Surveillance Law in Africa: a review of six countries

Egypt country report

Mohamed Farahat

DOI: 10.19088/IDS.2021.059

Introduction

Surveillance affects many human rights, including the right to freedom of expression, right to assembly, right to information and communication, and right to privacy. In Egypt, surveillance practices were used before 2011 under the regime of Hosni Mubarak to monitor terrorist activities. Following the key role that social media played during the 2011 revolution and later protests, the regime took specific measures to control access to the internet and target activists with surveillance. Since 2011, different Egyptian regimes have used various technical means to surveil activists and online content. They have used legislation to ban websites, obtain personal data, abuse citizens' right to privacy and criminalise the right to freedom of expression using accusations of fake news.

Although Egypt is party to a number of international conventions protecting citizens' right to privacy, several state agencies are exempt from legislation and there is evidence that the government regularly violates citizens' right to privacy. According to Paradigm Initiative (2019: 15): 'In 2019, a series of sophisticated cyber-attacks targeting the nation's journalists, academics, lawyers, opposition politicians and human rights activists [took place]'. The report added that since that time 'the surveillance activity of government has only deepened and not ceased. A number of the targets of surveillance were then arrested by Egyptian authorities' *(ibid.)*. These surveillance practices and newly adopted legislation led to the closing of civic space in Egypt and abuse of the right to privacy and digital rights (Farahat 2020a).

This report reviews the Egyptian 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 2014). It makes this assessment by answering a series of questions that reflect on surveillance practices in the Egyptian context. The report will first outline the content of existing national legislation and then measure it 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 a number of recommendations.

Communications surveillance has been defined in various ways. In the International Principles, the term refers to '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'. According to article 2(1) of the United Nations (UN) Draft Legal Instrument on Government-led Surveillance and Privacy (2018):[1]

> surveillance is any monitoring, collecting, observing or listening by a state or on its behalf or on its orders of 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 definitions refer to the broad definition of surveillance, which includes all practices that constitute surveillance whether directly or indirectly. Therefore, this section of the report will address all related legislation that enables or limits surveillance practices, whether directly or indirectly.

The remainder of this report takes the form of answers to 12 questions.

1 This draft text for a Legal Instrument 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.

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

According to principle 1 of the International Principles (legality):

> 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.
> (EFF 2014)

Citizens' right to privacy is protected in Egyptian law. However, state agencies have been given permission to violate this right in specific circumstances. Reasons the government argues justify breaching privacy and carrying out surveillance include national security, states of emergency, terrorism and cybercrime. These are referred to as 'legitimate aims' in the language of the International Principles.

2. Which international conventions protecting privacy has Egypt adopted?

The 2014 Constitution of Egypt (art. 151) states that, 'Egypt is obliged by all international human rights conventions that it has ratified, and they have the same power as the law once published' [author's translation].

International human rights conventions

In the context of privacy, Egypt is party to several international human rights instruments that provide the right to privacy, such as the Universal Declaration of Human Rights (UDHR) 1948 and International Covenant on Civil and Political Rights (ICCPR) 1966. Egypt is also a party to the African (Banjul) Charter on Human and Peoples' Rights 1980 and Arab Convention of Anti-information Technology Crimes (Cybercrimes) 2010.

Table 1.1 Egypt's ratification status

Instruments of the International Labour Organization	Date of signature	Date of ratification
Universal Declaration of Human Rights	1948	
International Covenant on Civil and Political Rights	04 August 1967 (optional protocol not signed)	14 January 1982
International Covenant on Economic, Social and Cultural Rights	04 August 1967 (optional protocol not signed)	14 January 1982
Convention on the Elimination of All Forms of Discrimination against Women	16 July 1980	18 September 1981
UN Convention on the Rights of the Child	05 February 1990	06 July 1990
African (Banjul) Charter on Human and Peoples' Rights	16 November 1981	20 March 1984
Arab Charter on Human Rights		2018
Arab Convention of Anti-information Technology Crimes (Cybercrimes) 2010		8 October 2014
Cairo Declaration on Human Rights in Islam	05 August 1990	

