refer to a broad definition of surveillance that includes all practices that constitute surveillance, whether direct or indirect. This report will therefore address all related legislation that enables or limits surveillance practices, either directly or indirectly.

The right to privacy in Sudan is protected in three ways: by the 2019 Sudanese Constitution; through international conventions that Sudan is a party to; and in Sudanese laws. But Sudanese laws also enable surveillance. While surveillance always violates the right to privacy, it is argued that narrowly targeted surveillance in strictly limited cases is legitimate to prevent greater violations such as terrorist attacks. Carefully crafted surveillance legislation and safeguards are needed to balance the tension between the right to privacy and the need for surveillance. This report will show that excessive surveillance and privacy violations occur in Sudan; it will also identify opportunities to improve privacy protections and the legal practice of narrowly targeted surveillance.

Before 2011, Sudan witnessed offline and online surveillance practices by the government, which targeted activists, lawyers and journalists (Amnesty International 2010). According to the OpenNet Initiative (2009: 4), 'the government of Sudan monitors Internet communications, and the National Intelligence and Security Service reads e-mail messages between private

1 This draft text for a Legal Instrument (LI) on Government-led Surveillance and Privacy is the result of meetings and exchanges between the MAPPING project and several categories of stakeholders shaping the development and use of digital technologies. These include leading global technology companies, experts with experience of working within civil society, law enforcement, intelligence services, academics and other members of the multi-stakeholder community shaping the internet and the transition to the Digital Age.

citizens. Media reports reveal that Sudan's police have a special unit that monitors internet cafés to stop them from providing access to sexual content'. In 2007, the National Telecommunication Corporation (NTC) 'set up a special unit to censor and filter internet content before it reaches users inside Sudan' (Abubkr 2014: 228). In 2011, under Al-Bashir's regime, the National Intelligence Security Services (NISS) established a special unit called the 'Cyber-Jihadists' to exercise online surveillance practices, conduct 'online defence operations' and 'act as a special internet and social media surveillance unit to spy on government critics, human rights activists, journalists and opposition parties' (Paradigm Initiative 2019) and censor private accounts such as emails, Twitter and Facebook (Ali 2020). Sudan is one of 21 countries that has used Hacking Team's RCS spyware (Marczak *et al.* 2014).

These state surveillance practices were present during the Sudanese revolution in 2018 as they have been in other North African countries. Sudan has used various legal tools to close civic space and control the online activities of those calling for change. According to the African Freedom of Expression Exchange (AFEX 2019: 8), 'Online expression is susceptible to monitoring, removal of content and self-censorship as individuals, and journalists fear arrests and prosecution under the existing criminal laws including the Law on Combating Cybercrimes of 2018'. In common with other countries, Sudan has seized on the Covid-19 pandemic to increase surveillance practices. Ali (2020: 121) argues that 'The government continues to rely on foreign software to spy on citizens and has taken the Covid-19 pandemic as an opportunity to use technology to increase surveillance and limit people's digital rights'.

This report reviews the Sudanese legal framework regulating surveillance practices, and examines its conformity with international standards, particularly the International Principles on the Application of Human Rights to Communications Surveillance (EFF 2013). It makes this assessment by answering a series of questions that reflect the surveillance practices in the Sudanese context. The report first outlines the contents of existing national legislation and then measures these against relevant international comparators. The report pays particular attention to the parameters within which surveillance is permitted in law and to the legal safeguards detailed in the legislation, before concluding with recommendations that aim to improve the legal framework and surveillance practices in Sudan.

The remainder of this report takes the form of answering 12 questions to enable the reader to make direct comparisons with the other five country reports.

1. What reasons does the Sudanese government use to justify surveillance?

According to principle (1) of the International Principles on the Application of Human Rights to Communications Surveillance (legality principle), 'Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.' The OpenNet Initiative (2004: 6) argues that 'Countries usually justify the laws that enable filtering by invoking one of two broad themes: upholding "community standards" and ensuring "national security"'. Sudan uses both justifications. Reviewing Sudanese domestic legislation illustrates the use of community standards and of morals, national security, and indecency as justifications for surveillance. The details of these justifications will be elaborated in Section 3 of this report.

The Sudanese Constitution and the Cybercrimes Law provide the legal basis for the right to privacy in Sudan, but other national security laws provide the basis for breaching this right, as we discuss in detail later in this report.