Source: Adapted from University of Minnesota, Human Rights Library[2]

2 http://hrlibrary.umn.edu/research/ratification-egypt.html

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

It is not only the legality principle that the state should adhere to; surveillance should also have a legitimate aim. According to principle 2 of the International Principles:

> 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.
> (EFF 2014)

Not only do the key international conventions to which Egypt is party prohibit surveillance and protect the right to privacy, but the Egyptian constitution also emphasises the same rights and obligations. However, domestic laws do not align with these international and constitutional obligations, as is discussed later in this report.

a) 2014 Constitution of Egypt

Privacy of communication is constitutionally guaranteed for all Egyptian citizens. Article 57 of the constitution stipulates that:

> Telegraph, postal, and electronic correspondence, telephone calls, and other forms of communication are inviolable, their confidentiality is guaranteed, and they may only be confiscated, examined or monitored by causal judicial order, for a limited period, and in cases specified by the law; the state shall protect the rights of citizens to use all forms of public means of communication, which may not be arbitrarily disrupted, stopped or withheld from citizens, as regulated by the law.
> (Arab Republic of Egypt 2014 [author's translation])

According to article 71 of the constitution: 'it is prohibited to censor, confiscate, suspend or shut down Egyptian newspapers and media in any way. In exceptional circumstances, they may be subject to limited censorship in times of war or general mobilization' *(ibid.)*. Despite these constitutional

guarantees some Egyptian laws provide a legal basis for surveillance in certain circumstances.

Egypt has domestic legislation that provides the legal basis for surveillance such as Emergency Law no. 162 (1958), Telecommunications Regulation Law no. 10 (2003), Anti-Terrorism Law no. 94 (2015), Anti-Cyber and Information Technology Crimes (Cybercrime Law) no. 175 (2018) and Personal Data Protection Law no. 151 (2020).

b) Emergency Law no. 162 (1958)

The Emergency Law is one of the legal tools that permits surveillance in the context of a declared emergency. This law is designed to be used only in a state of emergency, which by its nature is temporary, exceptional and for a limited time. However, in Egypt states of emergency have been used on a regular basis and, having been declared, are frequently extended (often multiple times). One is in place at the time of writing this report. Article 3(2) of the Emergency Law stipulates that, 'the President has a right to order surveillance of all messages, whatever their type, and to monitor all means of expression.' Although the constitutionality of article 3 has been challenged before the Constitutional Court (case no. 17/15/2013), the court ruled that searching physical spaces was unconstitutional but made no ruling on digital surveillance.

c) Telecommunications Regulation Law no. 10 (2003)

Article 64(1) of the law prohibits using devices to encrypt communication without permission from security agencies. Article 64(2) stipulates that service providers should collect accurate information and data about service users. Article 67 gives the competent authority power to control all communication services. Prevention of encrypted communication violates citizen's right to privacy and to anonymity.

d) Anti-Terrorism Law no. 94 (2015)

Without clarifying the grounds that justify surveillance, article 46 of the law authorises public prosecutors or 'any other investigating authority' in the case of terrorist crime, upon a justifiable order to surveil, to record conversations and messages; and to record and photograph what happens in private places or via websites for a period of not more than 30 days. The surveillance order is renewable for another period or periods. This means that the surveillance order could be renewed indefinitely, particularly as the law does not identify safeguards for renewing the surveillance order.

e) Cybercrime Law no. 175 (2018)

The law enables state surveillance by requiring all phone and internet service providers to record and store all communications and metadata and to make them available to state agencies. Article 2/first/(1) of the law states that service providers should retain and store information system records for a period of 180 continuous days. The retained information should include: data that can identify service users; and data relating to the contents of the information system used. Article 2(2) adds that service providers should maintain the confidentiality of retained and stored data, including: users' personal data; information relating to the websites and private accounts they navigate and log into; and persons and destinations they communicate with.

Article 6 gives the power to the investigating authority to issue a decision allowing surveillance and access to information. Although individuals have the right to challenge the surveillance order before a court (art. 6(2)), the order can be issued without obtaining prior court authorisation. This means investigating authorities are able to access data possessed by internet service providers relating to all user activities, including phone calls, text messages, websites navigated, and applications used on smartphones and computers.

In a different context, article 25 criminalises breaches of the 'principles and values of Egyptian families', without providing a legal definition of those principles and values. As a result, in July 2020 several Egyptian women were arrested on charges related to this article, now known as the 'TikTok girls' case (Columbia University n.d.).

f) Personal Data Protection Law no. 151 (2020)

The UN Human Rights Committee in its general comment no. 16 on article 17 of the ICCPR states that:

> integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.
> (UNHRC 1988)

Article 3 of the Egyptian Personal Data Protection Law stipulates that 'the law will not apply to the personal data in the possession of national security bodies'. Article 1 identifies the national security bodies as: 'The Presidency of

the Republic, the Ministry of Defence, the Ministry of Interior, the Intelligence Service and the Administrative Oversight Authority'. This means that national security bodies are able to possess all personal data without legal justification.

Although, the legislation's claimed purpose is to protect rights, in practice the Egyptian legal framework has been the strongest tool used to abuse digital rights during the coronavirus (Covid-19) pandemic (Farahat 2020b).

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

The previous sections give an overview of existing national laws regulating surveillance practices, highlighting the key international conventions that Egypt is part of and has used to prohibit communications surveillance. This section uses the Declaration of Principles on Freedom of Expression and Access to Information in Africa as a means to compare Egyptian law against an ideal rights-based approach to surveillance practice.

Principle 40 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa states that:

> Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information and 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.
> (African Commission on Human and Peoples' Rights 2019)

The Egyptian constitution guarantees the inviolability of private communication and prohibits surveillance (art. 57 and art. 71). However, article 6 of the Cybercrime Law as well as article 3(2) of the Emergency Law authorise the state to breach the right to privacy and enable it to practise surveillance under legal cover.

In addition, principle 4(1) of the African Declaration of Principles on Freedom of Expression and Access to Information in Africa 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 above-mentioned declaration, 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.
> (ibid.)

Nevertheless, the Egyptian legal framework does not require any test for reasonable suspicion prior to authorising surveillance targeting communications. Egyptian laws enumerate the circumstances in which

authorities are allowed to target communications. Moreover, article 67 of the Telecommunications Law gives the competent authority the right to control all communications services. According to a report by the **Association for Freedom of Thought and Expression** (2020): '[mobile telecoms operator Orange Egypt] said on its website that it "has the right to disclose all or some of the data and information of its customers if this is in implementation of the law or a decision issued by a competent judicial authority or any of the national security agencies"'.

In the context of principle 42 of the declaration ('Legal framework for the protection of personal information'), Egypt has adopted a legal framework for data protection. Although the law attempts to align with international standards, especially the European Union (EU)'s General Data Protection Regulation (GDPR), the law contains some provisions that contradict the right to privacy, such as article 3, which gives security agencies the right to access personal information without specific restriction. Although Egypt has adopted legislation that is apparently in line with international standards, on closer inspection these pieces of legislation have many legal gaps, as discussed in section 9 of this report.

The International Principles are an additional point of comparison for Egyptian surveillance law. The International Principles were cooperatively drafted by more than 40 international privacy and security experts at a meeting in Brussels in October 2012 and officially launched at the UN Human Rights Council in Geneva in September 2013 (EFF 2014).

When assessing Egyptian laws against the 13 International Principles, it is clear that Egyptian legislation falls short in a number of regards. Gaps exist particularly regarding the principle of legality, which refers to the fact that any surveillance practices should be as prescribed in legislation. Although surveillance takes place according to law, ambiguous provisions and the exemption of some security agencies from the law's applicability make surveillance practices in Egypt illegal. Moreover, Egyptian laws do not align with the principles of necessity and legitimate aim, which refer to the fact that surveillance should have to achieve a legitimate aim (such as preventing terrorist attacks). It is important the legislation defines clearly what are considered to be legitimate aims. The issue of proportionality is also central to the principles. This requires the authorities to weigh the benefit sought from surveillance against the violation of privacy rights. The Emergency Law exempts security agencies from the applicability of the principle of proportionality, and it constitutes the root of all abuses of human rights in Egypt according to Hassanin (2014), who argues that: 'The emergency law seems to be diametrically opposed to the [International Principles]'.