2. Which international conventions protecting privacy has Sudan adopted?

Sudan is party to most of the international human rights instruments that provide the basis for the universal right to privacy. This includes the Universal Declaration of Human Rights (UDHR) 1948, the International Covenant on Civil and Political Rights (ICCPR) 1966, the Arab Charter on Human Rights and the Cairo Declaration on Human Rights in Islam. In 2013, Sudan also ratified and became part of the Arab Convention of Anti-Information Technology Crimes (cybercrimes).

Table 1.1 International conventions signed and ratified by Sudan

International Conventions	Signature	Ratification
Universal Declaration of Human Rights	1948	-
International Covenant on Civil and Political Rights	N/A	1986
Convention of the Elimination of All Forms of Discrimination against Women	N/A	N/A
UN Convention on the Rights of the Child	24 Jul 1990	3 Aug 1990
Optional Protocol to Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography	N/A	2004
African (Banjul) Charter on Human and Peoples' Rights	3 Sep 1982	18 Feb 1986

Source: Adapted from University of Minnesota, Human Rights Library (no date) and Human Rights Library.

All the international instruments detailed in Table 1.1 clearly ensure the right to privacy and data protection.

3. Which domestic laws enable or limit permitted surveillance in Sudan?

Principle (2) of the International Principles states that 'Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.'

It is not only the key international conventions that Sudan is party to that prohibit surveillance and protect the right to privacy, the Sudanese Constitution also emphasises the same rights and obligations. However, domestic laws are not aligned with these international and constitutional obligations, as we discuss subsequently.

Sudan's Constitution (2019)

In 2019, the Transitional Military Council (TMC) issued the Constitution document for the transitional period (Republic of Sudan 2019). Article 42/2 stated that 'all rights and freedoms, which included in human rights instrument that ratified by Sudan are integrated part of the document'. Item (2) of same article added that all rights and freedoms in this document will be regulated by law in a manner so as to ensure that those rights and freedoms are not restricted unless it is necessary as in a democratic society.

Article 55 addresses privacy and stipulates that abuse of a person's privacy is prohibited. Interference in one's personal and family life, correspondence and home is not allowed except as prescribed by law.

Combat Information Technology crimes Law of 2018

Sudan's 2007 **Combat Information Technology crimes** (Cybercrimes Law) was revised in 2018 and amended in 2020 to increase the severity of available punishments. According to article 5/1/A of the Cybercrimes Law 2018 (amended 2020), the court will imprison for five years anyone who intentionally accesses websites that are owned by others without permission, which constitutes a safeguard to protect the right to privacy. It is worth mentioning that the punishment was previously two years (before the 2020 amendment). Article 5/1/B adds that the court will imprison for six years anyone who intentionally accesses information systems owned by others, or

deletes, destroys, discloses, copies, uses or changes that information. (The punishment term was three years prior to the 2020 amendment.)

Chapter 14 of the law, entitled Crimes Related to Moral and Public Order, criminalises the production, publishing, promotion, possession or storing of contents that breach moral and public order according to article (19). Moreover, article 22 criminalises using the internet to assault religions or their leaders. Article 20 adds prohibition of the online promotion of prostitution, indecent actions, and using applications to breach the moral and public order. Article 21 stipulates that it is considered a crime under this law to spread ideas, programmes, sayings or actions that breach 'the moral and public order'. However, there is no legal definition of 'moral and public order' or the actions considered acceptable within those terms, which leaves the law open to abuse.

Article 23/1 amended by law No. 14/2020 stipulated that the state will punish (with up to four years in prison or a fine or both) anyone who sets up or uses information and communication networks or other cyber means or applications to abuse the privacy of any person or interfere in his or her personal and family life through taking and publishing photos, reading and publishing messages, or spreading fake news. The lack of a clear definition of fake news and the legal criteria that would identify fake news give ground for surveillance practices and undermine human freedoms, particularly freedom of expression and opinion.

Article 23/2 states that the action described in 23/1 does not constitute a crime if it took place upon judicial decision, upon decision from public prosecution, or by 'competent authority'. Competent authority is not necessarily a judicial body, whereas it could be a security agency. Without a clear definition of moral and public order, the right of privacy is at risk of abuse. Lack of definition and legal criteria embody the state of legal uncertainty. The legal certainty principle as one of the rule of law indictors, simply refers to the fact that 'enforcement of legal norms in a given situation to be predictable, the incident legal norm to be easily to establish, its recipients to be certain a legal provision corresponding offense is applied, and not another one, and that it will be interpreted in a uniform manner' (Ciongaru 2016: 45). Sudan is not the only country that uses undefined words and reasons to justify and 'legalise' surveillance and breaches of the right to privacy. For example, article 25 of Egyptian cybercrime law No. 175/2018 uses the same strategy.