According to the authors of the International Principles (EFF 2014), 'States should enact legislation criminalizing 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 not be retained, but instead be destroyed or returned to those affected.'

This principle reflects that:

> 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.
> (ibid.)

According to article 36 of the Personal Data Protection Law:

> the controller and possessor shall be punished with a fine of not less 100,000 Egyptian pounds[3] and not more than 2m Egyptian pounds,[4] [and] anyone who collects, processes, discloses, or circulates any personal data which is electronically processed in non-permissioned cases or without consent of data subject.

According to the same article:

> the punishment will be jail for not less six months and a fine of not less than 200,000 Egyptian pounds[5] and not more than 2m Egyptian pounds or one of these punishments if the purpose was not for material or moral benefit or for the purpose of exposing the data subject to harm and risk.

Article 41 of the same law stipulates that the:

> processor, controller and possessor shall be punished with jail for no less three months and a fine of not less than 500,000 Egyptian pounds[6] and not more than 5m Egyptian pounds[7] or one of these punishments, for collecting, processing, disclosing, circulating, storing and maintaining any sensitive personal data in non-permissioned cases or without consent of the data subject.

3 c.US$6,400.
4 c.US$127,400.
5 c.US$12,800.
6 c.US$31,850.
7 c.US$318,450.

5. How does Egyptian 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 principles that ensure the elimination of unauthorised electronic surveillance. Article 4 of the UN Draft Legal Instrument set out, *inter alia,* principles that ensure that surveillance systems shall be authorised by law prior to use. This law identifies the purposes and situations where surveillance systems are to be used and defines the category of serious crimes and/or threats for which surveillance system are to be used. States should set up and promote procedures to ensure transparency about and accountability for government demands for surveillance data and non-surveillance data for surveillance purposes.

A review of sections 3, 4 and 9 of this report illustrate that Egyptian laws regarding surveillance are not in line with the UN Draft Legal Instrument, specifically in terms of identifying the purposes and situations in which surveillance systems are to be used and defining the category of serious crimes and/or threats for which they are to be used. Moreover, the applicability of the Emergency Law constitutes a permanent legal challenge to the right to privacy and undermines any attempts to combat surveillance practices. Therefore, one of the indispensable recommendations of this report is to amend the Emergency 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 aim):

> 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. (EFF 2014)

According to principle 3 (necessity):

> 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. (ibid.)

The review of the national laws in section 3 of this report reveals that they do not include an adequate definition of key legal terms or use vague terms. For example, article 1 of the Cybercrimes Law defines national security as: 'everything related to the independence, stability, and security of the homeland and anything related to the affairs of the Presidency, the Ministry of Defence and General Intelligence, and the Administrative Oversight Authority'. The same article and article 1 of the Personal Data Protection Law identifies the national security bodies as: 'The Presidency of the Republic, the Ministry of Defence, the Ministry of Interior, the Intelligence Service and the Administrative Oversight Authority'. Other than these definitions, no existing laws address or explain the definitions of key legal terms such as reasonable grounds, legitimate purpose, etc.

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

Although the existence of the laws ensures the right to privacy and restricts surveillance practices, constituting a legal guarantee, it does not at all demonstrate the efficiency of the laws, particularly if these legal safeguards are not clear or if they are restricted by exceptional laws, namely emergency laws. Article 3 of the Personal Data Protection Law specifies the pre-conditions for collecting data. These include: collecting data for a specific purpose; declaring to the data subject that their collected data will be processed legitimately and explaining the relevance and purpose of collecting their data; and not retaining data for longer than the period necessary to fulfil the purpose of collecting it.

However, article 2/first/(1) of the Cybercrime Law states that service providers should retain and store records of information systems for a period of 180 continuous days. The retained information should include: data that can identify service users; and data relating to the contents of the information system used. Item 2 of the same article adds that service providers should maintain the confidentiality of retained and stored data, including: users' personal data; information relating to the websites and private accounts they navigate and log into; and persons and destinations they communicate with it.

This reflects that legal guarantees in the Personal Data Protection Law directly conflict with the Cybercrime Law.

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

Principle 5 of International Principles (proportionality) states that:

> Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interest.
> (EFF 2014)

As mentioned in the previous section, existing laws are not sufficient to ensure respect for privacy or to eliminate surveillance and they do not consider the sensitivity of information and data. Although Egypt is party to the ICCPR and other human rights conventions that protect the right to privacy guaranteed in the constitution, there is no specific guarantee of privacy written into domestic Egyptian law. Additionally, new legislation about data protection only applies to electronic data and does not address physical data, which means that privacy is still at risk of abuse.

On the other hand, the exception which excludes information in the possession of security agencies from application of the Personal Data Protection Law reflects that the existing laws are not efficient at protecting privacy or limiting surveillance. On the contrary, they allow the expansion of surveillance. For example, existing laws have been used to enable surveillance of social media platforms and to track information posted about Covid-19, which has led to the arrests of many people who have been interrogated for circulating 'fake news' (Farahat 2021b). In addition, the Emergency Law is the main factor in the breakdown of legal guarantees, in contravention of the International Principles (Hassanin 2014).

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

All surveillance is a violation of the right to privacy. However, some surveillance is legal. Legislation can define 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. They aim to protect human rights against arbitrary state practices (EFF 2014).

Article 2/first/(1) of the Cybercrime Law allows personal information to be retained for 180 days, as discussed in sections 3 and 7 of this report. The article does not mention what constitutes a legal and proportionate purpose behind obliging service providers to retain this information for six months.

In conclusion, although being legal, necessary and proportionate are mentioned in some provisions, without clear definition in law it is not possible to apply these tests prior to authorisation. Without transparency in the decision-making process, and publication of statistics on requests and authorisation, it is not possible to verify whether practices are aligned with the intent of legislators or fulfil the International Principles. Moreover, the investigating authority and national security bodies are the only bodies that have the absolute discretionary power to define, determine and assess the legality, necessity and proportionality of surveillance, which creates a state of legal uncertainty. Without independent oversight, the state is judge, jury and regulator.

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

Laws do not operate and are not implemented in a vacuum. How courts apply and interpret the law and identify judicial trends needs to be explored, and this would help evaluate to what extent using litigation in surveillance cases could help to change and improve – in strategic ways – existing laws, practices and surveillance-related policies. Despite the absence of surveillance test cases brought before the courts, it is important to point out two court cases. According to a report by Amnesty International (2014):

> the Interior Ministry calls for tenders for a more sophisticated mass monitoring system which will scan social media networks for 26 topics including defamation of religion, calling for illegal demonstrations, strikes and sit-ins as well as terrorism and inciting violence. However, the full list of topics to be monitored has not been made public, leaving individuals unsure of whether and when their communications will be targeted.

In case no. 63055 (28 February 2017), the plaintiff, Egyptian citizen Mustfa Hussien Hassan, brought a case against the Minister of Interior, asking the court to suspend and cancel the decision of the Minister of Interior to conduct a tender for a social media security risk monitoring software system, known as the public opinion measurement system. Although the administrative judiciary court dismissed the case for procedural errors, the court clearly stated that the contract process for this project had already been completed and had entered into force. What is remarkable about this court decision is that the Ministry of Interior did not deny using a surveillance system and surveillance techniques.

In Constitutional Court case no. 17/2013 the court ruled that article 3(1) of the Emergency Law, which allowed authorities to search and arrest persons without the restriction of the criminal procedure code, to be unconstitutional. This is evidence that the courts could play a potentially significant role in challenging surveillance practices. These two cases highlight the great potential of using strategic litigation as a mechanism to test surveillance practices, which in the long term could assist in amending the laws that enable surveillance.