Communication and Post Regulation Law 2018

Without including a clear definition of 'national security' or what is considered a 'high interest of Sudan', article 6/J of the Communication and Post Regulation Law 2018 states that the purpose of the regulatory authority is to protect the national security and the high interest of Sudan in the field of ICT.

National Security Law 2010

According to the National Security Law 2010, amended by law No. 12/2020 (Republic of Sudan 2020), article 25 gives power to the National Security Agency to request any information, data or document and to retain it.

Under a previous article, the National Security Agency has a right to collect information and exercise surveillance legally. Moreover, the law did not provide any sort of guarantees that ensure the right to privacy; national security officers are not required in advance to provide any sort of justification for collecting data and using surveillance. Moreover, the law did not require any previous judicial review for such a request.

4. How does Sudanese surveillance law compare with that in other countries in Africa/US/EU/UK?

The previous sections give an overview of existing national laws that regulate surveillance practices, highlighting the key international conventions that Sudan is party to and has used to prohibit communications surveillance. This section uses the Declaration of Principles on Freedom of Expression and Access to Information in Africa (hereafter the African Declaration) (African Commission on Human and Peoples' Rights 2019) as a means to compare Sudanese law against a rights-based ideal approach in the practice of surveillance.

While principle 40 of the Africa Declaration states that 'Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information', it also states that 'Everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies'. Although the Sudanese Constitution and the Cybercrimes Law emphasised the right to privacy, this is contradicted by article 25 of the National Security Law and Article 23/2 of the Cybercrimes Law, which enable the state to breach the right of privacy and permit surveillance practices. Therefore, Sudanese legislation is not in line with international standards that guarantee the right to privacy and the inviolability of personal life and communications.

In addition, principle 41 adds that 'States shall only engage in targeted communication surveillance that is authorized by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim'. In this regard, the African Declaration is aligned with the International Principles (EFF 2013). However, Sudanese legislation breaches the principle of legal certainty as it does not clearly stipulate the legitimate aims that allow the authorities to practice surveillance, and it does not set specific time periods for the validity of judicial orders and their expiry.

5. How does Sudanese surveillance law compare with the UN Draft Legal Instrument?

As addressed in previous sections, the principles of legality, legitimate aim, proportionality and transparency are key to ensure elimination of electronic surveillance. Article 4 of the UN Draft Legal Instrument set out principles to ensure that surveillance systems shall be authorised by law prior to use. The law shall identify the purposes and situations in which the surveillance system is to be used, and define the category of serious crimes and/or threats for which the surveillance system is to be used (legitimate aims). The principles argue that states should set up and promote procedures to ensure transparency about and accountability of surveillance data and non-surveillance data for surveillance purposes. Sections 3, 4 and 9 of this report illustrate that Sudanese laws regarding surveillance are not in line with the UN Draft Legal Instrument, specifically in terms of identifying the purposes and situations where the surveillance system is to be used and defining the legitimate aims of surveillance. Moreover, applicability of the emergency law constitutes a permanent legal challenge against the right to privacy and undermines any attempts to combat surveillance practices. Therefore, one key recommendation of this report is to amend Sudan's National Security Law to bring it in line with international standards.

6. Does legislation provide adequate definitions of key legal terms?

According to principle 2 of the International Principles (legitimate aims), 'Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status'. Principle 3 (necessity) states that 'Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights'.

As already noted, existing surveillance laws in Sudan do not include definitions or explanations of key legal terms such as reasonable grounds or legitimate purpose. According to the Paradigm Initiative (2019), the Sudanese Cybercrimes Law 'uses vaguely defined terms that help regulate the content produced and consumed online'. For instance, article 21 stipulates that it is considered a crime under this law to spread ideas, programmes, sayings or actions that breach 'the moral and public order'. However, there is no legal definition of 'moral and public order' or which acts would be considered contravening that order, which leaves the law open to abuse. Furthermore, article 23/1 amended by law No. 14/2020 stipulates that the state will punish (with up to four years in prison or a fine or both) anyone who spreads fake news. Again, there is no clear definition of what constitutes fake news, which gives ground for surveillance practices and undermines human freedoms, particularly freedom of expression and opinion. In the same context, without a clear definition of 'national security' or what is considered a 'high interest of Sudan', article 6/J of the Communication and Post Regulation Law 2018 states that the purpose of the regulatory authority is to protect national security and the high interest of Sudan in the field of ICT.