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

Although personal data protection refers to 'law designed to protect your personal data' (Privacy International 2018: 9), the first article of the Personal Data Protection Law stipulates that data protection law only applies to data that is processed electronically, which means that adoption of the law does not really aim to protect personal data and the right to privacy (Technology & Law Community 'Masaar' 2021: 1). Publishing the executive regulation of law would reveal the exact aim behind adopting the new Personal Data Protection Law. It is doubtful this would change the perception of the law.

Although the Egyptian Personal Data Protection Law resembles international standards on privacy and data protection, the law does not align with these international standards where it exempts security agencies from data protection law. Egyptian law gives security agencies the power to process personal data without the prior consent of the data subject. Collecting, accessing, and processing data do not constitute a breach of the right to privacy if they occur in a legitimate manner, for a legitimate purpose and in a lawful way. However, the existence of the national security exemption significantly weakens data protection and privacy (SMEX 2021).

In the context of principle 42 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa ('Legal framework for the protection of personal information'), Egypt adopted the required legal framework on data protection in July 2020. Although the law attempts to align with international standards, especially GDPR, it contains provisions that contradict the right to privacy; for example, the third article, which gives security agencies the right to access personal information without specific restriction. This supports the conclusion that: 'Numerous Egyptian security agencies are permitted to conduct electronic surveillance, frequently with limited court oversight' (Marczak *et al.* 2015:18).

The Telecommunications Regulation Law constitutes an additional legal challenge, motivating and protecting illegal surveillance practices. Article 64(1) of the law prohibits using devices to encrypt communication services without permission from security agencies. Moreover, article 64(2) of the same law states that the 'services provider should collect accurate information and data about service users' [author's translation]. As a result, some reports

state that: 'Telecommunications surveillance is facilitated under the 2003 Telecommunications Regulation Law' (Marczak *et al.* 2018: 26).

The same report states that:

> This law compels telecommunications operators to provide technical capacity for the military and national security entities to 'exercise their powers within the law' as well as prohibiting the use of 'telecommunication services encryption equipment' without written authorization from entities including the armed forces.
> (ibid.)

In terms of privacy and communication surveillance, article 6 of the Cybercrime Law authorises the investigation authority to issue a decision that allows surveillance and access to personal information. Although the article reveals that it is in line with international standards and principle 41 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa, in practice there have been many breaches of this provision, with people subjected to searches of their mobile phones without advance permission from the investigation authority; for example, 'police stopping young persons in public places and searching their telephones for evidence of involvement in political activities deemed antigovernment in nature' (US Embassy in Egypt 2021).

There is a clear conflict between article 3 of the Personal Data Protection Law and article 2/first/(1) of the Cybercrime Law, which obliges service providers to retain personal data and data related to online activities, messages and communication. As a result, activists have been interrogated over circulating fake news (Farahat 2021a) about Covid-19; for example, as detailed in State Security cases no. 535 and no. 558 of 2020, involving doctors, journalists, activists, citizens and researchers, which indicate that there was government surveillance of social media targeting users who circulated information about Covid-19 or criticised the performance of government in dealing with the crisis.

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

In conclusion, the existing legal framework in Egypt is not effective at protecting citizens' right to privacy. Existing legislation does not sufficiently define what constitutes a legitimate aim or reasonable grounds for surveillance. It does not provide sufficient clarity about the assessment of whether proposed surveillance is legal, necessary or proportionate. Although the constitution makes citizens' privacy inviolable, and parliament has adopted international conventions expanding and extending these rights, existing laws falls short of the International Principles and the Declaration of Principles on Freedom of Expression and Access to Information in Africa. Therefore, the following actions are strongly recommended.

General

- Surveillance practice should be within very narrow limits. Legality, necessity and proportionality of surveillance decisions and orders should be subjected to prior judicial review. Any exceptional authority for any agency should be suspended immediately. As long as surveillance practices affect human rights, there should be oversight by a competent judicial body.

For the Egyptian parliament

- Parliament should amend or cancel article 2/first/(1) of the Cybercrime Law regarding retaining data for 180 days in a manner that prevents abuse of users' privacy.
- Parliament should amend the Telecommunications Regulation Law and ensure the legitimacy of surveillance practices. It should require that surveillance has an explicit legitimate aim. Courts should be responsible for assessing the existence of a legitimate aim for surveillance and issuing the surveillance order based on their own assessment, giving a person who will be under surveillance the right to challenge the first instance court decision before higher or appeal court.
- Parliament should activate its parliamentary oversight tools to monitor abuses of the right to privacy and illegitimate surveillance practices.
- Parliament should establish a fact-finding committee responsible for investigating surveillance practices and its root causes, which would

report its findings and make recommendations before the whole parliament.

For academia and researchers

- Court cases and decisions related to surveillance practices should be analysed and studied, and judicial trends in this respect should be identified at regional and national levels.
- The impact and potentiality of using judicial bodies to change existing laws, practices and policies should be assessed.

For NGOs

- Capacity-building is required for lawyers and NGOs on using strategic litigation mechanisms nationally, regionally and internationally in surveillance and digital rights cases.
- Public awareness on privacy rights and surveillance practices needs to be increased.
- Concerns should be raised about surveillance practices during universal periodic reviews and via shadow reports.

References

African Commission on Human and Peoples' Rights (2019) ***Declaration of Principles on Freedom of Expression and Access to Information in Africa***, Banjul (accessed 18th September 2021)

Amnesty International (2014) ***Egypt's plan for mass surveillance of social media an attack on internet privacy and freedom of expression*** (accessed 4 August 2021)

Arab Republic of Egypt (2014) Egyptian Constitution, *Official Gazette* issue 3 (bis)A, 18 January

Association for Freedom of Thought and Expression (2021) ***The Internet and the Law in Egypt Series*** (accessed 4 August 2021)

Columbia University (n.d.) ***The Case of the Egyptian TikTok Influencers*** (accessed 4 August 2021)

Electronic Frontier Foundation (EFF) (2014) ***Necessary & Proportionate: The International Principles on the Application of Human Rights to Communications Surveillance*** (accessed 18th September 2021)

Farahat, M. (2021a) ***Coronavirus Trials in Egypt: Blurring the Lines Between Fake News and Freedom of Expression***, SMEX (accessed 4 August 2021)

Farahat, M. (2021b) Egypt Digital Rights Landscape Report, in T. Roberts (ed.), ***Digital Rights in Closing Civic Space: Lessons from Ten African Countries,*** Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2021.014**

Hassanin, L. (2014) *Global Information Society Watch 2014*, APC and Hivos

Marczak, B; Dalek, J.; McKune, S.; Senft, A.; Scott-Railton, J. and Deibert, R. (2018) ***Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?***, Citizen Lab Research Report No. 107, University of Toronto (accessed 18th September 2021)

Marczak, B.; Scott-Railton, J.; Senft, A.; Poetranto, I. and McKune, S. (2015) ***Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation***, Citizen Lab Research Report No. 64, University of Toronto (accessed 18th September 2021)

Organisation of African Unity OAU) (1981) *African (Banjul) Charter on Human and People's Rights*, OAU Doc. CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982), Banjul

Paradigm Initiative (2019) *Digital Rights in Africa Report 2019,* Lagos: Paradigm Initiative

Privacy international (2018) ***A Guide for Policy Engagement on Data Protection – Part 1: Data Protection, Explained*** (accessed 4 August 2021)

SMEX (2021) ***Data Protection and Privacy Laws in MENA: A Case Study of Covid-19 Contact Tracing Apps***, Social Media Exchange Association (accessed 4 August 2021)

Technology & Law Community 'Masaar' (2021) ***Personal Data Protection Law: Does it Really Aim at Bolstering the Right to Privacy? Or is it an Attempt to Give the Illusion of an Improvement in the Legislative Environment?*** (accessed 4 August 2021)

United Nations Human Rights Committee (UNHRC) (1988) CCPR General Comment No. 16: Article 17 (Right to Privacy), ***The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation***, 8 April (accessed 2 July 2021)

US Embassy in Egypt (2021) ***2020 Country Reports on Human Rights Practices: Egypt, Bureau of Democracy, Human Rights, and Labor*** (accessed 4 August 2021)