7. How do legal safeguards, checks and balances, and independent oversight operate in practice?

According to the EFF (2014), the International Principles stipulate that 'States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties…' In addition, 'States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual'. Furthermore, the duty of governments to deter unlawful surveillance by way of criminal and civil sanctions reflects the requirements of international human rights law to protect individuals from breaches of their privacy, not only by the state but also by private individuals (EFF 2013).

Although Sudanese law prohibits surveillance except where authorised by judicial decision, and emphasises the right to privacy, and article 23/1 (amended by law No.14/2020) prohibits the breach of the privacy of others, article 25 of the National Security Law gives national security officers the powers to use surveillance. It is difficult to assess legal safeguards in the context of surveillance because – according to article 25 – there is no requirement for judicial permission in advance. Moreover, the lack of clear criteria, list of reasons, justifications and cases that allow issuance of a judicial decision to permit surveillance reflects the fact that existing safeguards are not sufficient and have not eliminated surveillance practices. In addition, the lack of clear definitions of key terms, legal criteria and definitions of acts that would constitute a crime under the Cybercrimes Law make legal procedures and actions unpredictable.

In conclusion, the way of drafting Sudanese law, the included legal guarantees in Sudanese laws, and using ambiguous terms are not operating to ensure elimination of surveillance practices.

8. How effective are existing laws and practices in protecting privacy and limiting surveillance?

Although Sudan is party to the ICCPR and other human rights conventions that protect the right to privacy, the Sudanese legal framework lacks a specific law to protect and guarantee the right to privacy. Despite the Constitution prohibiting abuse of personal privacy, and the Cybercrimes Law clearly prohibiting abuse of an individual's privacy (which is considered a crime), the Cybercrimes Law gives the investigating authority the right to issue orders that could abuse a person's right to privacy without providing specific grounds for doing so. Moreover, as already noted, the National Security Law gives national security agencies the power to access information without judicial review and without oversight by an independent authority.

9. Are existing surveillance practices in Sudan 'legal, necessary and proportionate'?

All surveillance is a violation of the right to privacy. However, some surveillance is legal. Legislation can define the legitimate aims of surveillance, such as the prevention of serious crimes. These legal boundaries refer to the legality of practices that constitute a restriction on human rights, and aim to protect human rights against arbitrary practices by the state (EFF 2013).

The lack of specific criteria for justifying the issuance of a judicial order and thereby permission for surveillance constitutes a breach of privacy. Lack of clear definitions of 'moral and public order' as justifications for breaching the right to privacy and lack of reasons for authorised national security officers to collect personal information reflect the difficulties in assessing whether existing surveillance practices in Sudan are legal, necessary and proportionate. The Sudanese state has absolute discretionary power to assess the necessity and proportionality of surveillance practices without any sort of judicial review.

10. How has surveillance law played out in court in Sudan?

No surveillance law cases were identified by the literature search for this report. There was one court decision related to an internet shutdown, which is reviewed here because of its potential relevance to strategic litigation on surveillance within the Sudanese judicial system.

In 2019, the Court of Appeal in Khartoum, in its decision in the case recorded under No. (M1/ASM/520/2019-/520/2019 م س أ/1م), upheld the decision of the lower court and required the mobile internet service provider (El Zain) to reconnect the communication and internet services to the plaintiff. The appellant stated that the shutdown of internet and communication in Sudan was upon verbal request from the Telecommunication Regulatory Authority on the basis of threats to national security. The court stated that the internet shutdown occurred after the success of the Sudanese revolution, which led to removing Al-Bashir's regime on 11 April 2019, successfully arguing that there was no national threat at that time. The court found that the internet shutdown was in breach of Article 39/1 of the suspended Sudanese Constitution, which stipulated that each citizen has the unrestricted right to freedom of expression and to receive and spread information.

11. What is working? What gaps are there in existing policy, practice, knowledge and capacity?

Although Sudanese law includes basic effective legal provisions that could play a role in protecting the right to privacy, the same law includes other provisions that compromise its effectiveness.

The lack of personal data protection law in Sudan is a major gap in privacy protection. Moreover, article 25 of the National Security Law, which gives the National Security Agency the right to request personal data and keep a copy of it, opens the door to secret and arbitrary surveillance practices.

Article 23/2 of the Cybercrimes Law does not specify the legitimate aims that allow the investigating authority or judicial bodies to breach privacy and carry out legitimate surveillance practices. This constitutes abuse of the principle of legal certainty.

In light of Chapter 14 of the Cybercrimes Law, entitled Crimes Related to Moral and Public Order, definitional clarity is needed. The lack of a legal definition of what constitutes 'fake news' or 'public and moral order' leaves the law open to abuse.

12. What recommendations arise for future legislation, practice, or further research?

Parliament and legislators

- Amend article 23/2 of the Cybercrimes Law by specifying the 'legitimate aims' that investigating agencies can use to request permission to conduct targeted surveillance.
- Ensure respect for the principle of legal certainty by clearly defining in law the parameters of national security, fake news and moral and public order.
- Require prior authorisation from a judicial authority for all surveillance. Require a judge to test requests for reasonable grounds, legality, necessity and proportionality.
- Amend the National Security Law and specify the cases that give the National Security Agency the right to collect information, which should be upon judicial order in advance.
- Adopt a data protection law.

Non-governmental organisations (NGOs)

- Build the capacity of lawyers on digital rights to enable them to conduct strategic litigation in surveillance practices and right to privacy, and encouraging them to challenge surveillance motivation laws before constitutional courts.
- Establish a coalition between NGOs working on digital rights to engage in the policy-making process and communicate with decision-makers to advocate for improvements to existing laws and practices and bring them in line with the International Principles.
- Use international and regional human rights mechanisms to change existing policies, practices and laws.

Academia and research centres

- Produce a policy paper focusing on surveillance legislation gaps and suggest changes required to ensure the right to privacy.
- Conduct comparative analysis of experiences of other countries in the region to explore applicable experience and solutions that could apply in Sudan.

References

Abubkr, L.E. (2014) 'Sudan', in A. Finlay (ed), ***Global Information Society Watch 2014: Communications Surveillance in the Digital Age***, APC and Hivos (accessed 10 August 2021)

AFEX (2019) ***AFEX Annual Report on the State of Internet Freedom in Africa - 2019***. Accra: African Freedom of Expression Exchange (accessed 13 August 2021)

African Commission on Human and Peoples' Rights (2019) ***Declaration of Principles on Freedom of Expression and Access to Information in Africa*** (accessed 10 August 2021)

Ali, A.M. (2020) **'Sudan Digital Rights Landscape Report'**, in T. Roberts (ed), *Digital Rights in Closing Civic Space: Lessons from Ten African Countries*, Brighton: Institute of Development Studies (accessed 10 August 2021)

Amnesty International (2010) ***Agents of Fear: The National Security Service in Sudan***, London: Amnesty International (accessed 10 August 2021)

Ciongaru, E. (2016) **'Constitutional Law Connotations of Legal Certainty in the Rule of Law'**, *Fiat Iustitia* No. 1/2016: 43–50

EFF (2013) ***International Principles on the Application of Human Rights to Communications Surveillance***, Electronic Frontier Foundation (accessed 9 August 2021)

Marczak, B.; Guarnieri, C.; Marquis-Boire, M. and Scott-Railton, J. (2014) **'Mapping Hacking Team's "Untraceable" Spyware'**, *The Citizen Lab,* 17 February (accessed 10 August 2021)

OpenNet Initiative (2009) ***Internet Filtering in Sudan*** (accessed 10 August 2021)

OpenNet Initiative (2004) ***A Starting Point: Legal Implications of Internet Filtering*** (accessed 10 August 2021)

Paradigm Initiative (2019) ***Digital Rights in Africa Report 2019***, Lagos: Paradigm Initiative (accessed 10 August 2021)

Republic of Sudan (2020), Khartoum: Ministry of Justice, Government of the Republic of Sudan, *Official Gazette* Issue No. 1904, 13/7/2020

Republic of Sudan (2019) The Constitutional Document for the Transitional Period, *Official Gazette,* Issue No. 1895, 3/10/2019

UN (2018) ***Draft Legal Instrument on Government-Led Surveillance and Privacy*** (accessed 10 August 2021)

University of Minnesota, Human Rights Library (no date) ***'Ratification of International Human Rights Treaties – Sudan'*** (accessed 10 August 2021)